THÈSE

Pour l'obtention du grade de
DOCTEUR DE L'UNIVERSITÉ DE POITIERS
Institut d'administration des entreprises (Poitiers)
Centre de recherche en gestion
(Diplôme National - Arrêté du 25 mai 2016)

École doctorale : Sciences de la Société, Territoires, Sciences Économiques et de Gestion (Limoges)
Secteur de recherche : Sciences de gestion

Présentée par :
Jean-Jacques YAMMINE

LE ROLE DE L'AUDIT INTERNE DANS LA CYBERSECURITE D'ETABLISSEMENTS BANCAIRES : UNE COLLABORATION INTERPROFESSIONNELLE AU PRISME DES IDENTITES PROFESSIONNELLES

Directeur(s) de Thèse :
MERIC Jérôme

Soutenue le 20 décembre 2024 devant le jury

Jury :

Président	**Stéphane Bellini**	Professeur - Université de Poitiers
Co-directeur	**Nicolas Moinet**	Professeur - Université de Poitiers
Rapporteur	**Christophe Assens**	Maître de Conférences HDR – Université de Saint Quentin en Yvelines -
Rapporteur	**Amaury Grimand**	Professeur – Université de Nantes
Membre	**Julie Demaret**	Maître de Conférences HDR – Université Paris 1 Sorbonne

Pour citer cette thèse :
Jean-Jacques YAMMINE. *Le rôle de l'audit interne dans la cybersécurité d'établissements bancaires : Une collaboration interprofessionnelle aux prismes des identités professionnelles* [En ligne]. Thèse Sciences de gestion. Poitiers : Université de Poitiers, 2023. Disponible sur Internet <http://theses.univ-poitiers.fr>

UNIVERSITE DE POITIERS

ÉCOLE DOCTORALE – Société, Territoires, Sciences Économiques et de Gestion – n°613

LABORATOIRE CEREGE, UR13564

LE ROLE DE L'AUDIT INTERNE DANS LA CYBERSECURITE BANCAIRE :

Une collaboration interprofessionnelle aux prismes des identités professionnelles

---

Thèse pour l'obtention du titre de Docteur en Sciences de Gestion

Présentée et soutenue publiquement le 20/12/2024 par

Jean-Jacques YAMMINE

Sous la direction de :

Monsieur Jérôme Méric, Professeur des universités, Université de Poitiers

Monsieur Nicolas Moinet, Professeur des universités, Université de Poitiers

Rapporteurs :

Monsieur Amaury Grimand, Professeur des universités, Université de Nantes

Monsieur Christophe Assens, Maître de Conférences HDR, Université de Saint Quentin en Yvelines

Suffragants :

Monsieur Stéphane Bellini, Professeur des universités, Université de Poitiers

Madame Julie Demaret, Maître de Conférences HDR, Université Paris 1 Sorbonne

« L'université de Poitiers n'entend donner aucune approbation ni improbation aux opinions émises dans les thèses ; elles doivent être considérées comme propres à leurs auteurs. »

Remerciements

La réalisation de cette thèse n'aurait jamais été possible sans le soutien inébranlable et l'aide précieuse de plusieurs personnes, à qui j'aimerais exprimer ma plus profonde gratitude. C'est un exercice tout particulier que celui de rédiger des remerciements à la personne qui a permis, de par son soutien scientifique, de concrétiser mon projet de thèse en un travail rigoureux, dense mais ô combien passionnant. Je choisis de me dégager d'un conformisme attendu tant cette rencontre recouvre une valeur inestimable à mes yeux. **Jérôme Méric** a porté une vigilance particulière à ma démarche, me guidant dans mes choix méthodologiques, m'ouvrant de nouvelles perspectives analytiques dans un secteur complexe et innovant, me dirigeant dans la restructuration de mes écrits … Monsieur Méric, je vous prie de trouver ici toute ma reconnaissance et ma gratitude pour votre humanité, votre disponibilité et votre simplicité : la richesse de votre accompagnement a participé à la formation du scientifique que je suis mais également de l'homme qui aujourd'hui accompagne à son tour d'autres personnes. Vous avez cru en moi, vous faites partie des très rares personnes à avoir incarné la solidarité humaniste après l'explosion du port de Beyrouth en 2020. Vous avez œuvré à ma venue en France et avez accepté de cheminer à mes côtés malgré les difficultés rencontrées de par ma situation administrative. Grâce à vous, je suis non seulement en phase de devenir docteur mais suis aujourd'hui en mesure d'offrir une vie meilleure à ma petite famille, Sally et Rita. Vous incarnez à mon sens la fameuse expression qui aujourd'hui est mise à mal « France, terre d'accueil ». *Choukrane Djazilane, ytawel omrak.* Merci infiniment, longue vie à vous.

Je tiens également à exprimer ma reconnaissance à Monsieur **Nicolas Moinet**, mon co-directeur de thèse, dont l'expertise et les conseils avisés ont grandement enrichi ce travail. Ses remarques pertinentes, en particulier sur les aspects liés à la cybersécurité, m'ont permis d'approfondir des thématiques essentielles dans ce domaine complexe et en constante évolution. Grâce à son vaste savoir en sciences de l'information et à sa compréhension fine des enjeux de la cybersécurité, il a su orienter mes recherches avec rigueur et m'ouvrir à de nouvelles perspectives analytiques. Je lui suis extrêmement reconnaissant pour son accompagnement précieux et son engagement tout au long de ce parcours.

Je souhaite exprimer ma reconnaissance aux membres du jury, dont les observations et le regard critique ont enrichi ce travail de manière significative. Leurs questions et commentaires avisés ont permis de renforcer la rigueur scientifique de cette recherche, et je leur suis reconnaissant d'avoir consacré leur temps et leurs efforts à l'examen de mon travail.

Je tiens à remercier du fond du cœur mon épouse, **Sally Matrak**, dont le soutien indéfectible et l'amour inconditionnel ont été des piliers tout au long de cette aventure. Elle a été à mes côtés à chaque étape, m'encourageant dans les moments difficiles et célébrant chaque petite victoire avec moi. Son soutien a été bien plus qu'une simple présence ; il a été la lumière qui m'a guidé à travers ce long chemin.

Je voudrais également exprimer ma reconnaissance infinie à mes parents, **mon père et ma mère**, qui m'ont toujours soutenu avec amour et générosité. Sans leur éducation, leurs sacrifices, et leur croyance inébranlable en mes capacités, je n'aurais jamais pu parvenir à la réalisation de cette thèse. Ils m'ont enseigné la valeur du travail, de la persévérance et de la détermination, des qualités qui m'ont accompagné tout au long de ce parcours.

Un merci particulier à mon oncle, Dr **Fady Fenianos**, qui m'a constamment rappelé l'importance de mener à bien une thèse doctorale. Son expérience, ses conseils éclairés, et sa conviction dans le fait que je pouvais atteindre cet objectif ont joué un rôle décisif dans ma persévérance à chaque étape de cette aventure académique.

Un remerciement spécial à Monseigneur **Estephan Frangieh**, Président du Club de football Salam Zgharta, dont l'aide financière durant les trois premières années de mes recherches a été essentielle. Son soutien généreux a permis à ce projet de prendre son envol, et sans cette aide cruciale, je n'aurais pas pu mener à bien ces premières étapes de manière aussi sereine.

Je tiens à remercier chaleureusement Monsieur **Antonio Khawaja**, Directeur des Ressources Humaines à l'hôpital Notre Dame de Zgharta, qui a joué un rôle fondamental au tout début de cette aventure. En me proposant une alternative afin de trouver une université ainsi qu'un directeur de thèse, il a ouvert la porte à cette incroyable opportunité de réaliser un doctorat. Son soutien et ses efforts pour me guider vers le bon chemin ont été déterminants pour la suite de mon parcours.

À toutes ces personnes, ainsi qu'à tous ceux qui m'ont encouragé, soutenu, et inspiré de près ou de loin au cours de ces dernières années, je tiens à exprimer ma plus sincère reconnaissance. Merci de m'avoir permis de concrétiser ce projet qui me tenait tant à cœur.

Sommaire général

INTRODUCTION GENERALE

Introduction générale

La transformation numérique rapide et continue a engendré des avantages sans précédent, notamment en améliorant l'efficacité opérationnelle et la connectivité à l'échelle mondiale. Cependant, elle a également amplifié les risques en matière de sécurité des informations, particulièrement dans les secteurs sensibles comme le secteur bancaire. La numérisation massive des transactions financières, la dématérialisation des services et l'interconnectivité des systèmes ont exposé les banques à des cybermenaces croissantes et diversifiées. De fait, la cybersécurité est devenue une problématique centrale dans les banques, en raison de la nature critique des informations financières qu'elles gèrent et de l'importance systémique de ces institutions pour l'économie mondiale (PWC, 2021).

Les attaques informatiques contre les banques se sont intensifiées au cours des dernières années, tant en fréquence qu'en sophistication. Les cybercriminels exploitent de plus en plus les vulnérabilités des systèmes bancaires pour accéder à des données sensibles, telles que les informations financières des clients, ou pour provoquer des perturbations dans les services financiers. Par exemple, l'attaque contre la banque Capital One en 2019, où les informations personnelles de plus de 100 millions de clients ont été exposées, démontre l'ampleur des cybermenaces auxquelles les banques sont confrontées (Wang, 2020). De même, l'attaque massive subie par le Crédit Agricole en 2021 montre que même les plus grandes institutions financières ne sont pas à l'abri de telles menaces (KPMG, 2021). Ces événements témoignent de la nécessité pressante pour les institutions bancaires de renforcer leurs dispositifs de cybersécurité.

Pour faire face à ces risques, les banques doivent mettre en place des stratégies de cybersécurité robustes, basées sur une gestion proactive des risques, l'adoption de technologies de protection avancées, et une sensibilisation accrue de leur personnel (Deloitte, 2023). L'évolution des régulations, telles que la directive européenne NIS2 ou le cadre du GDPR, impose également aux institutions financières de renforcer leurs protocoles de protection des données et de se conformer à des normes de sécurité plus strictes. Par conséquent, une approche holistique intégrant des mesures techniques, organisationnelles et réglementaires s'avère cruciale pour contrer les menaces cybernétiques dans le secteur bancaire (Forum, 2023).

Les banques sont parmi les cibles les plus fréquentes des cyberattaques, en raison de la richesse des informations sensibles qu'elles traitent, telles que les données financières et les informations personnelles de leurs clients. Selon un rapport récent de l'Agence européenne pour la cybersécurité ENISA, les menaces contre le secteur financier ont augmenté de manière

exponentielle au cours des dernières années, et les banques continuent d'être des cibles de choix pour les cybercriminels (ENISA, 2023). Parmi les principales menaces, on retrouve les ransomwares, les attaques par déni de service distribué (DDoS), le phishing ciblé, ainsi que l'exploitation des vulnérabilités zero-day. Ces formes d'attaques permettent aux cybercriminels de contourner les défenses traditionnelles des institutions financières, rendant les systèmes bancaires de plus en plus vulnérables (Kumar, 2021).

Les ransomwares, par exemple, sont devenus l'une des menaces les plus dévastatrices pour le secteur bancaire, causant des interruptions prolongées des services et entraînant des pertes financières significatives. Une étude réalisée par IBM a révélé que les attaques de ransomware dans le secteur financier ont augmenté de 238 % entre 2020 et 2022, en raison de la sophistication accrue des techniques d'attaque et de l'utilisation croissante de la double extorsion, où les attaquants non seulement chiffrent les données mais menacent de les divulguer si la rançon n'est pas payée (Security, 2022). Les attaques par DDoS, quant à elles, visent à rendre les systèmes indisponibles, perturbant les transactions financières et affectant la confiance des clients envers les services bancaires en ligne (Radziwill, 2021).

En parallèle, les tensions géopolitiques exacerbent ces risques cybernétiques, les cyberattaques étant de plus en plus utilisées comme outils de guerre économique ou politique. Par exemple, l'attaque notoire de 2017 contre des banques ukrainiennes, attribuée à des acteurs soutenus par l'État russe via le malware NotPetya, a non seulement perturbé les systèmes financiers mais a également mis en évidence l'utilisation stratégique des cyberattaques à des fins géopolitiques (Greenberg, 2019). Selon une analyse du Journal of Strategic Studies, ce type d'attaques démontre comment des États-nations peuvent cibler des infrastructures financières critiques pour déstabiliser leurs adversaires, illustrant ainsi l'interconnexion croissante entre la cybersécurité et les enjeux géopolitiques (Healey, 2020).

Les cyberattaques dans le secteur bancaire ont des conséquences qui vont bien au-delà des pertes financières immédiates. Elles compromettent également la confiance des clients dans les institutions financières, ce qui peut avoir des répercussions à long terme sur leur réputation et leur rentabilité. Une étude publiée dans le Journal of Banking and Finance montre que les institutions financières qui subissent des cyberattaques importantes voient leur capitalisation boursière chuter en moyenne de 5 à 7 % dans les semaines suivant une attaque, en raison des inquiétudes des investisseurs quant à la sécurité des données et à la stabilité de l'infrastructure (Kovacevic, 2021). Cela souligne l'urgence pour les banques d'adopter des mesures de cybersécurité robustes et de s'assurer que les systèmes d'information soient capables de résister

à des attaques de plus en plus sophistiquées.

Dans le contexte actuel de la cybersécurité, plusieurs auteurs s'accordent sur le fait que la sécurité de l'information ne peut plus être perçue simplement comme une question technique. Elle relève désormais d'une approche organisationnelle et systémique. En effet, selon Von Solms et Van Niekerk (Von Solms, 2013), les menaces cybernétiques ne concernent pas uniquement les infrastructures technologiques, mais elles impliquent également des dimensions humaines, culturelles, et organisationnelles. Cette approche élargie exige donc la mobilisation d'une diversité d'acteurs, dont les rôles et responsabilités sont distincts mais complémentaires, afin de garantir une réponse cohérente et efficace aux risques liés à la cybersécurité (Von Solms, 2013).

La gestion des risques cyber ne se limite plus à la responsabilité exclusive des départements de sécurité informatique, mais s'étend aux autres fonctions telles que la direction de l'audit interne, la gestion des risques, et la conformité. Dhillon & Backhouse (Dhillon, 2000) ont souligné que la sécurité de l'information exige une coordination interprofessionnelle, qui ne se limite pas à la mobilisation des spécialistes techniques, mais implique également les cadres ayant une compréhension globale des processus organisationnels. Cette approche systémique nécessite que ces différentes fonctions collaborent étroitement pour identifier, évaluer, et atténuer les risques cyber, tout en assurant la conformité aux normes réglementaires en constante évolution (Siponen, 2022).

Les Responsables de la Sécurité des Systèmes d'Information (RSSI) et les auditeurs internes jouent un rôle central dans la gestion de la cybersécurité au sein des banques. Le RSSI a pour mission de développer, implémenter et maintenir les dispositifs techniques de sécurité, tels que les systèmes de détection d'intrusion, le chiffrement des données, et la gestion des accès (Puhakainen, 2010). En parallèle, les auditeurs internes sont chargés d'évaluer l'efficacité des contrôles internes, de vérifier la conformité avec les normes de sécurité et de s'assurer que les risques sont correctement gérés (ISACA, 2021). Cette dynamique renforce la nécessité d'une coordination fluide entre les départements techniques et les fonctions d'audit, afin d'assurer une réponse intégrée aux cybermenaces (Soomro, 2016).

Cependant, malgré l'importance cruciale de cette coopération, de nombreux auteurs ont observé des difficultés dans la collaboration entre le RSSI et les auditeurs internes. Willcocks et Margetts (Willcocks, 2019) notent que ces deux groupes professionnels ont souvent des identités professionnelles, des objectifs et des méthodes de travail divergents. Les RSSI, qui viennent généralement de milieux techniques, se concentrent sur la mise en place de solutions

concrètes pour prévenir et atténuer les cybermenaces, tandis que les auditeurs internes adoptent une approche plus analytique et centrée sur la conformité, cherchant à identifier les écarts par rapport aux normes et procédures établies. Cette divergence peut mener à des tensions, notamment en ce qui concerne les priorités et les méthodes de travail, rendant la collaboration parfois complexe.

Pour surmonter ces obstacles, il est essentiel de promouvoir une culture de collaboration au sein des institutions financières, où les différents acteurs de la cybersécurité travaillent de manière transversale, avec une vision partagée des risques. L'implication des dirigeants est cruciale pour faciliter cette coopération, en créant des mécanismes de communication et de prise de décision qui favorisent une approche intégrée (Tounsi, 2018). Des initiatives telles que des comités de gestion des risques cyber, où siègent à la fois les RSSI, les auditeurs internes et d'autres parties prenantes clés, peuvent aider à renforcer cette synergie et à garantir une réponse cohérente aux cybermenaces.

De plus, la mise en œuvre de cadres tels que l'ISO 27001, qui promeut une approche holistique de la gestion de la sécurité de l'information, peut également contribuer à formaliser cette collaboration interprofessionnelle. Ces cadres établissent des lignes directrices claires sur la manière dont les différentes fonctions au sein de l'organisation doivent travailler ensemble pour identifier, traiter et surveiller les risques cybernétiques (Haque, 2020). En conséquence, ils jouent un rôle central dans la promotion d'une culture organisationnelle où la cybersécurité est perçue comme une responsabilité partagée, et non l'apanage d'une seule fonction.

L'enjeu principal de cette recherche réside donc dans l'analyse de la manière dont les identités professionnelles distinctes des RSSI et des auditeurs internes influencent l'organisation de la réponse aux risques cyber dans les banques. La gestion des risques met en avant deux métiers distincts, avec des responsabilités qui peuvent parfois se chevaucher et conduire à des conflits de juridiction. Face à ces tensions potentielles, la question centrale qui se pose est la suivante : **quelle est l'interaction des identités professionnelles et de l'organisation de la réponse aux risques cyber dans les banques ?**

Pour répondre à cette question, il est essentiel de traiter plusieurs sous-questions de recherche :

- Comment caractériser les identités professionnelles des auditeurs internes et des RSSI ?
- Quelle est la nature des interactions entre ces acteurs dans la gestion des risques cyber ?
- Quel est l'impact de ces interactions sur la qualité des réponses aux risques cyber ?

Ces questions permettront de comprendre plus finement la dynamique de collaboration, ou de conflit, entre ces deux professions et d'évaluer comment ces interactions influencent la capacité des banques à gérer efficacement les risques liés à la cybersécurité.

Nous avons choisi d'étudier la cybersécurité dans les banques à travers l'examen des identités professionnelles des auditeurs internes et des RSSI. La cybersécurité englobe une multitude de professionnels aux compétences diverses travaillant ensemble pour atteindre un objectif commun : la protection des systèmes et des données informatiques. Ces professionnels peuvent inclure des experts en sécurité de l'information, des administrateurs réseau, des développeurs de logiciels, des ingénieurs en informatique, des avocats spécialisés en cybersécurité, des responsables de la conformité réglementaire et des professionnels des relations publiques, entre autres.

Chacune de ces professions possède une identité professionnelle distincte, qui comprend des connaissances, des compétences, des normes de conduite et des codes de déontologie spécifiques. Ces identités professionnelles peuvent parfois entrer en conflit les unes avec les autres, ce qui peut créer des défis pour la collaboration efficace et la communication dans le cadre de l'action cybersécurité, ce qui aboutit à des problèmes de juridiction. Par exemple, les avocats spécialisés en cybersécurité peuvent se concentrer sur les implications juridiques et réglementaires de la cybersécurité, tandis que les experts en sécurité de l'information peuvent se concentrer sur les aspects techniques et pratiques de la cybersécurité.

Les différences entre les identités professionnelles peuvent également entraîner des divergences sur la manière de gérer les incidents de sécurité, de prioriser les menaces et les vulnérabilités, ainsi que de mettre en place des stratégies et des politiques de cybersécurité. En outre, les identités professionnelles peuvent être réglementées par différents organismes de réglementation, ce qui peut entraîner des contraintes de juridiction entre les professions. Par exemple, les avocats spécialisés en cybersécurité peuvent avoir des pratiques nommées par les barreaux d'avocats, tandis que les experts en sécurité de l'information peuvent être réglementés par des organismes professionnels de la sécurité de l'information.

Comprendre les identités professionnelles des différentes professions impliquées dans la cybersécurité est donc essentiel pour favoriser une collaboration efficace et une communication claire et cohérente entre les professionnels impliqués. Cela permettra également de surmonter les contraintes de juridiction et de développer des approches intégrées pour la protection des systèmes et des données informatiques.

Le sujet des identités professionnelles est pertinent pour comprendre la manière dont se structure la cybersécurité et les contraintes de juridiction entre les professions d'audit interne et d'informatique pour plusieurs raisons. Tout d'abord, les identités professionnelles définissent les rôles, les responsabilités et les compétences des différents acteurs impliqués dans la cybersécurité. Par exemple, les auditeurs internes et les RSSI ont des responsabilités distinctes en matière de cybersécurité, avec des compétences et des connaissances spécifiques à leur domaine d'expertise. Comprendre les identités professionnelles de chacun de ces acteurs permet de mieux comprendre leurs rôles et responsabilités respectifs, et comment ils collaborent pour assurer la sécurité des systèmes d'information dans le secteur bancaire.

En outre, les identités professionnelles peuvent également jouer un rôle dans la définition des règles de gouvernance et des normes de cybersécurité. À la BPVF, nous avons observé que les auditeurs internes ont été impliqués dans l'élaboration de politiques de sécurité et à travers leur audit interne sur le département informatique, ils ont recommandé l'embauche d'un deuxième RSSI, tandis que les professionnels de l'informatique sont souvent chargés de mettre en œuvre ces politiques. En abordant les identités professionnelles des différents acteurs, il est possible de mieux comprendre comment les politiques et les normes de sécurité sont élaborées et mises en œuvre.

Les identités professionnelles peuvent avoir un impact sur les contraintes de juridiction entre les professions d'audit interne et d'informatique. Dans les banques libanaises et la BPVF, nous avons remarqué qu'il peut y avoir des conflits entre les professionnels de l'audit interne et de l'informatique sur la question pour savoir qui est responsable de la cybersécurité et de la gestion des risques. En abordant chaque groupe sous l'angle de son identité professionnelle, nous avons mieux compris ces conflits et comment nous pouvons proposer de trouver des moyens de résolution.

La compréhension des identités professionnelles est essentielle pour comprendre la manière dont se structure la cybersécurité et les contraintes de juridiction entre les professions d'audit interne et d'informatique. En comprenant les rôles, les responsabilités et les compétences de chaque groupe, il est possible de mieux comprendre comment ils collaborent pour assurer la sécurité des systèmes d'information, comment les politiques et les normes de sécurité sont élaborées et mises en œuvre, et comment résoudre les conflits entre les groupes.

Les auditeurs internes et les RSSI sont des professionnels clés de la cybersécurité bancaire, chacun ayant un rôle important à jouer dans la protection des systèmes d'information et des données sensibles de l'entreprise. Cependant, en raison de leurs responsabilités distinctes, ils

possèdent des divergences dans leurs identités professionnelles qui ont abouti à un problème de juridiction sur l'assurance de la cybersécurité bancaire.

La présente recherche s'appuie sur une revue de littérature en deux parties distinctes :

- Chapitre 1 : cybersécurité et acteurs de la gestion des risques. Ce chapitre abordera les principales menaces auxquelles les banques sont confrontées et les rôles joués par les différents acteurs dans la prévention et la gestion de ces risques. Une attention particulière sera portée sur le rôle des RSSI et des auditeurs internes, en lien avec les cadres théoriques de la gestion des risques cyber (PWC, 2022 ; ENISA, 2023).

- Chapitre 2 : identités professionnelles et cadre d'analyse. Dans ce chapitre, nous explorerons la notion d'identité professionnelle, un concept central pour comprendre les interactions entre les différents acteurs de la cybersécurité bancaire. La littérature sur les identités professionnelles (Sainsaulieu, 1977 ; Dubar, 2010) sera mobilisée pour construire un cadre d'analyse permettant d'examiner les spécificités des identités des RSSI et des auditeurs internes. Ce cadre nous aidera à comprendre comment ces identités influencent la gestion des risques cyber au sein des banques, et notamment les conflits de juridiction.

- Chapitre 3 : cadre méthodologique et design de recherche. Ce chapitre explore le rôle primordial de l'audit interne dans la cybersécurité bancaire en adoptant une approche méthodologique rigoureuse et comparative. À travers une analyse théorique et empirique, il met en lumière les interactions entre les auditeurs internes et les responsables de la sécurité des systèmes d'information (RSSI), en tenant compte des spécificités du secteur bancaire en France et au Liban. L'analyse comparative inter-cas, basée sur des entretiens et un processus de codage approfondi, révèle des différences contextuelles significatives dans les pratiques de cybersécurité et les identités professionnelles. Ces résultats permettent de formuler des recommandations adaptées à chaque environnement, contribuant ainsi à une meilleure compréhension des enjeux de cybersécurité bancaire.

- Chapitre 4 : résultats de la recherche : contexte organisationnel et construction identitaire. Ce chapitre 4 présente les résultats de l'étude sur la cybersécurité à la BPVF, en se concentrant sur les identités professionnelles des auditeurs internes et des responsables de la sécurité des systèmes d'information (RSSI). Il révèle l'importance des compétences techniques en cybersécurité et les tensions entre les auditeurs internes, en

tant que contrôleurs, et les RSSI, qui malgré leurs limitations techniques, jouent un rôle central dans la gestion de la sécurité. L'analyse met également en évidence l'impact de la structure organisationnelle et des contraintes budgétaires sur la gestion de la cybersécurité, notamment à travers l'externalisation de certaines fonctions.

- Chapitre 5 : présentation des résultats : l'identité affecte la gestion du risque cyber. Ce chapitre présente une analyse approfondie des enjeux, pratiques et résultats liés à la cybersécurité dans le secteur bancaire français et libanais. Il souligne l'importance croissante de la cybersécurité dans un contexte de numérisation des services financiers et examine les stratégies variées mises en œuvre pour gérer les risques, de l'audit interne aux normes de sécurité. L'étude révèle des différences marquées dans les rôles et perceptions des acteurs clés, comme les auditeurs internes et les RSSI, selon les contextes nationaux, tout en identifiant des points communs, notamment la nécessité d'améliorer l'expertise et la collaboration en cybersécurité.

- Chapitre 6 : discussion et propos conclusif. Ce chapitre analyse la cybersécurité dans le secteur bancaire en mettant l'accent sur l'influence des identités professionnelles des auditeurs internes et des RSSI. La première partie explore comment ces identités façonnent la gestion de la sécurité informatique, avec des différences notables entre les contextes français et libanais, soulignant la nécessité d'une approche plus coordonnée, notamment au Liban. La seconde partie examine les défis actuels de la cybersécurité bancaire, révélant son importance stratégique croissante et le rôle central des RSSI dans l'élaboration des stratégies de sécurité. Ce chapitre souligne ainsi l'évolution de la cybersécurité, devenue un enjeu stratégique nécessitant une collaboration accrue et des compétences diversifiées.

Nous présentons à travers la figure 1 ci-dessous le design de la recherche à travers lequel nous pouvons observer clairement la représentation schématique de la structure de la thèse.

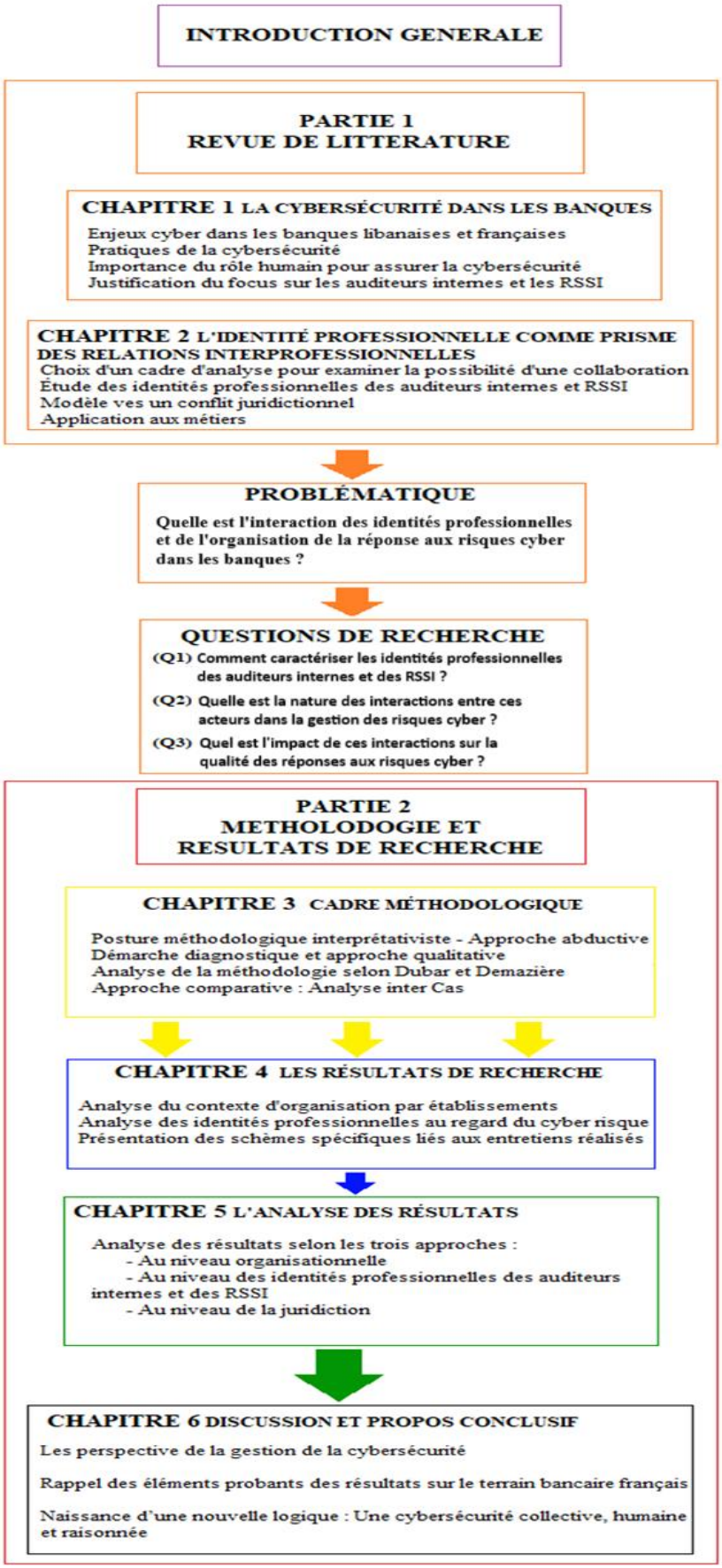


Figure 1 : design de Recherche - Représentation schématique de la structure de thèse

PARTIE 1.

REVUE DE LITTERATURE

CHAPITRE 1.

ENJEUX, DEFIS ET COOPERATION INTERPROFESSIONNELLE DANS LA CYBERSECURITE BANCAIRE

Sommaire du chapitre 1. Enjeux, défis et coopération interprofessionnelle dans la cybersécurité bancaire

1. Enjeux, défis et coopération interprofessionnelle dans la cybersécurité bancaire

Le chapitre 1 souligne que la cybersécurité va bien au-delà de la simple technologie. Elle est également étroitement liée aux aspects humains et organisationnels. La cybersécurité est essentielle, en particulier dans le secteur bancaire, où les risques financiers et de réputation sont énormes. Les banques doivent investir massivement dans la protection de leurs systèmes informatiques et de leurs données tout en garantissant des responsabilités claires au sein de l'organisation.

Ce chapitre permet de positionner la cybersécurité comme un défi en constante évolution qui nécessite une technologie avancée, des ressources humaines qualifiées et une collaboration étroite entre les différentes parties prenantes.

1.1 Comment cerner la cybersécurité ?

La partie 1.1 explore les fondements de la cybersécurité à travers son historique, son étymologie et sa définition actuelle, en examinant ensuite son positionnement dans le cadre de la gestion des risques informatiques, avant de conclure sur les principaux défis technologiques, humains et organisationnels qu'elle implique.

1.1.1 Historique et étymologie

La cybersécurité couvre un large éventail de pratiques, d'outils et de concepts, souvent associés à la sécurité de l'information et à la technologie opérationnelle. Ce domaine se distingue par l'intégration d'aspects défensifs et parfois offensifs, tels que l'utilisation de la technologie pour contrer des adversaires. En général, la cybersécurité est souvent perçue comme une réponse aux logiciels malveillants et aux cyberattaques (Galinec, 2017).

Bay (2016) souligne la complexité de ce concept à multiples facettes, nécessitant une distinction claire entre la sécurité informatique et celle de l'information.

Le terme « sécurité », aux nombreuses acceptions, reflète la complexité de la cybersécurité. Utilisé par des acteurs variés tels que des politiciens, des informaticiens, des entrepreneurs et des agents de sécurité nationale, il est interprété différemment selon le contexte. Au niveau institutionnel, il s'agit de protéger le public et les infrastructures des menaces du cyberespace, tandis qu'au niveau individuel, il concerne la protection des appareils contre les virus et autres attaques. Pour mieux comprendre ce domaine, il est utile de décomposer le mot cybersécurité en ses deux éléments : « cyber » et « sécurité » (Bay, 2016).

Historiquement, le préfixe « cyber » renvoie au concept de cyberespace, défini par les réseaux de communication et la réalité virtuelle. Le terme est issu de « cybernétique », un mot introduit par Norbert Wiener en 1948 pour désigner la communication et le contrôle dans les systèmes machines et biologiques (Dupuy, 1994). Plus tard, « cyberspace » fut popularisé par William Gibson dans son roman *Neuromancer* (1984), où il décrit un espace virtuel tridimensionnel de flux d'information (Craigen, 2014). Selon Lévy (1997), le cyberespace représente un lieu d'échanges et de conflits, une nouvelle frontière économique et culturelle, symbolisant les réseaux numériques.

Avec l'émergence de la société de l'information à la fin du XX^{e} siècle, le terme « cyber » a été associé à de nombreux concepts liés aux réseaux et à la sécurité, tels que cybercriminalité, cyberattaque ou cyberespace. Arpagian (2015) relie la cybersécurité à la gestion des conflits dans le cyberespace, y compris la cyberguerre et le cyber-terrorisme. Il distingue deux niveaux d'attaque : d'abord, les réseaux informatiques, téléphoniques ou satellitaires peuvent être infiltrés, altérés ou suspendus. Ensuite, les contenus numériques, tels que les bases de données ou les communications, peuvent être ciblés.

Cavetly (2010) définit le cyberespace comme un écosystème virtuel, distinct du monde physique, mais reliant des fils, câbles et ondes qui transportent l'information. Elle précise que la cybersécurité vise à protéger cet environnement bioélectronique, ainsi que les appareils et données qui y circulent.

Concernant le terme « sécurité », il n'existe pas de définition universelle. Selon le dictionnaire Oxford (2014), la sécurité est un état de protection contre les menaces. Ainsi, la cybersécurité peut être vue comme l'ensemble des lois, politiques, outils et technologies utilisés pour protéger les systèmes informatiques et les données contre diverses menaces, que ce soit pour les États, les entreprises ou les individus.

La cybersécurité est devenue une priorité stratégique à l'échelle mondiale. Le président Obama, dans un discours à la Maison-Blanche en 2009, a affirmé que la prospérité des États-Unis dépendrait de la cybersécurité, soulignant que sa protection relève d'une responsabilité partagée entre les gouvernements et les secteurs privés. En France, le Premier ministre Ayrault a également insisté en 2014 sur son importance nationale, évoquant un enjeu de sécurité pour tous les citoyens. (The white house, 2015)

En France, le premier ministre Ayrault, déclarait le 21 février 2014 : *« la cybersécurité est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement »* (Chava, 2014)

Sous la présidence de Donald Trump, la cybersécurité a également été mise en avant avec des

mesures visant à renforcer les dispositifs aux niveaux gouvernemental et privé, notamment via le SHIELD Act en 2017, destiné à protéger l'État de New York contre les cybermenaces. De plus en plus intégrée aux politiques publiques, la cybersécurité couvre un large éventail de domaines, allant de la formation militaire à la gestion des données personnelles dans l'ère du big data (Kulesza, 2018). Elle désigne les mesures prises pour sécuriser les communications, les ressources en ligne et les infrastructures critiques, tout en protégeant la vie privée et les informations sensibles.

1.1.2 Définition de la cybersécurité

La cybersécurité, bien que souvent perçue comme un domaine technique, possède une dimension multidimensionnelle qui va au-delà de la simple protection des systèmes informatiques contre les cybermenaces. Pour éclaircir ce concept, nous avons élaboré un tableau qui classe les diverses définitions de la cybersécurité selon leurs similarités et leurs différences contextuelles.

Tableau 1 : les perspectives de la définition de la cybersécurité

Perspectives		**Auteurs**		
Prévention avant tout	L'organisation internationale de normalisation (ISO) 27032	Bayuk et Healey	Homeland département de la cybersécurité	L’agence de sécurité nationale (NSA)
Divergences sur la manière dont elle est conçue	Touhill, Asher et Gonzalez	Kaplan, Kramer	Anderson, Wamala et Leclair	Grady et Parisi
Protections contre les attaques et les cybermenaces	Refsdal, Solhaug et Stolen	Lehto et Neittaanmäki	Carr, Hatleback	UIT, Conseil national de recherche
Sans Aborder le contexte	Benkler	Stratégie de la cybersécurité de la Finlande	Comité de professionnalisation de la main d’œuvre	

Plusieurs définitions soulignent son caractère préventif et sa nécessité d'intégration dans la gestion des risques au sein des organisations. Par exemple, une définition du droit militaire fédéral inclut la sécurité des ordinateurs, des réseaux et de toute autre technologie d'information, tandis que l’Agence de sécurité nationale (NSA) met l'accent sur des mesures visant à garantir la disponibilité, l'intégrité, l'authenticité, la confidentialité et la non-

répudiation des systèmes d'information. Les travaux de chercheurs tels que Fisher (2009) articulent la cybersécurité autour de trois axes : un ensemble d'activités et de mesures de protection, un état de protection contre les menaces, et un domaine d'activité visant à améliorer ces mesures. L'organisation internationale de normalisation (ISO) 27032 définit également la cybersécurité comme la préservation des propriétés fondamentales des informations dans le cyberespace (Vaseashta, 2014).

D'autres comme Refsdal, Solhaug et Stolen (2015) mettent l'accent sur la cybersécurité en tant que protection contre les cybermenaces tandis que Hatleback (2018) aborde la défense des actifs technologiques contre des tentatives d'intrusion. La gestion des risques, l'identification des vulnérabilités et l'amélioration de la résilience des systèmes sont également des éléments clés, comme le soulignent Lehto et Neittaanmäki (2015).

La cybersécurité est perçue comme un défi national majeur, abordé par des acteurs tels que l'union internationale des télécommunications (UIT), qui la décrit comme un ensemble de mesures de protection des environnements numériques. La question de la cybersécurité est ainsi liée à des enjeux de sécurité nationale, de politique publique et de protection des infrastructures critiques (UIT, 2023).

Une dimension supplémentaire est apportée par des auteurs comme Anderson (2012), qui considèrent la cybersécurité comme un défi évolutif, nécessitant une adaptation constante aux nouvelles menaces. Cela souligne l'importance d'une approche proactive, impliquant non seulement des technologies de défense, mais aussi des stratégies de gouvernance et d'éducation des utilisateurs.

En conclusion, la cybersécurité ne se limite pas aux technologies de l'information ; elle est un enjeu organisationnel qui requiert une approche interdisciplinaire intégrant l'humain, la technologie et les structures organisationnelles. Les entreprises doivent donc adopter des stratégies de cybersécurité qui reconnaissent cette complexité et mettent l'accent sur une gouvernance efficace, afin de garantir la protection de leurs actifs contre une multitude de menaces dans un environnement numérique en constante évolution.

1.1.3 Positionnement de la cybersécurité

La cybersécurité se concentre généralement sur la protection des actifs informationnels et des infrastructures. Pour mieux définir ce champ d'action, il est essentiel de délimiter ses frontières par rapport à des concepts connexes tels que le cyberspace, les cyberattaques, la cybercriminalité, la cyberguerre et la sécurité de l'information. Cette clarification permet d'éviter des confusions et de préciser la place de la cybersécurité dans cet ensemble.

1.1.3.1 Cybersécurité et cyberespace

Le cyberespace a profondément transformé nos modes de communication, facilitant les interactions entre individus, entreprises et gouvernements tout en rendant la notion de fuseau horaire presque obsolète. Cependant, il n'existe pas de définition universelle du cyberespace, chaque gouvernement ayant sa propre interprétation. Pour mieux cerner ce concept, nous le classons en trois dimensions : matérielle, connectique et de données.

La dimension matérielle englobe les éléments tangibles du cyberespace, tels que les ordinateurs, les appareils mobiles, les serveurs et les infrastructures de communication. Bien que le cyberespace lui-même soit neutre, son utilisation peut avoir des conséquences néfastes, comme en témoigne l'augmentation des cyberattaques ciblant des infrastructures critiques. Ces menaces soulignent la nécessité d'une cybersécurité proactive, visant à réduire le risque de cyberattaques réussies (Hammond, 2016).

La dimension connectique, selon l'UIT, se réfère aux systèmes et services interconnectés à Internet et aux réseaux informatiques (Wamala, 2011). L'organisation internationale de normalisation (ISO/IEC 27032) définit le cyberespace comme l'environnement résultant de l'interaction entre personnes, logiciels et services via des dispositifs technologiques, sans référence explicite à l'infrastructure physique (ISO/IEC, 2012).

Enfin, la dimension des données considère le cyberespace comme un système global d'information interconnectée, regroupant les infrastructures informatiques, Internet et les systèmes embarqués (Kuehl, 2009). Le Pentagone définit également le cyberespace comme un domaine global d'interconnexion des technologies de l'information (Castelli, 2008).

Ainsi, nous proposons une définition globale : le cyberespace est un domaine dynamique caractérisé par l'utilisation d'électrons et de spectres électromagnétiques pour créer, stocker, modifier et partager des informations. Cela inclut les infrastructures physiques de télécommunication, les systèmes informatiques et les données associées (Mayer, 2013).

Avec l'évolution technologique, le cyberespace se transforme rapidement, ce qui, bien que favorable à l'efficacité opérationnelle, expose également les utilisateurs à de nouveaux risques de sécurité. Les avancées en automatisation et en intelligence artificielle, par exemple, peuvent renforcer les capacités de communication tout en rendant les systèmes plus vulnérables aux cyberintrusions (Bochman, 2019).

La dépendance croissante aux technologies numériques rend impératif un renforcement de la cybersécurité. Alors que les entreprises adoptent des systèmes interconnectés pour optimiser leur efficacité, elles s'exposent également à une multitude de cybermenaces. Un développement sans accompagnement adéquat des technologies peut aggraver leur vulnérabilité, chaque

nouvel appareil introduisant des points d'entrée supplémentaires pour les cyberattaques (Trouchaud, 2018).

Il est donc essentiel que les organisations adoptent une approche proactive, intégrant des stratégies de protection dès la conception des systèmes numériques. Cela inclut des évaluations de risque régulières, la mise à jour des protocoles de sécurité et la formation des employés aux bonnes pratiques. Un équilibre entre l'exploitation des avantages technologiques et la mise en place de mesures de sécurité robustes est crucial. En cultivant une culture de sécurité numérique et en intégrant la cybersécurité dans leur stratégie d'affaires, les entreprises peuvent maximiser les bénéfices des innovations tout en se protégeant contre les menaces émergentes.

1.1.3.2 Cybersécurité et cyberattaque : concepts et cadres d'interprétation

Une entreprise qui investit continuellement dans des mesures de cybersécurité et qui dispose d'une protection adéquate demeure néanmoins vulnérable aux cyberattaques. Aucune stratégie d'investissement en cybersécurité ne peut garantir une sécurité absolue des informations ni prévenir entièrement les intrusions malveillantes. Les cyberattaques évoluent constamment, et celles qui sont bien planifiées et ciblées, comme les attaques de type *Spear phishing* ou les *Ransomwares*, posent des défis particuliers aux organisations. Par exemple, une étude de l'IBM X-Force Research (Research, 2024) révèle que les attaques par ransomware ont augmenté de 1000 % entre 2015 et 2019, soulignant la sophistication croissante des menaces. De plus, selon le rapport de Verizon sur les violations de données (Verizon, 2024), près de 85 % des violations impliquent une forme d'ingénierie sociale, ce qui indique que les entreprises doivent non seulement renforcer leurs défenses techniques, mais également sensibiliser et former leur personnel. Les investissements en cybersécurité, bien qu'indispensables, ne peuvent remplacer une approche globale de gestion des risques. Cela inclut l'évaluation régulière des vulnérabilités, la mise en place de politiques de sécurité rigoureuses, et la réalisation de simulations d'attaques pour tester les réponses aux incidents. Par exemple, le Framework NIST fournit des lignes directrices sur l'identification, la protection, la détection, la réponse et la récupération face aux cybermenaces, insistant sur l'importance d'une stratégie proactive (NIST, 2018).

En somme, bien qu'un investissement constant en cybersécurité soit essentiel pour minimiser les risques, il est crucial de reconnaître qu'il n'existe pas de solution miracle. La cybersécurité requiert une vigilance continue, une adaptation aux nouvelles menaces et un engagement à tous les niveaux de l'organisation pour être réellement efficace.

1.1.3.2.1 Définition d'une cyberattaque

Les cyberattaques sont devenues de plus en plus fréquentes ces dernières années. Selon

Hathaway (2012), une cyberattaque est définie comme toute action visant à compromettre les fonctions d'un réseau informatique à des fins de sécurité politique ou nationale. Alors que Hathaway se concentre sur les motivations politiques des cyberattaques, le cybercommandement des États-Unis en offre une vision plus opérationnelle, orientée vers les systèmes critiques. En 2011, il introduit une définition militaire officielle, décrivant une cyberattaque comme un acte hostile utilisant des réseaux informatiques pour perturber ou détruire les systèmes critiques d'un adversaire, avec des effets pouvant s'étendre au-delà des systèmes informatiques eux-mêmes, notamment vers des infrastructures (Cartwright, 2011).

De plus, Kevin O'Shea (2003) précise que les cyberattaques consistent en des intrusions d'ordinateur à ordinateur qui compromettent la confidentialité, l'intégrité ou la disponibilité des informations. Ces définitions mettent en lumière la complexité et la portée croissante des cybermenaces dans le paysage actuel.

1.1.3.2.2 Typologie des hackers et analyse des menaces en cybersécurité

Les cyberattaquants se caractérisent par une diversité de motivations, allant des hackers éthiques aux acteurs malveillants, chacun jouant un rôle distinct dans l'écosystème des menaces numériques. Cette partie propose une analyse des différentes catégories de cyberattaquants et examine les types de menaces internes et externes, en mettant en lumière leur impact sur la sécurité des organisations et la gestion des risques.

Au niveau du profil des cyberattaquants, L'image stéréotypée du *hacker* comme un individu isolé, masqué, et engagé dans des activités illicites, ne représente qu'une fraction de la réalité. Les cyberattaquants agissent pour des motifs variés, et leurs actions peuvent aller du hacking éthique au cybercrime organisé. Les premières formes de *hacking* malveillant remontent au *phreaking* (piratage des lignes téléphoniques), mais cette activité a rapidement évolué vers d'autres formes plus complexes comme le *trolling*, où certains utilisateurs perturbent les discussions en ligne pour provoquer des réactions négatives. Avec le temps, certains de ces trolls ont migré vers le hacktivisme, un mouvement qui utilise les plateformes en ligne pour défendre des causes politiques. Cette évolution a également conduit à des pratiques comme l'utilisation de langages codés tels que le leet speak, initialement vus comme des manifestations marginales. Ces cyberattaquants, autrefois perçus comme des outsiders, sont désormais intégrés dans un écosystème plus large où cohabitent des criminels organisés, redéfinissant les enjeux et les défis de la cybersécurité contemporaine (Pech, 2023).

Figure 2 : types des cyberattaques

Source : thèse de doctorat en Sciences de l'information et de la communication de Yannik Pech, Intelligence cyber : intégrer les hackers dans une stratégie de sécurité numérique globale. Le modèle de l'intelligence économique, soutenue à l'université de Poitiers le 20 décembre 2023

Au niveau des types de menaces en cybersécurité, elles peuvent être classées en deux grandes catégories : internes et externes.

Les menaces internes proviennent souvent d'erreurs humaines non intentionnelles, comme l'oubli de données sensibles dans un lieu public par un employé. Bien que ces incidents ne soient pas toujours directement imputables à l'entreprise, ils révèlent la fragilité des systèmes de sécurité. Les menaces internes peuvent aussi être délibérées, avec des employés malveillants cherchant à tirer profit de données sensibles ou des employés mécontents décidés à nuire à leur entreprise en dénonçant des pratiques illégales. Ces attaques internes, bien que moins fréquentes, sont souvent plus difficiles à détecter et à prévenir.

Les menaces externes, considérées comme plus dangereuses, se déclinent en plusieurs profils de hackers :

- Hackers éthiques : ils réalisent des attaques pour démontrer les failles des systèmes, espérant ensuite collaborer avec les organisations ciblées.
- Hackers activistes : utilisant leurs compétences pour défendre des causes, comme

l'exemple d'Edward Snowden[1].

- Hackers concurrents : motivés par la recherche de secrets d'entreprise.
- Hackers criminels : souvent organisés en groupes, leur but est de s'enrichir par le vol de données ou d'argent.
- Hackers étatiques : participant à des cyber guerres entre pays (Trouchaud, 2016).

Au niveau des incidents de cybersécurité, le rapport Data Breach Investigations Report de Verizon (2018) recense 53 000 incidents de cybersécurité et 2 216 intrusions dans 65 pays. Ce rapport met en évidence la prédominance des menaces internes dans certains secteurs d'activité, notamment dans la santé et l'administration publique, où les informations sensibles attirent particulièrement les attaquants comme le montre la figure 3. En revanche, le secteur bancaire, fortement dépendant des interactions avec les clients, est davantage ciblé par des menaces externes, avec des hackers spécialisés représentant 61 % des intrusions comme indiqué dans la figure 4.

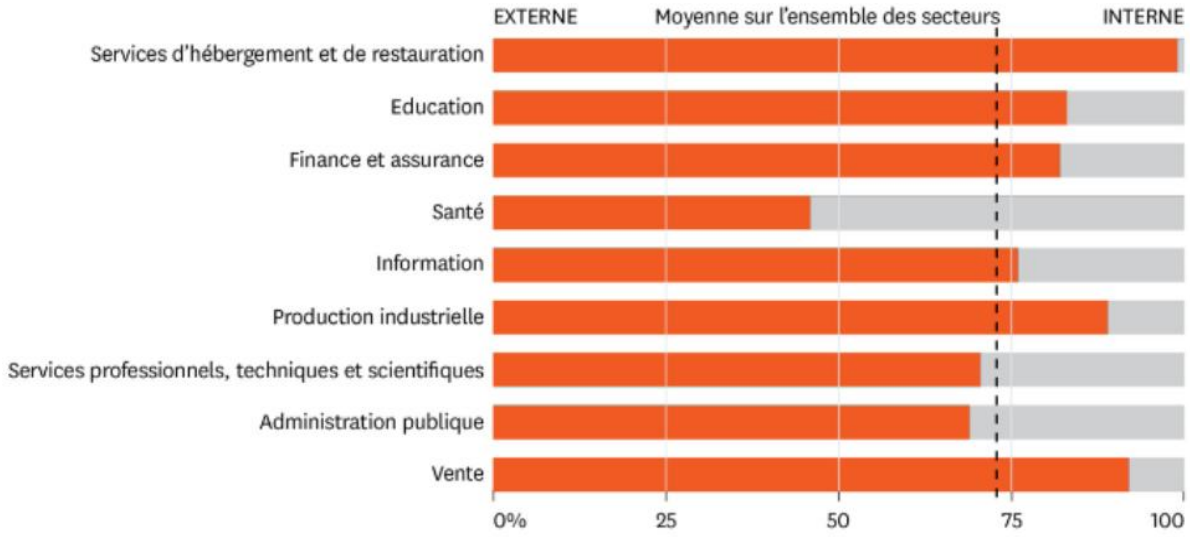


Figure 3 : cartographie des Menaces Cyber selon les Secteurs

Source: the End of Cybersecurity Harvard business Review 2019 p63-65

Selon le rapport de Verizon (2018), les menaces internes représentent environ 25 % des attaques, mais ce pourcentage varie en fonction du secteur. Dans les secteurs où les données sensibles sont critiques, telles que la santé ou les services professionnels, les menaces internes sont plus fréquentes. Dans le secteur bancaire, qui repose sur la confiance et la sécurité des transactions financières, les attaques externes dominent. Ce même rapport présente une

[1] Edward Snowden Edward Joseph Snowden, né le 21 juin 1983 à Elizabeth City, en Caroline du Nord est un lanceur d'alerte américain. Informaticien, ancien employé de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA), il a révélé l'existence de plusieurs programmes de surveillance de masse américains et britanniques. (Https://fr.wikipedia.org/wiki/Edward_Snowden)

cartographie des cibles les plus fréquentes des hackers, où les attaques les plus réussies ne coïncident pas toujours avec les cibles les plus souvent visées. (Bochman, 2019)

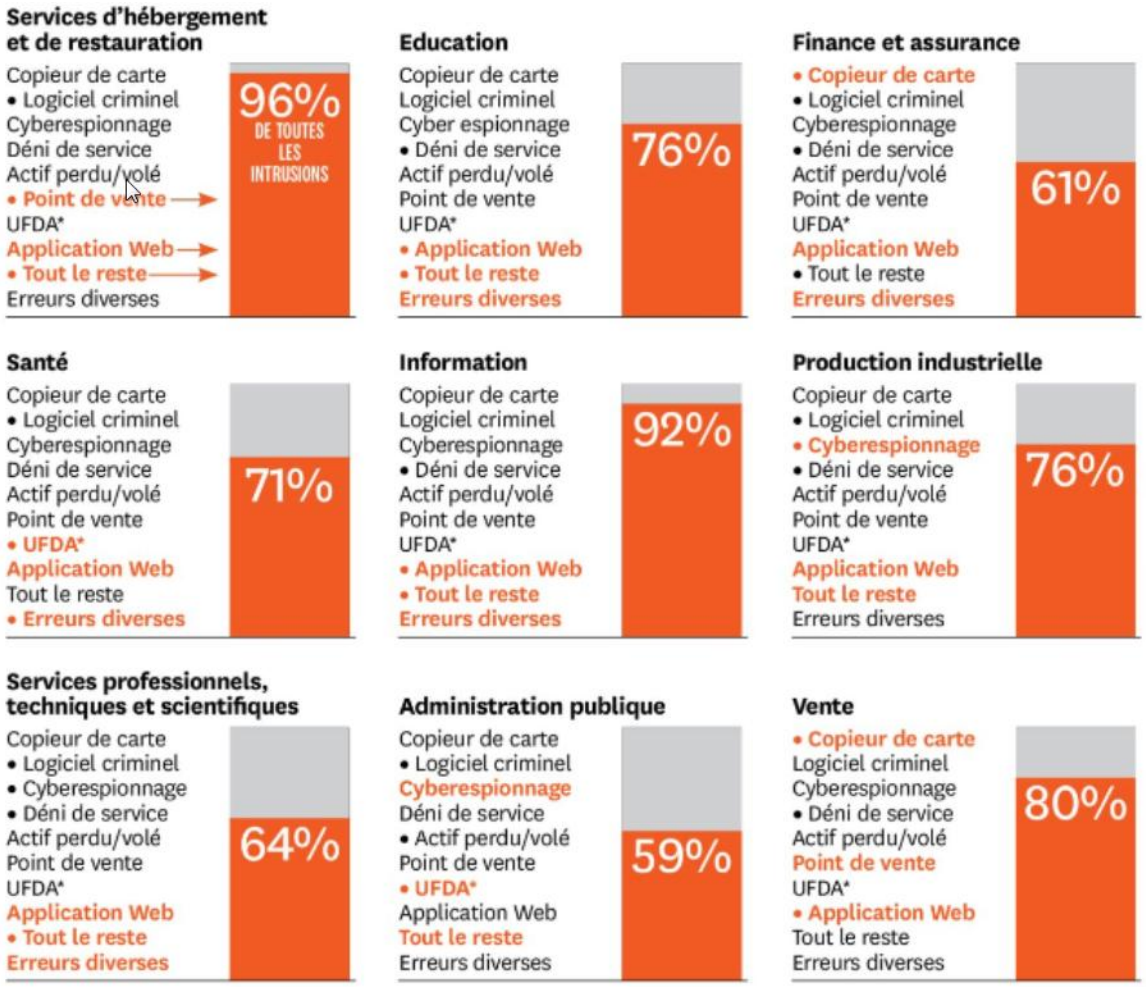


Figure 4 : les cibles les plus fréquentes des Hackers et les cibles qu'ils attaquent le plus souvent avec succès ne sont pas toujours les mêmes

Source: the End of Cybersecurity Harvard business Review 2019 p65-67

Pour faire face à ces menaces, les dirigeants des entreprises, et en particulier des institutions financières, doivent adopter une approche intégrée de la cybersécurité. Cela signifie ne pas se reposer uniquement sur des solutions technologiques, mais également sur des politiques robustes de gestion des risques, incluant la formation des employés et une veille active contre les nouvelles menaces. La cybersécurité doit donc être perçue non seulement comme une question technique, mais également comme un enjeu organisationnel, impliquant tous les niveaux de l'entreprise dans la protection des données sensibles.

En conclusion, bien que les technologies de défense avancées soient essentielles, une stratégie complète de cybersécurité exige une combinaison d'outils technologiques, de sensibilisation humaine et d'une organisation adaptée pour protéger efficacement les entreprises des menaces internes et externes. Les définitions de cyberattaques mentionnées précédemment reflètent la

diversité des motivations des cyberattaquants, qu'il s'agisse de hacktivisme, de cybercriminalité ou de cyberguerre, comme nous l'avons exploré dans la typologie des hackers.

1.1.3.2.3 Les cyberattaques détruisent la confiance

Les cyberattaques représentent une menace majeure non seulement pour la sécurité des systèmes, mais aussi pour la confiance, élément fondamental dans les relations entre entreprises et clients. Le rapport 2017 sur le coût de la cybercriminalité, réalisé par Accenture en collaboration avec le Ponemon Institute, souligne l'augmentation significative des cyberattaques ciblant des infrastructures critiques, privant les utilisateurs de l'accès à leurs données, souvent jusqu'au paiement d'une rançon (Bochman, 2019).

L'attaque WannaCry, lancée en mai 2017, en est l'un des exemples les plus marquants. Exploitant une vulnérabilité de Windows, déjà signalée par Microsoft, ce logiciel malveillant a touché des organisations telles que Vodafone, Renault et Fedex, entraînant des pertes financières massives. Cette cyberattaque est qualifiée comme le plus grand piratage à rançon de l'histoire d'Internet. Plusieurs victimes ont souffert de cette attaque comme Vodafone, Renault, Fedex qui ont tous été assujettis à des pertes de millions de dollars.

L'impact des cyberattaques dépasse le cadre strict de la cybersécurité. Elles affectent profondément la confiance, tant dans les entreprises qu'au niveau sectoriel. Une étude d'OpinionWay sur la confiance dans le secteur bancaire a révélé que les cyberattaques érodent durablement la confiance des clients. L'exemple de la société Equifax, victime d'une attaque en septembre 2017 ayant compromis 143 millions de données personnelles, démontre l'ampleur des conséquences. La capitalisation boursière d'Equifax a chuté de 25 % en seulement 18 jours, illustrant l'impact financier direct et la destruction de la confiance dans la marque. Les cyberattaques peuvent être fatales aux entreprises, en particulier aux petites et moyennes entreprises (PME). Selon une étude américaine, plus de 60 % des PME touchées par une cyberattaque majeure ont fait faillite dans les six mois suivant l'incident (Trouchaud, 2018).

Les coûts liés aux cyberattaques, notamment ceux générés par WannaCry et NotPetya, qui ont causé respectivement plus de 4 milliards et 850 millions de dollars de dommages en 2017, continuent de croître de manière exponentielle (Bochman, 2019).

Face à cette situation, les investissements en cybersécurité ne cessent d'augmenter, les entreprises cherchant à se prémunir contre ces menaces et à restaurer la confiance de leurs parties prenantes. Une gestion proactive de la cybersécurité, en intégrant des mesures préventives robustes, demeure essentielle pour éviter les conséquences dévastatrices des cyberattaques, tant sur le plan financier qu'en termes de réputation et de survie d'entreprise. (Trouchaud, 2018).

1.1.3.2.4 La cybersécurité : une approche stratégique pour la protection des systèmes d'information

La cybersécurité émerge comme une solution stratégique pour restaurer la confiance et protéger les intérêts économiques des entreprises, en particulier dans des secteurs sensibles comme le bancaire.

Selon Trouchaud (2018), l'adoption d'une cybersécurité raisonnée, centrée sur des dispositifs technologiques robustes et des interventions humaines, peut rétablir durablement la confiance des clients. Cette approche ne se limite pas à une simple protection technique, mais renforce le lien de confiance en créant un climat de réassurance, indispensable dans un environnement digitalisé. En effet, dans le secteur bancaire, la confiance des clients repose autant sur la sécurité technologique que sur la solidité du capital de marque. La cybersécurité, en tant que pilier de la gestion de cette confiance, devient donc incontournable pour préserver la réputation des entreprises. Une cybersécurité basée sur une surveillance humaine combinée à une organisation moderne peut non seulement renforcer la confiance, mais également optimiser les coûts à long terme. En intégrant une gestion proactive des risques et des dispositifs de protection adaptés, les entreprises peuvent espérer une réduction progressive des coûts liés aux cyberattaques. Toutefois, cette évolution pourrait aussi inciter certaines institutions à externaliser, partiellement ou totalement, leurs services de cybersécurité, en raison des contraintes budgétaires. Cette tendance à l'externalisation souligne la nécessité d'une cybersécurité non seulement technique, mais également organisationnelle, adaptée aux réalités économiques et financières des entreprises.

1.1.3.3 Relations entre la cybersécurité et la cybercriminalité

La cybercriminalité, qui symbolise depuis longtemps l'insécurité dans le cyberespace (Wall, 2005), désigne toutes les activités criminelles impliquant l'utilisation d'ordinateurs et d'appareils connectés à Internet pour enfreindre les lois. Ce phénomène a évolué parallèlement au développement d'Internet et à l'essor des technologies de l'information. Penuel (2013) utilise le terme de manière interchangeable avec le crime technologique ou numérique, englobant aussi bien les crimes traditionnels transposés en ligne (fraude, menaces) que de nouvelles formes d'activités criminelles comme le piratage et la diffusion de virus.

Frunza (2016) identifie la cybercriminalité comme l'une des menaces les plus perturbatrices pour les marchés financiers, en particulier le secteur bancaire. Toutefois, cette menace reste sous-estimée par les institutions financières et les régulateurs, malgré les dommages importants causés par les escroqueries, notamment les fraudes par carte de crédit. Les infrastructures

numériques des marchés financiers sont particulièrement vulnérables, exposant le secteur à des pertes illimitées en cas d'attaque. La manipulation des informations sur les marchés via les médias sociaux et les plateformes en ligne constitue également un risque croissant, pouvant influencer la réalité économique. Frunza (2016) souligne également que la centralisation des contreparties expose tout le système financier à des cyberrisques majeurs, encore insuffisamment étudiés. Cette situation, associée aux coûts croissants de la cybersécurité, confirme la nécessité d'investissements importants dans ce domaine. Selon le rapport de Norton (2011), la cybercriminalité coûte à l'économie mondiale 338 milliards de dollars par an, un chiffre en constante augmentation. Le rapport de 2017 d'Accenture et du Ponemon Institute montre une augmentation de 62 % du coût de la cybercriminalité entre 2013 et 2017, confirmant la tendance mondiale à la hausse des coûts liés aux attaques. L'étude s'appuie sur des réponses obtenues auprès de 254 entreprises à travers 15 Pays. Comme l'affiche la figure 5 ci-dessous, le coût de la cybercriminalité augmente de 62% entre 2013 et 2017 (Bochman, 2019).

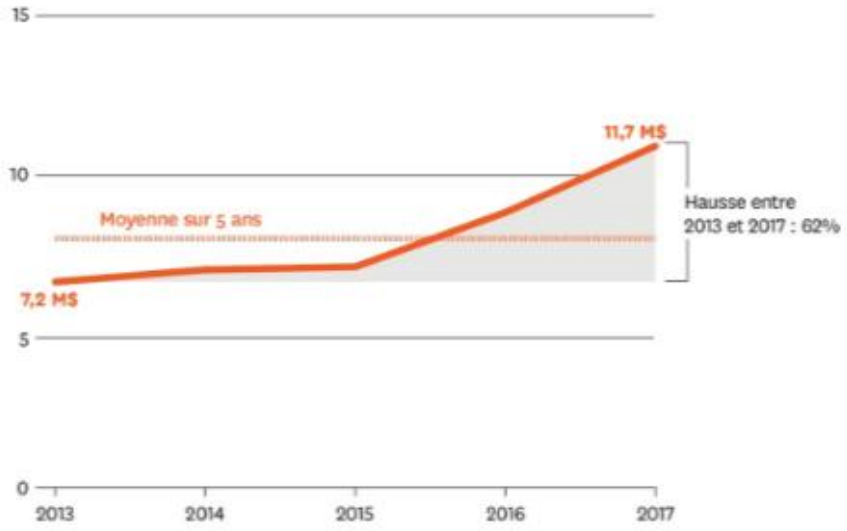


Figure 5 : coût moyen de la cybercriminalité par entreprise (en millions de dollars)

Source: 2017 Cost of Cybercrime study: Insights on the security investments that make a difference » de Verizon et Ponemon.

Les études de Berinato et Perry (2019), révèlent que les entreprises des secteurs financier et public sont particulièrement vulnérables aux cyberattaques, en raison de la sensibilité accrue des données qu'elles manipulent. Bien que les dépenses liées à la détection et au contrôle des attaques aient enregistré une légère augmentation, les pertes de revenus n'ont pas suivi une baisse proportionnelle. Cela suggère que, malgré une meilleure maîtrise des dispositifs de cybersécurité, les entreprises continuent de subir des pertes croissantes en matière de données sensibles et de capital. Comme illustré dans la figure 5, l'investissement dans la cybersécurité a augmenté de 5 % entre 2015 et 2017, de même que les taux de prévention des intrusions.

Toutefois, les figures 6 et 7 montrent que les pertes de revenus liées aux cyberattaques n'ont pas diminué proportionnellement à l'amélioration des systèmes de défense. Bien que les perturbations des activités soient moins coûteuses qu'auparavant, les entreprises peinent toujours à réduire les pertes de données, malgré la croissance continue des menaces cybernétiques.

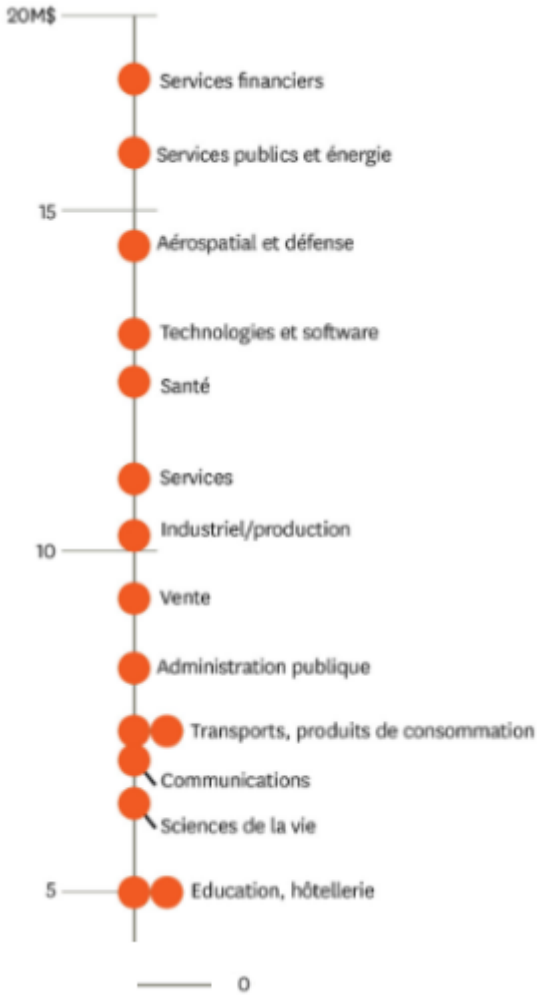


Figure 6 : coût moyen de la cybercriminalité par secteur en millions de dollars

Source: 2017 Cost of Cybercrime study: Insights on the security investments that make a difference » de Verizon et Ponemon.

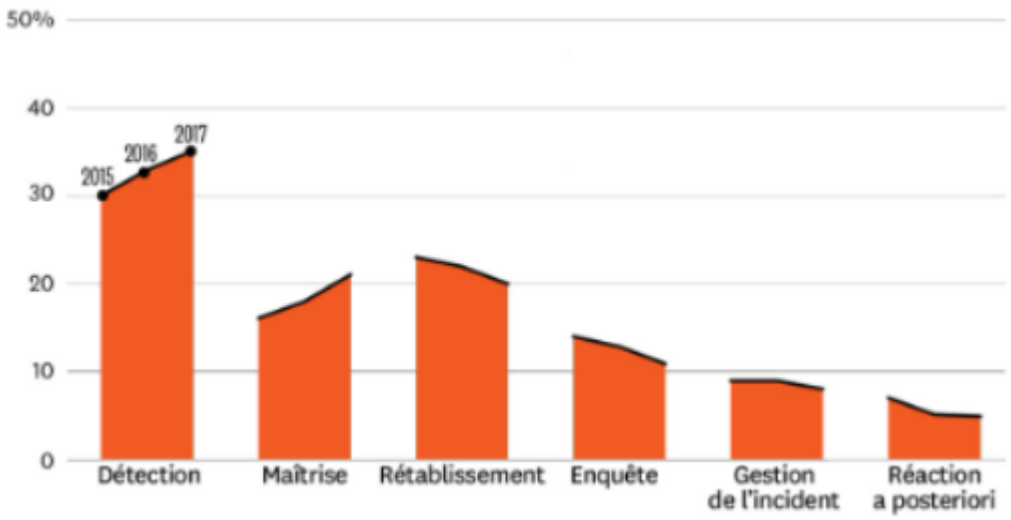


Figure 7 : part des coûts à la suite d'activité

Source: 2017 Cost of Cybercrime study: Insights on the security investments that make a difference » de Verizon et Ponemon.

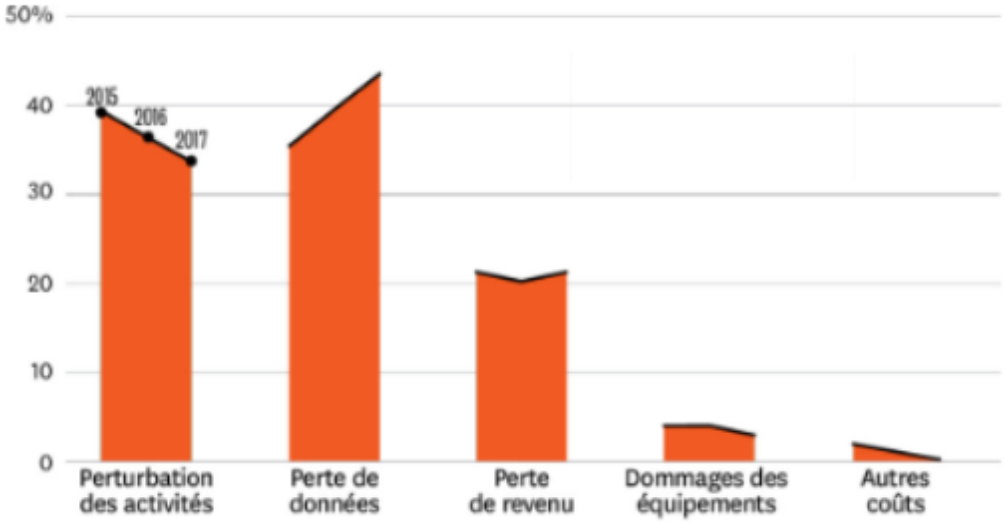


Figure 8 : part des coûts à la suite d'attaques

Source: 2017 Cost of Cybercrime study: Insights on the security investments that make a difference » de Verizon et Ponemon.

Malgré l'augmentation des investissements dans la cybersécurité, les entreprises peinent encore à limiter les pertes résultant des attaques réussies. Le secteur bancaire, particulièrement vulnérable, subit des risques accrus en raison de la valeur des données sensibles et des actifs financiers qu'il gère. Dès lors, il est essentiel pour les entreprises de repenser leur approche de la cybersécurité en adoptant une gestion plus stratégique et adaptée à la nature évolutive des cybermenaces. Pourtant, nombre d'entre elles continuent à sous-évaluer ces risques et à insuffisamment investir, ce qui les empêche de répondre de manière adéquate aux menaces actuelles.

1.1.3.4 Interdépendance entre Cybersécurité et Cyberguerre

La cyberguerre se distingue des cyberattaques et de la cybercriminalité par son contexte et ses objectifs. En effet, bien qu'il existe un chevauchement entre la cyberguerre et la cyberattaque, la première est généralement liée à des motivations politiques ou de sécurité nationale, et souvent associée à un conflit armé. Contrairement à la cybercriminalité, qui est motivée principalement par des gains financiers, la cyberguerre vise à perturber ou endommager des infrastructures critiques, des réseaux ou des systèmes d'information à des fins stratégiques. Elle peut donc impliquer des violations du droit pénal, notamment des crimes de guerre, lorsqu'elle compromet des réseaux à des fins de déstabilisation politique ou de sécurité nationale (Hathaway, 2012).

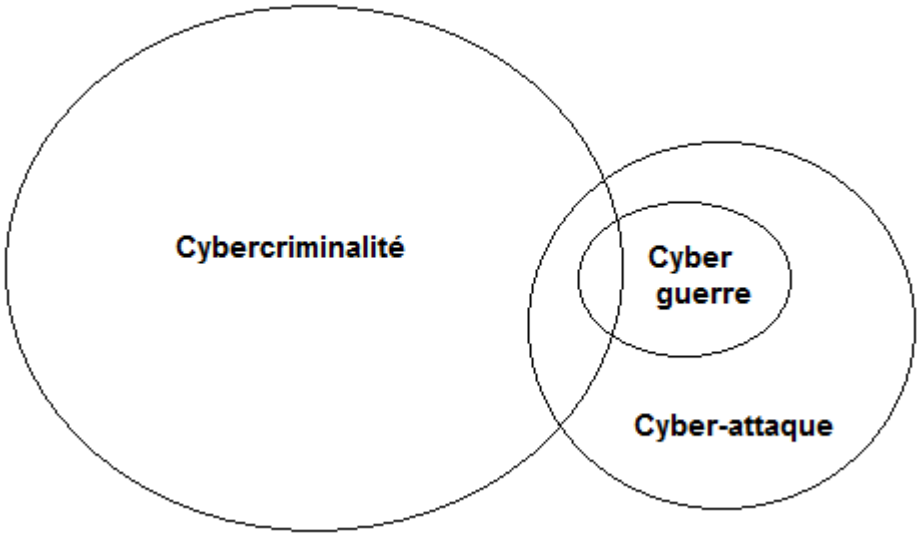


Figure 9 : interactions entre la cyberguerre, la cybercriminalité et les cyberattaques

Source: adaptive Random Mac Strategy for IoT Security through Network Forensics Investigation (Abid, 2024).

En pratique, la cyberguerre se concentre sur l'utilisation de l'information et des connaissances techniques pour mener des attaques ciblées sur les systèmes d'un autre État, cherchant à paralyser ou endommager les infrastructures essentielles. Ces attaques peuvent survenir en temps de guerre, mais aussi en période de paix, lorsque les cyberopérations visent à exercer une pression sans recourir à des hostilités conventionnelles (Eun, 2016).

Par ailleurs, les cyberattaques qui causent des destructions physiques ou la perte de vies humaines sont souvent considérées comme des actes de guerre ou de terrorisme. Ces opérations ne se limitent pas aux seuls États-nations ; des acteurs non étatiques peuvent également les mener, illustrant ainsi la complexité et la diversité des menaces dans le domaine de la cyberguerre.

1.1.3.5 Synergie entre Cybersécurité et systèmes d'information

La cybersécurité et la sécurité de l'information sont souvent confondues, bien qu'il soit essentiel de les distinguer tout en reconnaissant leurs chevauchements. La cybersécurité va au-delà de la sécurité de l'information classique en englobant non seulement la protection des données, mais aussi des infrastructures et des individus, qui peuvent être à la fois des cibles et des participants involontaires à des cyberattaques. Cette distinction inclut des enjeux éthiques et sociétaux, tels que la protection des groupes vulnérables, comme les enfants (Von Solms, 2013).

L'organisation internationale de normalisation (ISO) (2014) définit la sécurité de l'information comme la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations, qu'elles soient électroniques ou physiques. La cybersécurité, quant à elle, se concentre sur la protection de l'information dans le cyberespace, un environnement virtuel résultant de l'interaction entre technologies, réseaux et utilisateurs. Malgré des définitions proches, la cybersécurité se distingue en se concentrant sur la protection contre les menaces spécifiques à l'Internet et au cyberespace, tandis que la sécurité de l'information englobe une plus grande diversité d'environnements, incluant des menaces physiques et humaines (ISO/IEC 27002, 2013).

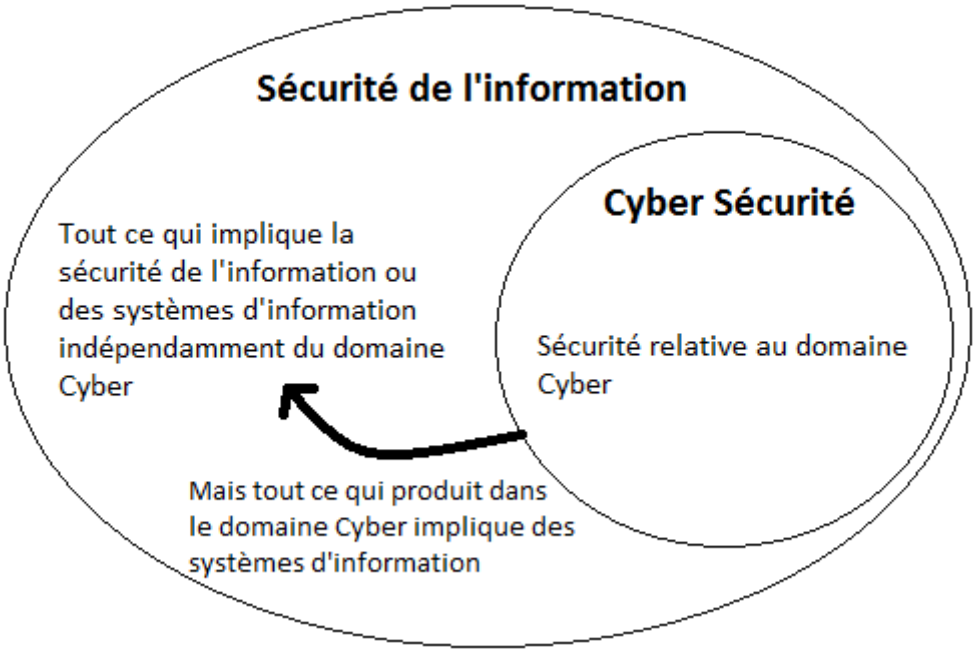


Figure 10 : relation entre la cybersécurité et la sécurité de l'information

Source: élaboration personnelle

La cybersécurité reste un sous-ensemble de la sécurité de l'information, mais elle ne se limite pas à celle-ci. Elle nécessite des compétences techniques approfondies et couvre une large

gamme de pratiques allant de la protection des infrastructures à la gestion des accès aux données (Valparaiso University, 2017).

La sécurité de l'information, pour sa part, concerne la protection des informations dans tous les contextes, qu'elles soient en ligne ou non (Von Solms, 2013).

Par ailleurs, le développement du cloud computing a transformé les pratiques de stockage et de gestion des données. Le cloud permet aux entreprises de stocker et de gérer leurs données à distance, offrant une plus grande flexibilité et des coûts réduits. Cependant, il pose également des défis supplémentaires en matière de cybersécurité. Les prestataires de cloud doivent garantir la sécurité des données sensibles et stratégiques des entreprises, tout en respectant les réglementations sur la protection des données. Cette évolution entraîne une convergence des rôles entre la cybersécurité et la gestion de l'information, nécessitant des outils robustes pour protéger les données stockées dans le cloud, prévenir les attaques et assurer la conformité (Braudo, 2022) (Chambre de commerce et d'industrie, 2022).

Enfin, il est important de noter que la cybersécurité joue un rôle critique dans la protection des infrastructures et des systèmes d'information contre les menaces liées au cyberespace. Alors que la sécurité de l'information protège les données sous toutes leurs formes, la cybersécurité se concentre sur les menaces provenant spécifiquement du cyberespace. Ensemble, ces deux disciplines contribuent à une gestion globale des risques et à la protection des actifs informationnels et stratégiques des entreprises (Refsdal, Solhaug, et Stolen, 2015).

1.1.4 Les défis de la cybersécurité

La cybersécurité est un problème permanent pour les gouvernements, le secteur privé et les individus du monde entier. Il est inhabituel pour plus d'un mois de passer sans nouvelles d'une cyberattaque importante. Pour certaines victimes, ces attaques sont un désagrément, alors que pour d'autres elles sont coûteuses et se soldent par des confusions de secrets, des conceptions de biens volés ou des dommages à la réputation. Le problème de la cybersécurité ne peut jamais être résolu. Cela peut seulement être pire ou plus amélioré. Les tentatives d'améliorer la sécurité ou d'optimiser la situation existante dépendront de la disponibilité de ressources limitées telles que le temps, l'argent, la réputation et la volonté politique (Clemente, 2011).

En effet, pratiquement tous les domaines, de la médecine à l'éducation, de la finance aux achats en ligne, sont concernés par la nécessité de protéger les informations personnelles, institutionnelles et professionnelles et de ne pas être victimes de prédateurs et d'escrocs. C'est ce que la cybersécurité implique. Elle comprend également les renseignements nationaux et internationaux liés à la protection et à la défense (Gay, 2011).

1.1.4.1 Un problème mondial

Au début des années 2010, une prise de conscience politique majeure de l'importance de la cybersécurité a émergé, portée notamment par des figures comme Barack Obama et David Cameron. Obama, lors de son premier mandat, a souligné que la multiplication des cyberattaques représentait l'une des menaces les plus sérieuses pour la sécurité nationale et économique des États-Unis. En mai 2011, il a introduit une stratégie nationale pour le cyberespace, axée sur l'amélioration de la sécurité Internet, la protection de la vie privée, la liberté d'expression et la lutte contre la cybercriminalité. Il a toutefois reconnu que, malgré des progrès significatifs, les États-Unis restaient vulnérables face à ces menaces mondiales croissantes (Office of the Press Secretary, 2016).

Simultanément, David Cameron, lors de la *London Cyber Conference*, a affirmé que la cybersécurité internationale était devenue une urgence mondiale, citant des tentatives à grande échelle de vol de secrets d'État (Cameron, 2011). Ce discours reflète une tendance générale : à mesure que les cyberattaques se multiplient, notamment contre les secteurs sensibles comme les banques, les gouvernements et les organisations prennent conscience de la nécessité de renforcer leur cybersécurité.

Le FBI a rapporté qu'en 2014, environ 800 millions de dollars de pertes liées à la cybercriminalité ont été signalées, soulignant l'ampleur du phénomène (Federal Burean Of Investigation, 2014). Le général Rogers, alors à la tête du Cyber Command américain, a également déclaré que chaque conflit moderne intégrait désormais une dimension cybernétique, reflétant l'internationalisation des cybermenaces (Rogers, 2015).

Les attaques ne sont pas limitées par les frontières, touchant aussi bien les pays développés que ceux en développement, avec une prédilection pour les institutions financières comme les banques, qui manipulent des données sensibles et des capitaux. Selon Tariq (2018), ces institutions présentent un risque cybernétique particulièrement élevé. Les cybercriminels ciblent souvent ces entités pour obtenir des avantages financiers ou perturber leurs services, rendant impératif pour les organisations de se protéger avec des outils et des stratégies à jour.

Ainsi, la cybersécurité est devenue une préoccupation globale, transcendant les sphères politique, économique, militaire et sociale, tout en constituant un enjeu stratégique pour les dirigeants d'institutions.

1.1.4.2 Une cybersécurité très coûteuse

La cybersécurité, bien qu'indispensable, représente un coût financier croissant pour les entreprises, en raison de la multiplication et de la sophistication des cyberattaques. Comme évoqué précédemment, les budgets alloués à la cybersécurité augmentent continuellement pour

répondre aux menaces. Par exemple, en 2015, Lloyd's of London estimait que les cyberattaques coûtaient jusqu'à 400 milliards de dollars par an aux entreprises, en incluant les dommages directs et les perturbations des activités. Ce chiffre pourrait même dépasser les 500 milliards selon certaines prévisions (Morgan, 2016).

La montée en flèche de ces coûts est particulièrement visible dans le secteur bancaire, où des attaques massives, comme celles visant la banque centrale du Bangladesh via le réseau SWIFT, ont mis en lumière la vulnérabilité des infrastructures numériques. Ces attaques, attribuées au groupe de hackers Lazarus, ont coûté environ 100 millions USD (Corkery, 2016), mettant en évidence l'absence de systèmes sophistiqués de détection des menaces dans de nombreuses banques (KPMG, 2016)

Les cyberattaques ne sont pas seulement coûteuses en termes financiers, elles affectent également la réputation et la confiance accordées aux entreprises. Le Ponemon Institute (2012) a montré que la fréquence et la gravité des cyberattaques ont considérablement augmenté entre 2010 et 2012, notamment dans les secteurs les plus touchés comme la finance. Le coût de ces attaques varie en fonction de la taille de l'organisation, les attaques par déni de service et les intrusions malveillantes étant parmi les plus coûteuses.

En 2016, une enquête menée au Royaume-Uni a révélé que 52 % des entreprises avaient subi une cyberattaque, avec des pertes estimées à 30 milliards de livres sterling pour l'ensemble des entreprises britanniques (ISP Beaming, 2016). Ces données illustrent la tendance mondiale : la cybersécurité est non seulement un enjeu technique, mais également une question de survie économique et de maintien de la confiance pour les organisations.

En somme, il est indéniable que les cyberattaques imposent des coûts considérables aux entreprises, tant en termes de pertes directes que de perturbations des activités et de confiance publique. La gestion proactive de la cybersécurité est devenue un investissement essentiel pour limiter ces coûts et protéger les infrastructures numériques.

1.1.4.3 Évolution des fréquences des cyberattaques

Les menaces liées au cyberespace sont non seulement réelles, mais elles continuent de croître à un rythme alarmant. Des études récentes révèlent que 97 % des organisations dans 63 pays ont subi des violations de sécurité, et 98 % des applications testées dans 15 pays présentent des vulnérabilités. En moyenne, le coût annualisé de la cybercriminalité s'élève à 7,7 millions de dollars pour les 252 organisations mondiales évaluées en 2015. De plus, 60 % des entreprises allouent davantage de ressources à des mesures réactives qu'à une gestion proactive des risques (Matthews, Arata, et Hal, 2016).

Une enquête de Cybersecurity Ventures (2024) souligne qu'une entreprise devient la cible d'une

attaque toutes les 40 secondes, une fréquence qui pourrait atteindre une attaque toutes les 14 secondes prochainement. La cybersécurité, en tant qu'industrie de plusieurs milliards de dollars, fait face à une augmentation exponentielle des attaques, estimée à 350 % par an. Selon des projections, d'ici 2025, les coûts globaux liés à la cybercriminalité pourraient dépasser les 10 trillions de dollars.

Walters (2022) note que ces incidents notables ne représentent qu'une fraction des attaques mineures survenant quotidiennement. D'après la Cyberthreat Map de Kaspersky, en 2024, les attaques se multiplient à un rythme accéléré, avec des détections en temps réel dans le monde entier. Différents types de menaces, tels que les ransomwares, les botnets et l'exploitation des vulnérabilités, touchent de nombreuses régions, révélant l'adaptation continue des cybercriminels. Cette évolution souligne l'importance pour les individus et les organisations d'adopter des mesures de cybersécurité proactives et robustes pour faire face à cette menace croissante. (Kaspersky, 2024)

1.1.4.4 L'essor technologique : une vulnérabilité en expansion continue

Une étude menée par CEO *Survey* de *PwC*, 82% affirme que leur priorité est l'investissement technologique. Ils justifient cela pour améliorer la logistique, la satisfaction client et la sécurité du réseau. (Trouchaud, 2016)

L'investissement dans les nouvelles technologies entraîne inévitablement l'apparition de nouveaux risques et de vulnérabilités qu'il convient d'adresser. Si l'adoption de systèmes technologiques de protection est indispensable, il est tout aussi crucial de réinvestir dans la dimension humaine pour assurer une gestion efficace des risques. La cybersécurité repose sur la prévention, la régulation et l'anticipation de ces menaces. Bien que la technologie soit essentielle, elle génère également des risques considérables. Une contrainte technologique se manifeste, car si les bonnes technologies peuvent automatiser la gestion des risques classiques, elles doivent impérativement être associées à une approche stratégique globale et humaine pour garantir leur efficacité.

Conclusion intermédiaire

La cybersécurité constitue un domaine complexe englobant une variété de pratiques, de politiques et de technologies visant à protéger les systèmes informatiques et les informations contre les cyberattaques. Elle se distingue par sa nature défensive, contrairement à l'utilisation offensive des technologies de l'information dans le cyberespace. Face à une augmentation constante et à la sophistication des cyberattaques, la cybersécurité se présente comme un enjeu mondial majeur, impliquant des coûts importants et une évolution perpétuelle des menaces.

Les statistiques mettent en lumière l'ampleur de ce problème, avec un nombre croissant d'organisations victimes de cyberattaques coûteuses. Cette situation souligne la nécessité d'adopter une approche proactive en matière de gestion des risques. En effet, la cybersécurité touche tous les secteurs, de la médecine à la finance, nécessitant ainsi des stratégies adaptées à chaque domaine.

Investir dans de nouvelles technologies s'avère crucial pour renforcer la sécurité des systèmes. Toutefois, cette démarche doit s'accompagner d'une gestion humaine stratégique afin d'anticiper et de répondre efficacement aux menaces émergentes. Ainsi, la cybersécurité demeure un défi permanent qui ne peut jamais être entièrement résolu. Néanmoins, elle peut être améliorée par des efforts humains continus, la mobilisation de ressources limitées et une collaboration mondiale.

En conclusion, il est évident que la cybersécurité ne se limite pas à une question technologique ; elle implique également des dimensions humaines et organisationnelles. Cette première section (1.1) met en exergue l'importance d'une approche intégrée pour faire face aux menaces croissantes du cyberespace.

1.2 L’importance d’une collaboration interprofessionnelle

La cybersécurité est désormais une priorité nationale de premier plan, dont l'importance ne peut que croître à mesure que notre dépendance aux systèmes informatiques augmente. Jusqu'à présent, la majorité des recherches en cybersécurité ont été centrées sur les applications technologiques, négligeant ainsi les rôles critiques des acteurs humains dans les opérations cybernétiques. Dans la partie précédente (1.1), nous avons souligné que la cybersécurité ne se limite pas à un enjeu technologique ; elle revêt également une dimension humaine et organisationnelle.

Au cours des dernières années, la communauté des facteurs humains a commencé à explorer les problématiques centrées sur l'humain dans les opérations cybernétiques. Cependant, par rapport aux avancées réalisées dans les communautés technologiques, nous n'avons qu'effleuré la surface de cette question. Bien que les publications sur les facteurs humains dans le cyberespace se multiplient, il subsiste un écart significatif entre la compréhension théorique du domaine et la recherche appliquée destinée à traiter des enjeux concrets.

Il est donc essentiel de clarifier et d'élargir le rôle des facteurs humains dans la cybersécurité en examinant les fonctions, les tâches et les responsabilités des opérateurs dans ces environnements. Les humains sont souvent perçus comme le maillon le plus faible de la cybersécurité, car toute solution technique est vulnérable aux défaillances causées par des erreurs humaines. En conséquence, une quantité considérable de recherches vise à mieux comprendre les utilisateurs et les facteurs qui influencent leurs comportements en matière de sécurité. Bien que plusieurs études aient identifié des traits humains corrélés à de mauvaises pratiques de sécurité et une susceptibilité accrue aux cybercrimes, tels que le phishing ou l'ingénierie sociale, les travaux dans ce domaine demeurent encore limités (Egelman, 2015).

La cybersécurité est un enjeu à la fois technologique et humain, intimement lié aux risques organisationnels. La technologie seule ne saurait suffire ; la cybersécurité requiert une synergie entre les systèmes informatiques, les innovations technologiques et le facteur humain. Sans une dimension humaine intégrée et une organisation adéquate, les initiatives en cybersécurité resteront constamment remises en question. La mise en œuvre d'une stratégie de cybersécurité efficace nécessite une collaboration étroite entre les managers, les dirigeants, les auditeurs internes et les responsables de la sécurité de l'information. Ainsi, il s'agit d'une véritable coopération entre les différentes parties prenantes de l'entreprise pour garantir une cybersécurité optimale.

1.2.1 Le facteur humain non formé demeure le maillon le plus faible

Les erreurs humaines constituent un défi majeur en matière de cybersécurité, pouvant engendrer des conséquences significatives, allant parfois jusqu'à des dommages catastrophiques. Ces erreurs peuvent être classées en deux catégories : intentionnelles et involontaires. Les erreurs involontaires, telles que les lapsus, les oublis ou les défaillances d'attention, surviennent fréquemment dans des environnements stressants ou mal adaptés. En revanche, les erreurs intentionnelles peuvent inclure des violations délibérées des règles de sécurité, des actes de sabotage ou des manquements aux protocoles établis. Bien que la formation et l'éducation puissent contribuer à réduire les erreurs liées à la connaissance et aux règles, elles ne suffisent pas à prévenir les erreurs involontaires, surtout dans des contextes environnementaux exigeants. Il a été démontré que de nombreuses menaces internes proviennent principalement d'erreurs non intentionnelles, souvent dues à des employés mal informés ou négligents. Ce constat souligne l'importance de mieux comprendre les rôles, les tâches et les responsabilités des opérateurs humains dans les environnements de cybersécurité.

Gratian (2018) examine comment les différences individuelles influencent les comportements en matière de cybersécurité. Cette recherche est cruciale pour aider les professionnels de la sécurité et les organisations à identifier les utilisateurs susceptibles de recourir à des pratiques de sécurité inappropriées. Une telle compréhension permettrait de développer des programmes éducatifs ciblés et d'orienter les efforts de sensibilisation vers les utilisateurs les plus à risque.

La cybersécurité ne se limite pas aux technologies et aux systèmes ; elle implique également les personnes et les processus qui en dépendent. Le département de la Sécurité intérieure Homeland Security a la responsabilité de sécuriser les infrastructures technologiques des entités publiques et privées. Cet objectif ne peut être atteint uniquement par des avancées technologiques ; il nécessite une attention particulière aux individus et aux processus qui soutiennent ces technologies (Bowen, 2012).

Les erreurs humaines demeurent un facteur de risque majeur en cybersécurité. Selon le rapport 2023 d'IBM, ces erreurs sont responsables de plus de 95 % des incidents de sécurité analysés, soulignant une tendance préoccupante (Security, 2023).

De même, une enquête menée par *PwC* a révélé que 50 % des violations de cybersécurité les plus graves en 2019 étaient attribuables à des erreurs humaines involontaires, une augmentation notable par rapport à l'année précédente (Arora, 2019).

D'après *CompTIA*, l'erreur humaine est la principale cause de violations de données, représentant 52 % des incidents signalés. Pourtant, paradoxalement, seuls 30 % des répondants

considèrent cette erreur parmi les employés comme une préoccupation sérieuse (Harvey, 2016). Cette dichotomie souligne l'importance d'une meilleure sensibilisation et d'une formation adéquate.

Des menaces comme l'ingénierie sociale exploitent les erreurs humaines en utilisant des manipulations psychologiques pour inciter les utilisateurs à divulguer des informations sensibles ou à effectuer des actions compromettantes, telles que cliquer sur des liens malveillants ou fournir des mots de passe (Mak, 2017).

Un rapport de la *FINRA* en 2023 souligne que de nombreuses cyberattaques réussissent en raison du non-respect des protocoles de sécurité, révélant ainsi l'importance cruciale de la conformité et de la vigilance dans la protection contre ces menaces. (FINRA, 2023)

Malgré l'augmentation des violations et des cyberattaques, la cybersécurité reste souvent perçue comme une préoccupation secondaire dans de nombreuses industries. Cela s'explique par une certaine complaisance, où les employés et les dirigeants supposent à tort que la sécurité est déjà intégrée dans les systèmes existants ou qu'elle relève de la responsabilité d'autrui. Cette perception erronée est particulièrement courante parmi les petites entreprises, qui estiment à tort qu'elles ne sont pas des cibles potentielles.

Cependant, chaque entreprise est vulnérable, car elle détient des informations précieuses pour les cybercriminels, qu'il s'agisse d'accès financiers ou de données personnelles identifiables. Par conséquent, il est crucial que chaque organisation évalue ses processus de sécurité et les améliore de manière proactive (Quader, 2016).

Le risque posé par des employés non formés et non sensibilisés à la cybersécurité représente une menace sérieuse qui nécessite une attention immédiate.

1.2.2 La nécessaire prise en compte l'intervention humaine dans l'assurance de la cybersécurité

Les approches contemporaines en cybersécurité continuent d'ignorer le rôle crucial du facteur humain au sein des systèmes complexes. Bien que la cybersécurité repose sur des infrastructures technologiques, elle s'inscrit dans un contexte plus large où l'interaction humaine joue un rôle déterminant. Les défis tels que la détection d'intrusions et les menaces de piratage sont amplifiés par des caractéristiques spécifiques au cyberespace, notamment l'absence de contraintes physiques et la capacité de lancer simultanément des millions d'attaques.

La réponse initiale à ces défis a souvent consisté en l'implémentation de systèmes automatisés de détection, comme le souligne McNeese (2012). Cependant, ces systèmes génèrent un grand nombre de fausses alertes et reposent sur des algorithmes rigides qui peuvent nuire à l'efficacité

opérationnelle. Nicholson (2016) ajoute que, malgré les avancées technologiques, les menaces en cybersécurité continuent d'évoluer, et les organisations doivent s'assurer que leur personnel comprend son rôle dans la sécurité globale.

Trouchaud (2016) explique que les systèmes de cybersécurité, bien que sophistiqués, demeurent faillibles et augmentent les risques en raison des erreurs humaines. La sécurité absolue est un mythe ; plus nous investissons dans la technologie, plus nous sommes exposés à de nouveaux risques. Ainsi, il est crucial de se détourner d'une dépendance excessive à la technologie et de réévaluer le rôle de l'humain dans la surveillance des systèmes. Nicholson (2016) affirme que la cybersécurité ne se limite pas aux outils technologiques ; la sensibilisation des employés est essentielle pour atteindre un niveau de sécurité satisfaisant.

Pour assurer une cybersécurité efficace, il est nécessaire que les tâches critiques, telles que la mise à jour des procédures de sécurité, la gestion des incidents et la sensibilisation, soient supervisées par des humains. Ce besoin de supervision humaine découle du fait que les systèmes, bien qu'automatisés, nécessitent une intervention pour garantir leur fonctionnement optimal. Ainsi, une stratégie de cybersécurité devrait intégrer à la fois des algorithmes et l'intervention humaine pour gérer ces responsabilités.

L’accent sur le facteur humain est d’autant plus pertinent car il contribue à la sécurité d’une manière que les machines ne peuvent pas. Boyce (2011) souligne que la performance humaine est essentielle à l’efficacité des processus de cybersécurité. Pour intégrer efficacement l'humain dans ces systèmes, il est nécessaire de comprendre ses rôles, ses responsabilités et les exigences associées.

Singer (2014) renforce cette idée en affirmant que la véritable bataille de la cybersécurité ne repose pas uniquement sur la technologie, mais également sur le comportement humain. Les erreurs humaines, souvent causées par une méfiance ou un manque de vigilance, continuent d'être exploitées par les cybercriminels. Ainsi, il est impératif que tous les utilisateurs, du personnel subalterne à la direction, soient régulièrement formés aux bases de la cybersécurité.

En conclusion, il est essentiel de reconnaître que doter une organisation de technologies avancées sans les compétences humaines adéquates pour gérer et évoluer avec ces systèmes compromet l'intégrité de la cybersécurité. Pour une protection optimale contre les cybermenaces, une formation continue et une sensibilisation à la cybersécurité doivent devenir des priorités stratégiques.

1.2.3 Le rôle individuel et humain en cybersécurité

Des recherches montrent que les employés représentent la principale menace humaine pour la sécurité des ressources d'information d'une organisation. Il est donc essentiel de comprendre les facteurs qui influencent les comportements conformes et non conformes en matière de cybersécurité. Parmi ces facteurs, nous identifions :

- Le comportement sur le lieu de travail et les traits de personnalité ;
- La croissance rapide de la technologie ;
- La faible sensibilisation à la sécurité de l'information ;
- Le manque de formation en cybersécurité ;
- La gestion des équipes.

McBride (2012) souligne que la conception de programmes de cybersécurité doit s'appuyer sur une compréhension approfondie des profils psychologiques des employés. Les abus d'initiés, souvent causés par des violations des politiques de cybersécurité, représentent une menace significative. Les comportements des employés peuvent être accidentels, négligents ou malveillants, et varient selon les traits de personnalité. Par conséquent, les approches de formation devraient être personnalisées en fonction de ces différences pour être réellement efficaces. La croissance rapide de la technologie de l'information a également intensifié les risques de sécurité, en particulier dans les secteurs industriel et financier.

Vance (2013) indique que les violations de sécurité sont courantes dans les entreprises où les employés enfreignent les politiques de sécurité ou s'engagent dans des comportements à risque. Les défis liés à la sensibilisation à la sécurité, à la formation et à la gestion des équipes aggravent la situation. McFadzean (2006) et Puhakainen et Siponen (2004) ont montré que des formations fréquentes et une sensibilisation accrue peuvent améliorer la conformité des employés. Inversement, Rubinstein et Francis (2008) notent que les violations des politiques de sécurité ont des effets néfastes sur la cybersécurité. Les données empiriques de Jaeger (2013) révèlent que la négligence humaine est une cause majeure des violations de données : 38% des violations de données sont dues à la perte de fichiers papier ; 27% sont dus à la négligence humaine (par exemple, la perte de dispositifs de mémoire de données) ; et 11% des violations de données sont dues au piratage.

Le rôle des dirigeants est également crucial dans l'assurance de la conformité aux politiques de sécurité. Vance (2013) met en avant que des gestionnaires peu qualifiés augmentent le risque de violations. Il propose quatre mécanismes de responsabilisation : l'identifiabilité, la sensibilisation à l'exploitation forestière, la sensibilisation à l'audit et la présence électronique.

Ces mécanismes peuvent réduire les intentions de violations et, par conséquent, les cyberattaques. Le risque de sécurité ne peut être atténué uniquement par la sensibilisation, sans une mise en œuvre efficace des règles de conformité. L'audit interne joue un rôle essentiel en veillant au respect des politiques de cybersécurité. De plus, d'autres événements extérieurs peuvent enrichir les processus de formation à la sécurité de l'information.

Pour conclure, il est crucial d'adopter des méthodes variées et adaptées pour renforcer la conformité aux politiques de sécurité, tout en tenant compte de l'effet du leadership sur le comportement des employés. La sécurité de l'information nécessite une approche globale, intégrant formation, sensibilisation et gestion efficace des ressources humaines. Stewart et Jürjens (2017) mettent en avant que la sensibilisation seule ne suffit pas ; une formation adéquate est essentielle pour résoudre les défis liés à la gestion de la sécurité de l'information.

1.2.4 Les fonctions impliquées dans la cybersécurité sont multiples et doivent coopérer

La cybersécurité représente un enjeu transversal au sein des organisations, nécessitant l'engagement de tous les niveaux hiérarchiques, au-delà du seul responsable de la sécurité.

Visner (2016) souligne l'importance de l'implication collective des dirigeants et des employés pour renforcer la sécurité des informations.

Latour (2018) identifie plusieurs fonctions clés en cybersécurité, parmi lesquelles figurent les analystes d'intrusion, les auditeurs de sécurité, les responsables de la sécurité informatique et les directeurs des ressources humaines. Chaque acteur doit être conscient de sa responsabilité dans le maintien de la sécurité des données. Les analystes de cybersécurité, par exemple, sont confrontés à des volumes d'informations considérables et doivent établir des connexions temporelles et contextuelles entre ces données. Cela requiert une coopération efficace entre les analystes à différents niveaux, soutenue par des formations appropriées, afin d’optimiser le traitement des incidents de sécurité.

Pribish (2015) renforce cette idée en affirmant que la cybersécurité est une démarche collective, impliquant gestionnaires, auditeurs et employés. La coordination est essentielle, car les cybercriminels exploitent souvent les vulnérabilités humaines, en particulier dans les petites entreprises.

Carter (2015) rappelle que la cybersécurité doit être perçue comme un principe fondamental au sein des équipes gouvernementales, où chaque membre joue un rôle crucial. Tindall (2013) ajoute que la cybersécurité va au-delà des technologies de défense, impliquant une approche centrée sur les personnes, les processus et la technologie.

Pour une sécurité accrue, Rudiger (2017) insiste sur la nécessité d'une collaboration étroite entre

les parties prenantes, afin de créer transparence et responsabilité. Jollans (2018) soutient que la prise en compte des enjeux de sécurité dans le développement technologique favorise une intégration harmonieuse des besoins de l'entreprise.

Roth (2012) évoque également l'importance de la participation active non seulement des experts en technologie, mais de tous les acteurs, y compris les utilisateurs finaux et les décideurs. Elle met en lumière le fossé existant entre les besoins en sensibilisation à la cybersécurité et les outils disponibles pour y répondre.

Hui (2010) souligne que, bien que les responsabilités en cybersécurité puissent varier, une communication efficace entre les différentes fonctions est essentielle pour éviter la redondance et améliorer la réactivité..

Salas (2012) insiste sur les éléments fondamentaux tels que coopération, communication et coordination, qui sont cruciaux dans des environnements complexes comme la cybersécurité.

Des études, comme celle de Rajivan et al (2013) montrent que le travail d'équipe en cyberdéfense améliore significativement les performances face aux alertes.

Pace (2015) propose que la création de comités interdépartementaux facilite la résolution des questions liées à la cybersécurité. Cette approche encourage également une culture de vigilance, où les employés peuvent signaler les anomalies.

Jollans (2018) affirme que la collaboration entre les équipes informatiques et de sécurité est primordiale pour optimiser les initiatives de protection des données. Une coopération étroite permet de garantir que les exigences de sécurité sont intégrées dès le développement technologique.

En somme, la cybersécurité est un effort collectif qui nécessite une coordination efficace entre diverses fonctions au sein des organisations. Cette approche collaborative est indispensable pour anticiper et contrer les menaces en constante évolution.

Conclusion intermédiaire

La cybersécurité constitue un enjeu complexe qui transcende les seules considérations technologiques, englobant des dimensions humaines, organisationnelles et sociétales. Il est impératif de comprendre que la technologie à elle seule ne peut garantir une protection efficace des systèmes informatiques. La collaboration interprofessionnelle s'avère essentielle pour assurer la sécurité des données et des infrastructures.

Étant donné que les erreurs humaines représentent fréquemment le maillon faible de la chaîne de sécurité, il est crucial de mettre en place des formations et des programmes de sensibilisation destinés aux employés afin de minimiser les risques. La responsabilité de la cybersécurité

incombe à l'ensemble de l'organisation ; chaque département—de la direction aux ressources humaines, en passant par les équipes informatiques—doit intégrer des pratiques de sécurité de l'information.

Les équipes de sécurité informatique et les services informatiques doivent œuvrer de concert pour intégrer les exigences de sécurité dès le développement technologique, tout en utilisant les ressources technologiques pour résoudre les problématiques de sécurité et en redéfinissant les conversations autour de la cybersécurité. Cette approche collaborative favorise une meilleure transparence et permet de prendre des décisions éclairées en matière de sécurité.

Il est clair que la cybersécurité ne peut être abordée de manière isolée. Pour faire face aux défis d'un environnement cybernétique en constante mutation, il est indispensable que les diverses fonctions au sein de l'entreprise collaborent étroitement. Cette partie 2.1 a permis de mettre en lumière l'importance de la coopération entre les différentes entités de l'organisation pour garantir la cybersécurité, ainsi que le rôle crucial des individus dans la supervision des tâches effectuées par les systèmes de sécurité.

1.3 L’assurance d’une cybersécurité dans les banques : enjeux et acteurs concernés

Le secteur bancaire joue un rôle central dans l'économie mondiale et fait face à des transformations majeures, tant internes qu'externes, depuis les années 1980. Parmi les forces externes, l'évolution technologique, en particulier l'essor d'Internet, a eu un impact déterminant, facilitant l'émergence de nouveaux acteurs et accroissant l'influence des clients sur les services bancaires.

L'influence d'Internet s'étend à la manière dont les services sont délivrés, engendrant une transformation significative du secteur. La cybersécurité émerge comme une préoccupation cruciale, englobant la sécurité des transactions financières en ligne. Les banques mettent en œuvre une série de mesures de sécurité, notamment des technologies de cryptage, des identifiants uniques, et des protocoles d'authentification sophistiqués, tels que des saisies aléatoires d'informations et des déconnexions automatiques après une période d'inactivité (Jayawardhena, 2000).

Les grandes institutions bancaires se tournent vers le développement de services bancaires virtuels, mobiles et sans fil pour rester compétitives. Toutefois, cette numérisation accrue expose les banques à des risques cybernétiques significatifs, tels que les virus, les logiciels malveillants, et les cyberattaques ciblées. Chaque type de menace présente des caractéristiques spécifiques nécessitant des réponses adaptées.

Les organisations bancaires doivent naviguer dans un environnement technico-économique complexe qui influence la réussite de leurs stratégies de sécurité, en tenant compte des contraintes et des normes internationales (Venkatraman, 2008).

Les cyberattaques se font de plus en plus fréquentes et sophistiquées, alimentées par des groupes criminels organisés et des réseaux de cybercriminalité. La baisse des coûts technologiques abaisse les barrières à l'entrée pour ces activités illicites, rendant plus accessible la mise en œuvre de méthodes variées pour le vol et la fraude en ligne. Parallèlement, un marché noir florissant pour les données volées encourage ces comportements criminels (Cuomo, 2014).

Face à ces défis, la coopération entre les différents acteurs du secteur est indispensable pour développer des stratégies de cybersécurité efficaces et résilientes.

1.3.1 Enjeux de la cybersécurité dans les banques

Le secteur bancaire connaît une évolution significative dans la manière dont les clients effectuent leurs transactions, avec une adoption croissante des canaux numériques tels que les services bancaires en ligne, les portefeuilles numériques et les guichets automatiques. Cette

transition numérique accroît l'exposition aux cyberattaques, pouvant entraîner des pertes financières et de réputation. La confiance des clients est alors mise en péril, accentuant ainsi les enjeux liés à la cybersécurité.

Les banques doivent désormais faire face à un défi sans précédent en matière de violations de données. Comparativement à d'autres secteurs, le secteur financier subit près de trois fois plus d'attaques cybernétiques, ce qui entraîne une hausse exponentielle des coûts liés à la cybersécurité. Les investissements dans ce domaine sont de plus en plus cruciaux : la mise en œuvre et la gestion des infrastructures de cybersécurité devraient augmenter de plus de 40 % d'ici 2025. L'utilisation croissante de la biométrie pour sécuriser les transactions et l'accès aux services bancaires témoigne d'une volonté d'adapter les systèmes de sécurité aux nouvelles menaces, tout en veillant à ne pas nuire à l'expérience client. (BDO India LLP, 2023)

En réponse à l'augmentation des cybermenaces, les régulateurs bancaires imposent des normes de sécurité plus strictes. Les principales institutions doivent désormais adopter des outils de sécurité avancés et être capables de se remettre d'une attaque dans un délai réduit. La réserve fédérale et le département du trésor incitent les banques à suivre les recommandations du *Groupe des 7 (G7)* en matière de cybersécurité, notamment l'élaboration de stratégies de sécurité de l'information et le partage d'informations avec les autorités.

Le secteur bancaire a investi massivement dans la cybersécurité, avec des dépenses atteignant 8,6 milliards de dollars cette année. Des institutions comme JP Morgan et la Banque d'Amérique illustrent cet engagement, en consacrant des budgets considérables à la lutte contre la cybercriminalité (Bhargav, 2022).

La conformité aux lois et réglementations complexes constitue un défi majeur pour les banques. Les exigences de confidentialité et de sécurité définies par la loi *Gramm-Leach-Bliley* (GLBA) et d'autres réglementations, telles que celles imposées par la Californie avec l'avis de violation de la sécurité (NSB), ajoutent une couche de complexité à la gestion des données sensibles. Les banques doivent non seulement respecter des normes strictes de sécurité, mais aussi veiller à la protection des données personnelles, en s'assurant que les informations sont cryptées pendant leur transport et leur stockage.

Les défis de conformité s'étendent également aux réglementations fédérales et étatiques concernant la conservation des données et les transactions électroniques. Les exigences légales en matière de cybersécurité obligent les banques à mettre en place des mesures de protection appropriées, tout en évaluant les risques liés à leurs pratiques commerciales et à leur technologie. Alors que la technologie de l'information devient un pilier fondamental du secteur bancaire, la nécessité de développer un cadre de cybersécurité robuste et efficace est cruciale.

Ce cadre doit non seulement se conformer aux réglementations existantes, mais aussi favoriser la confiance entre les institutions financières et leurs clients. Les défis liés à la conformité, aux coûts et à l'interaction des processus internes compliquent encore davantage la situation. L'importance d'une coopération active avec d'autres entités financières est indéniable pour assurer la conformité et renforcer les capacités de défense contre les cybermenaces (Mohammed, 2017).

Une étude de l'Institut de génie logiciel *Carnegie Mellon* révèle que de nombreuses attaques internes dans le secteur bancaire résultent de l'exploitation de faiblesses organisationnelles et non nécessairement de compétences techniques avancées. Cela souligne la nécessité d'une approche systémique de la cybersécurité, intégrant la culture organisationnelle, les pratiques commerciales et les politiques en matière de sécurité (Randazzo, 2005).

Face à ces défis, il est impératif que les banques mettent en œuvre une stratégie proactive en matière de cybersécurité, notamment par le recrutement de spécialistes qualifiés et la mise à jour continue de leurs systèmes. Les défis internes, tels que l'inadéquation des opinions d'experts et les coûts élevés associés à l'emploi de spécialistes, doivent également être abordés pour garantir la résilience face aux cybermenaces (Pavlovska, 2018).

1.3.2 Défis rencontrés par les acteurs dans le domaine de la cybersécurité

La cybersécurité requiert une collaboration efficace entre divers acteurs pour assurer une protection adéquate. Cependant, plusieurs facteurs entravent la mise en place d'une stratégie collective et raisonnée en matière de sécurité numérique.

1.3.2.1 Manque aux Obligations : évasion de Responsabilité

Au sein des entreprises, la fonction d'audit interne joue un rôle clé dans la coordination des efforts de gestion des risques liés à la cybersécurité. Un rapport du Réseau canadien des comités d'audit (RCCA) souligne que la fonction d'audit doit être dotée de professionnels compétents pour évaluer les risques émergents. Cependant, une enquête d'Ernst & Young révèle que 68 % des répondants estiment que leur entreprise confie à l'audit interne la tâche d'évaluer la sécurité de l'information, bien que des doutes persistent quant à leurs compétences techniques. Les responsabilités de gestion des risques liés à la sécurité de l'information demeurent floues, chacun s'attendant à ce que d'autres prennent en charge ces questions, ce qui peut conduire à une déresponsabilisation au sein des équipes (Réseau Canadien des comités d'audit, 2013).

1.3.2.2 Pénurie de talents

La pénurie de professionnels qualifiés en cybersécurité est un enjeu majeur. En 2016, plus d'un million de postes demeuraient vacants, et des études montrent que 61 % des entreprises

françaises prévoyaient d'augmenter leurs effectifs spécialisés. Pourtant, seulement 44 % des informaticiens affirment posséder des compétences de base en cybersécurité, tandis que 56 % se jugent incompétents face aux défis actuels. Cette lacune en compétences techniques se traduit par des difficultés pour les entreprises à recruter des experts en cybersécurité, exacerbant ainsi le risque de cyberattaques. (Soussi, 2022)

1.3.2.3 Manque de compétences clés

Nous avons exposé le problème de juridiction qu'existe par manque de responsabilité et de personnes experts quand il s'agit de garantir en direct la cybersécurité. Une étude sur les informaticiens interrogés sur la sécurité des systèmes informatiques : 44% annoncent disposer des compétences de base en matière de cyber sécurité. Les autres 56% se déclarent incompétents et insuffisamment armés pour faire face aux défis cyber. Les entreprises manquent de talents sur la dimension cyber. Par contre, ceux qui développent des systèmes informatiques se qualifient dans leur majorité comme incompétents pour traiter ces questions.

Il faut ajuster la position des RSSI dans l'entreprise pour devenir exécutifs. 82% d'eux se déclarent malheureux dans leur poste. Ils se sentent insatisfait dans leur travail puisqu'ils s'estiment à être les boucs émissaires des défaillances et seuls dans la gestion des incidents. Ils doivent trouver un équilibre entre leur devoir d'alerte et celui de diplomatie. C'est pourquoi ils se retrouvent malheureux dans leur métier signe que la gestion de la cyber sécurité n'est qu'une gestion à court terme (Trouchaud, 2018).

Le problème des RSSI est qu'ils sont toujours en chasse à la recherche du dernier pare-feu à la mode. Les RSSI sont donc qualifiés comme des boucs émissaires désignés pour tous les problèmes cyber. Ils sont en stress permanent : soit l'attaque a lieu et ils seront jugés coupable pour ne pas l'avoir vue venir ou signaler rapidement, soit l'attaque n'a pas lieu, les systèmes sont bien protégés et ils seront malmenés sur des différents projets digitaux à livrer. En réalité, les alertes déclarées par les RSSI sur les systèmes de les mettre à jour ou de les modifier ne sont que rarement entendues par la direction générale puisque aucune attaque n'est à déplorer (Trouchaud, 2018).

C'est impossible de surarmer une entreprise avec des tas de systèmes de sécurité sans avoir les compétences humaines nécessaires pour intégrer, gérer et faire évoluer ces systèmes afin de ne pas répéter les mêmes erreurs lors d'une prochaine attaque. Les entreprises doivent donc envisager une nouvelle façon pour gérer la cyber sécurité.

1.3.2.4 Lacunes dans les politiques de gestion des ressources humaines

Les départements des ressources humaines n'adoptent pas toujours une approche proactive pour soutenir la cybersécurité.

McFadzean (2006) souligne que la haute direction a un rôle crucial dans la sensibilisation des employés à la sécurité de l'information. Par exemple, *BNP Paribas et Société Générale* mettent en œuvre des stratégies pour attirer et former des talents, mais cela reste insuffisant face à la pénurie persistante. La direction des ressources humaines doit non seulement attirer des candidats, mais aussi leur offrir des carrières attrayantes, y compris des grilles de rémunération compétitives, pour renforcer la sécurité dans le secteur bancaire. (L'assurance en mouvement, 2022)

Ces défis soulignent la nécessité d'une approche collaborative et intégrée pour faire face aux risques de cybersécurité, où chaque acteur a un rôle essentiel à jouer.

1.3.3 Rôle des différentes parties pour assurer la cybersécurité

Afin de dissiper les confusions de responsabilités entre les auditeurs internes, les responsables des systèmes d'information (TI) et les gestionnaires, il est crucial de clarifier les rôles de chaque fonction en matière de cybersécurité.

1.3.3.1 Rôle de l'audit interne

L'audit interne joue un rôle essentiel dans le maintien de l'intégrité des dispositifs de cybersécurité au sein des organisations. Idéalement, les plans de cybersécurité sont conçus, testés et mis en œuvre avec rigueur. Cependant, l'audit interne a pour mission de vérifier l'efficacité de ces contrôles, d'apporter une assurance à la direction et au conseil d'administration quant à leur robustesse, et de signaler toute défaillance avant qu'une crise réelle ne survienne.

Chambers (2017) identifie quatre domaines principaux où l'audit interne intervient :

- Assurer la préparation et la réponse : l'audit interne teste les plans de cybersécurité, la continuité des activités et la reprise après sinistre, identifiant les lacunes avant qu'elles ne causent de réels dommages.
- Évaluer les risques et les efforts d'atténuation : la communication avec la direction sur les risques cyber est primordiale. L'audit interne aide à comprendre les risques et à s'assurer que les mesures adéquates sont mises en œuvre.
- Collaborer avec les responsables de TI : le risque cybernétique étant avant tout un risque commercial, l'audit interne renforce les liens avec les TI pour garantir des défenses efficaces.
- Faciliter la communication et la coordination : grâce à sa vue d'ensemble, l'audit interne encourage la coopération entre les parties prenantes afin d'assurer une gestion harmonisée des cyber risques.

Les audits certifiés sont particulièrement efficaces pour remédier aux échecs en assurant la

sécurité entre les différentes entités, alors que les audits de base manquent souvent d'impact. La rigueur des contrôles doit être adaptée au contexte spécifique, en tenant compte des interconnexions et de l'efficacité des investissements en cybersécurité (Bohme, 2012).

Il est également essentiel que les conseils d'administration comprennent l'exposition aux cyber risques, même si cette situation peut parfois être floue. Les comités d'audit et de conformité se tournent vers l'audit interne pour obtenir une assurance sur la gestion de ces risques (Kahyaoglu, 2018).

Cependant, plusieurs défis persistent. Premièrement, les rapports techniques sur la cybersécurité peuvent être complexes et déconnectés des objectifs stratégiques de l'entreprise. Deuxièmement, l'assurance indépendante est souvent insuffisante, car les départements TI ne peuvent pas toujours fournir l'objectivité nécessaire. Les auditeurs internes, grâce à leur indépendance, jouent un rôle vital en apportant cette assurance. L'IIA souligne l'importance de l'indépendance et de l'objectivité des auditeurs internes, identifiant des menaces potentielles à leur intégrité et des garanties à mettre en place.

Un autre enjeu est la sensibilisation accrue aux cyber risques, demandée par les récents événements médiatiques et les réglementations émergentes (AHIA et Deloitte, 2017).

Kahyaoglu (2018) insiste sur la responsabilité de la direction et du conseil dans la gestion des risques, soulignant que l'audit interne doit être considéré comme un fournisseur d'assurance indépendant et essentiel pour la bonne gouvernance.

Pour renforcer leur rôle, les auditeurs internes doivent acquérir des compétences en audit informatique et se tenir informés des évolutions réglementaires et des tendances de l'industrie. La documentation de l'audit exige des connaissances approfondies en technologie de l'information pour évaluer efficacement les programmes de cybersécurité (IIA, 2017).

Une expertise technique en sécurité de l'information améliore également les relations avec les équipes de sécurité informatique, rendant la gestion des cybers risques plus efficace (Steinbart, 2012).

Enfin, l'audit interne doit jouer un rôle central dans la supervision de la cybersécurité en établissant des relations de collaboration avec divers responsables au sein de l'organisation. Cela permettra de mieux comprendre les cyber risques et d'améliorer la culture de cybersécurité globale (IIA, 2017).

1.3.3.2 Rôle des responsables informatiques et des RSSI

Les RSSI sont confrontés à des menaces internes et externes, ainsi qu'à des exigences législatives et réglementaires qui influencent leurs options stratégiques, notamment dans les

secteurs sensibles comme la finance, l'énergie et les télécommunications. Un défi majeur demeure : la non-conformité des employés aux politiques de sécurité de l'information. Souvent, ces derniers sont perçus comme les principaux obstacles à la sécurité, en raison de comportements influencés par des politiques mal conçues (Kolkowska, 2017).

Les départements informatiques doivent également gérer la formation et l'attribution des rôles au sein de leurs équipes, englobant des tâches variées telles que l'exploitation de systèmes, le développement de logiciels et le support technique (Schmidt, 2015).

La sécurité informatique, qui s'inscrit dans le cadre plus large des technologies de l'information, est essentielle pour protéger les systèmes contre les cybermenaces. Elle peut être considérée comme un synonyme de cybersécurité, bien que cette dernière se concentre spécifiquement sur la protection des données électroniques et l'accès non autorisé via Internet (Crawley, 2017).

Les professionnels de la sécurité informatique, ainsi que les auditeurs, collaborent souvent pour assurer la protection des données, bien qu'il arrive qu'ils ne soient pas employés par la même entreprise (Buchy, 2016).

Trouchaud (2016) révèle que près de la moitié des informaticiens se sentent incompétents face aux défis de la cybersécurité, ce qui souligne une déresponsabilisation et un manque de compétences dans le secteur.

Pour maintenir une cybersécurité efficace, il est impératif que les responsables de TI collaborent étroitement avec la direction et les auditeurs internes, renforçant ainsi la posture de sécurité au sein de l'organisation.

1.3.3.3 Rôle des managers

La sécurité ne se limite pas à une problématique technique, mais constitue également un enjeu de gestion. Elle s’articule autour de trois piliers fondamentaux : les infrastructures critiques, l’organisation et la technologie. Les infrastructures critiques, en particulier, échappent au contrôle direct des organisations et sont la cible d’un nombre croissant d'attaques, tant cybernétiques que physiques, menées par des acteurs aux motivations variées. Il appartient donc à la direction d’établir un équilibre entre ces trois dimensions. Les dirigeants sont responsables de la mise en place d'un dispositif de cybersécurité, une responsabilité qui incombe également aux managers au sein des entreprises (Trouchaud, 2016).

1.3.3.3.1 Rôle théorique des dirigeants

Les dirigeants, selon Brisch (2017), portent une responsabilité significative concernant les risques informatiques, étant tenus de protéger les intérêts de leur organisation en conformité avec les lois et règlements, notamment en matière de protection des données. Les tribunaux peuvent engager leur responsabilité personnelle si les normes de sécurité informatique ne sont

pas respectées. Ainsi, il est essentiel que la haute direction prenne l'initiative d'élaborer des politiques de sécurité équilibrées, car les échecs en matière de sécurité relèvent souvent de la gestion plutôt que de la technique (Dutta, 2002).

La cybersécurité est devenue une préoccupation cruciale pour les conseils d'administration, comme l'indique le PDG de *Deutsche Bahn*, Rüdiger Grube, soulignant que ce n'est pas seulement une responsabilité des départements informatiques. Bien qu'il n'existe pas de cadre juridique clair sur la cybersécurité, elle est intégrée à la gestion des risques, et les dirigeants doivent y participer activement pour éviter toute responsabilité personnelle (Gercke, 2017). Cependant, un défi majeur demeure : intégrer efficacement les membres des conseils d'administration dans la stratégie de cybersécurité, ce qui est souvent entravé par le manque de directives claires.

Peusquens (2017) identifie les lacunes en matière de sécurité informatique comme un point vulnérable, nécessitant une collaboration étroite entre auditeurs internes, managers et responsables de TI pour créer une transparence et établir des responsabilités claires. La cybersécurité doit être perçue comme essentielle plutôt que comme un simple ajout à l'informatique, et sa mise en œuvre doit être simple pour garantir son efficacité.

À mesure que les entreprises prennent conscience de l'ampleur des cyberattaques, il est crucial d'informer la direction et les managers de manière précise, comme le souligne Donaldson (2015). Une communication efficace peut aider à alléger la charge des employés et à garantir une réponse adéquate.

1.3.3.3.2 La réalité : une immaturité des dirigeants ?

Les entreprises reconnaissent l'existence des cyberrisques, mais montrent une réticence à les affronter de manière proactive. La plupart d'entre elles adoptent une approche défensive limitée, souvent incarnée par une petite équipe de deux ou trois personnes, qui tente de faire face à une menace globale par le biais de stratégies de cybersécurité disparates. Cette gestion du risque peut conduire à des décisions hâtives, souvent prises sous l'influence d'émotions fortes, entraînant un éloignement des principes fondamentaux de la gestion d'entreprise. Ce phénomène s'explique en partie par le fait qu'une seule personne est souvent désignée responsable de la cybersécurité.

Une étude réalisée par PwC révèle que 85 % des PDG admettent ne pas savoir comment leur entreprise est structurée pour faire face aux menaces cybernétiques, et 65 % d'entre eux ne savent pas où se situent leurs données stratégiques. Cela met en lumière une immaturité significative et une compréhension limitée des enjeux globaux de la cybersécurité. Dans leurs investissements numériques, les dirigeants tendent à privilégier des solutions tactiques à court

terme, en délaissant une vision stratégique globale nécessaire à une défense efficace contre les cyberattaques. Cette situation témoigne d'un manque de considération pour le risque cyber, souvent marqué par un sous-investissement chronique dans ce domaine.

Malgré la gravité des incidents, tels que la crise engendrée par WannaCry, certains dirigeants estiment encore que leur entreprise peut se défendre seule contre des menaces asymétriques, multiples et imprévisibles. Reconnaître que personne ne peut assurer la cybersécurité de manière isolée ne devrait pas être perçu comme un signe de faiblesse, mais plutôt comme une opportunité de repenser les stratégies de défense. Si un manager est censé jouer un rôle clé dans la gestion des cyberrisques, il ne peut agir efficacement sans collaboration. L'omniscience attribuée à une seule personne dans la gestion des risques constitue un danger majeur, en particulier dans le domaine de la cybersécurité (Trouchaud, 2018).

Par ailleurs, les dirigeants des banques se montrent culturellement et pratiquement mal préparés à affronter les cyberrisques. Ils se retrouvent souvent démunis lorsqu'il s'agit de concevoir des stratégies de défense face à des adversaires non commerciaux, n'ayant reçu aucune formation dans ce domaine durant leur parcours académique ou professionnel. Nous soutenons que la cybersécurité doit reposer sur une coopération étroite entre les managers, les responsables de la sécurité et les auditeurs internes, à tous les niveaux et dans tous les départements de l'organisation.

1.3.4 Des conflits propres à compromettre la coopération

Plusieurs contraintes entravent la coopération entre les acteurs de la cybersécurité dans le secteur bancaire, notamment la pénurie de talents, le manque de compétences, l'immaturité des dirigeants, et l'absence de politiques de ressources humaines adaptées. Ces défis entraînent des problèmes de juridiction et des conflits interprofessionnels qui compromettent la collaboration nécessaire pour garantir la sécurité.

La cybersécurité ne se limite pas à l'informatique ; elle requiert une approche holistique intégrant la sécurité physique, la préparation aux catastrophes et la protection des infrastructures critiques. Cette intégration nécessite une coordination entre militaires, forces de l'ordre, auditeurs, responsables de TI, et gestionnaires. L'élaboration de politiques de sécurité légitimes, fondées sur un consensus parmi les parties prenantes, est essentielle pour établir des normes pratiques que tous doivent suivre. Ces normes orientent les objectifs de sécurité et guident l'évaluation des risques, suivie par des audits pour garantir la conformité et l'efficacité des pratiques établies (Goodyear, 2010).

McNeese (2011) souligne que la détection des cybermenaces requiert un collectif d'analystes et

une technologie variée pour surveiller efficacement les réseaux. L'interdépendance entre l'analyse humaine et la technologie est cruciale pour traiter les informations sur les menaces.

Rajivan (2017) ajoute que la nature dynamique des attaques nécessite une équipe diversifiée de professionnels pour détecter et répondre à des menaces variées, incluant des techniques non techniques comme l'ingénierie sociale. Ainsi, une compréhension collective des menaces est indispensable, car les informations pertinentes sont souvent dispersées et nécessitent des contributions variées pour une réponse efficace.

Guenther (2014) note que la collaboration aide à surmonter la conscience limitée des individus, permettant une vision d'ensemble indispensable face aux incidents de sécurité.

Fourie (2014) renforce cette idée en soulignant que le traitement adéquat de la cybersécurité exige confiance et collaboration entre tous les acteurs concernés.

Cependant, l'acceptation de l'audit interne par les managers demeure insuffisante, due à une méconnaissance de son rôle, souvent confondu avec d'autres fonctions, et à un manque de pression pour investir dans cette fonction. Cette résistance est exacerbée par une culture organisationnelle autoritaire, reléguant les auditeurs internes à des rôles secondaires et les privant de l'influence nécessaire pour améliorer la cybersécurité (Benabid, 1995).

Les responsables de TI, quant à eux, peuvent être réticents à collaborer avec les auditeurs, ce qui nuit à la coopération nécessaire pour une cybersécurité efficace. Ce manque de coopération découle souvent d'un conflit d'identité professionnelle, où chaque groupe défend ses prérogatives. La construction de l'identité professionnelle des auditeurs internes et des responsables de TI est influencée par leurs relations sociales et leur environnement de travail, rendant les conflits d'identité inévitables (Beaudry, 2011).

Devenir manager peut être considéré comme un rite de passage sanctionnant la modification de l'identité professionnelle de l'auditeur. Ce rite de passage déstabilise mais forge aussi l'identité amenant à se dés-identifier du junior pour s'identifier progressivement à l'associé. L'auditeur ne peut être un manager qu'en modifiant son identité professionnelle. Ils doivent aussi dépasser certains stéréotypes négatifs qui entourent leur métiers tel que le rattachement hiérarchique, les personnes interroges, les rôles, la situation financière de l'entreprise… (Legalais, 2014)

Pour comprendre ces conflits, Abbott propose d'examiner des processus historiques qui mènent à des déséquilibres dans les revendications de compétence. Les conflits juridiques sont donc le reflet de tensions exacerbées durant les périodes de transformation professionnelle, appelant à une collaboration renforcée pour garantir une cybersécurité efficace et intégrée (Covaleski, 2003).

Conclusion intermédiaire

Avec la transformation numérique et l'augmentation des risques de cyberattaques, la cybersécurité est devenue un enjeu crucial pour le secteur bancaire. Les violations de données et les accès non autorisés entraînent des pertes financières et nuisent à la réputation des banques, ce qui justifie une hausse significative des investissements dans la cybersécurité.

Cependant, plusieurs obstacles entravent cette démarche. La pénurie de talents en cybersécurité complique le recrutement et la rétention des experts nécessaires. Par ailleurs, l'absence de clarté quant aux responsabilités en matière de cybersécurité peut entraîner une déresponsabilisation au sein des organisations.

Pour garantir une cybersécurité efficace, une collaboration entre toutes les parties prenantes — auditeurs internes, responsables informatiques, managers et direction des ressources humaines — est essentielle. Toutefois, des conflits et des tensions entre ces fonctions peuvent nuire à cette coopération. Le statut professionnel des auditeurs internes est également un facteur déterminant ; ceux-ci doivent adapter leur rôle et dépasser les stéréotypes négatifs associés à leur profession pour favoriser une meilleure synergie.

Ainsi, il est évident que la cybersécurité dans le secteur bancaire nécessite une approche collective, rationnelle et humaine pour répondre aux défis croissants de la cybercriminalité. Les banques doivent investir dans la formation, promouvoir la collaboration interprofessionnelle et établir des responsabilités claires pour renforcer leur résilience face aux menaces cybernétiques.

Synthèse du chapitre 1 : enjeux et acteurs de la cybersécurité bancaire

Dans ce chapitre, nous avons souligné l'importance cruciale de la cybersécurité dans un monde de plus en plus connecté. Cependant, il est essentiel de reconnaître que la cybersécurité ne se limite pas à des considérations techniques ; elle est profondément liée aux dimensions humaines et organisationnelles. En effet, l'erreur humaine est souvent la faille la plus significative dans la chaîne de sécurité, ce qui met en avant la nécessité de former et de sensibiliser les employés.

La collaboration interprofessionnelle émerge comme un pilier fondamental d'une cybersécurité efficace. Les parties prenantes, y compris la direction, les ressources humaines, les responsables informatiques et les auditeurs internes, doivent s'unir pour intégrer les pratiques de sécurité dans l'ensemble de l'organisation. Cette approche collaborative permet d'adopter une gestion proactive des risques et de répondre plus efficacement aux menaces croissantes dans le cyberespace.

La cybersécurité est particulièrement critique dans le secteur bancaire, où les enjeux financiers et réputationnels sont considérables. Les banques doivent donc investir significativement dans la protection de leurs systèmes et données tout en établissant des responsabilités claires au sein de leurs structures.

En somme, ce chapitre a mis en lumière la cybersécurité comme un défi en constante évolution, nécessitant une combinaison de technologies avancées, de ressources humaines compétentes et d'une coopération étroite entre toutes les parties prenantes. Seule une approche collective, rationnelle et humaine pourra faire face aux menaces croissantes du monde numérique.

CHAPITRE 2.

L'IDENTITE PROFESSIONNELLE COMME PRISME DE COMPREHENSION DES RELATIONS INTERPROFESSIONNELLES

Sommaire du chapitre 2. L'identité professionnelle comme prismes des compréhensions des relations interprofessionnelles

2.4 Le conflit juridictionnel a priori des auditeurs internes et des responsables de sécurité informatique

2.4.1 La notion de juridiction

2.4.2 La lutte pour le contrôle des connaissances

2.4.3 L'échec de la revendication juridictionnelle

2.4.4 Le rôle des parties prenantes et de l'environnement juridique

2.4.5 Dynamiques des sources internes et externes

2.4.6 Règlements juridictionnels

Conclusion intermédiaire

Synthèse du chapitre 2 : Relations et dynamiques identitaires au sein de la cybersécurité

2. L’identité professionnelle comme prisme des compréhensions des relations interprofessionnelles

Dans le chapitre précédent, nous avons exploré l'interaction complexe des facteurs humains, juridiques, techniques et commerciaux dans le domaine de la cybersécurité. Cependant, cette interaction ne garantit pas nécessairement une collaboration efficace ou une confiance mutuelle entre les parties prenantes. Nous nous proposons ici d’examiner ces dynamiques à travers le prisme du conflit d’identité, qui peut engendrer des tensions de juridiction entre les différentes professions concernées.

Mayer (2009) souligne que la gestion des conflits est influencée tant par des réalités externes qu'internes, notamment les valeurs personnelles et la hiérarchisation des identités. La réflexion sur soi-même et sur autrui peut ainsi faciliter une gestion constructive des conflits. Dans cette optique, l’identité professionnelle apparaît comme un facteur déterminant dans les interactions interprofessionnelles liées à la cybersécurité, influençant les comportements de coopération ou de conflit.

Ivanova et Bikmetova (2017) mettent en lumière le rôle crucial de la cognition sociale et de l’identité de soi dans la dynamique conflictuelle. Leur recherche montre que le type d’identité des individus affecte leurs comportements en situation de conflit. Les employés dont l’identité professionnelle est claire et mise à jour tendent à privilégier des stratégies de concurrence et de coopération, tandis que ceux ayant une identité plus complexe choisissent souvent des stratégies de compromis et de collaboration. Cette distinction souligne l'importance de l'identité dans la gestion des conflits, notamment au sein d'équipes composées de professionnels qualifiés.

Ce chapitre vise à démontrer que l’identité professionnelle des acteurs de haut niveau, bien qu'elle puisse générer des conflits, ouvre également des possibilités de coopération. Nous appliquerons cette analyse à deux fonctions spécifiques dans le contexte de la cybersécurité : les auditeurs internes et les responsables de la sécurité informatique.

Nous structurerons cette partie en quatre sections. La première se concentrera sur l’identité et l’identité professionnelle sous l’angle des juridictions, afin d'éclairer les origines des conflits et les possibilités de coopération. La deuxième section traitera de la profession d’audit interne, en examinant sa légitimité et sa dynamique identitaire à travers la littérature. La troisième section adoptera une approche similaire pour la profession de responsable de sécurité informatique. Enfin, la quatrième section abordera l'audit des systèmes d'information spécialisés, en tant que source de conflit, pour mieux comprendre les enjeux de coopération entre ces deux professions.

2.1 L’identité professionnelle : cadres d’analyses retenus

L’identité est une notion complexe et multidisciplinaire. Depuis la loi Sarbanes-Oxley, les auditeurs internes ont vu leur rôle évoluer, devant jongler entre la préservation de leur propre identité professionnelle et celle des employés qu’ils conseillent sur l’amélioration des systèmes de contrôle internes (Akerlof, 2010).

Cela soulève la question de savoir si ces identités multiples améliorent ou nuisent à l’évaluation des systèmes de contrôle interne, surtout en ce qui concerne la cybersécurité dans les banques. Parallèlement, les responsables informatiques investissent des années pour devenir des experts, ce qui influence également leur identité, étant donné l'importance du travail dans la vie adulte (Webb, 2015).

Nous examinerons la notion d'identité et sa construction professionnelle, en tenant compte des enjeux de juridiction qui peuvent engendrer des conflits entre auditeurs internes et responsables de sécurité informatique.

2.1.1 La notion d’identité : entre deux visions et plusieurs paradoxes

Les études sur l'identité se retrouvent dans des disciplines variées comme la psychologie, la sociologie et la théorie des organisations. Drouin-Hans (2006) affirme que l'identité est difficile à définir de manière exhaustive. Elle soulève plusieurs paradoxes, notamment les questions sur la définition de soi par rapport au regard d'autrui et la stabilité de l'identité au fil du temps.

Ainsi, l'identité peut être vue comme un ensemble de représentations et de sentiments qu'un individu développe à propos de lui-même, en interaction avec son environnement (Tap et Lecomte, 2016).

Nous nous concentrerons sur deux positions théoriques principales concernant l'identité : l'essentialisme et le nominalisme.

2.1.1.1 L’identité dans une vision essentialiste

L'approche essentialiste définit l'identité comme stable et intrinsèque, avec une essence constante tout au long de la vie (Tap, 2005). Cette perspective postule que chaque individu possède des caractéristiques fondamentales qui ne changent pas, ce qui renforce l'idée de différences spécifiques entre les individus. L’identité est ainsi vue comme un reflet de la personnalité fondamentale et des attributs authentiques (Tap et Lecomte, 2016).

Bourdieu offre une lecture sociale de l'identité, où elle est façonnée par des capitaux (économique, culturel, social, symbolique) et par l’habitus, qui englobe les dispositions acquises au cours de la socialisation.

Pour Bourdieu (2015), l’habitus joue un rôle central dans la construction identitaire, reflétant

une position sociale et des pratiques intégrées, favorisant ainsi la continuité de l'identité individuelle.

2.1.1.2 L'identité dans une vision nominaliste

À l'inverse, la perspective nominaliste considère l'identité comme un processus dynamique et socialement construit, évoluant au gré des expériences et interactions (TAP, 2005 ; Osty, 2002). Selon cette vision, les individus adaptent leur identité selon le contexte et les relations interpersonnelles, ce qui les pousse à se redéfinir en permanence. Dubar (2015) introduit les concepts d'*« identités pour soi »* et *« identités pour autrui »*, soulignant que l'identité dépend non seulement de l'auto-perception mais également du regard des autres.

Goffman (2017) approfondit cette idée, affirmant que l'identité émerge des interactions sociales et des mises en scène dans lesquelles les individus cherchent à contrôler leur image. Contrairement à une identité innée, Goffman voit l'identité comme le résultat de processus sociaux, où l'individu construit une face à travers ses interactions, soumise à l'évaluation des autres.

2.1.1.3 L'identité : un facteur clé dans l'analyse des interactions interprofessionnelles en cybersécurité

L'identité, qu'elle soit considérée sous l'angle essentialiste ou nominaliste, joue un rôle crucial dans la compréhension des relations interprofessionnelles, notamment pour les auditeurs internes et les responsables de sécurité informatique. L'identité professionnelle, construite à travers des dynamiques sociales et culturelles propres à chaque domaine, constitue un cadre analytique essentiel pour saisir les enjeux sous-jacents des interactions interprofessionnelles. Elle façonne non seulement les perceptions individuelles, mais aussi les rapports de pouvoir, la répartition des responsabilités et les priorités divergentes entre les différents acteurs. Dans le contexte de la cybersécurité, ces dimensions identitaires influencent directement la qualité des collaborations et peuvent soit renforcer, soit fragiliser les dynamiques de coopération (Croft, 2015).

2.1.2 La construction de l'identité professionnelle

Cette partie se concentre sur la construction de l'identité professionnelle, un processus crucial façonné par les interactions humaines au sein du lieu de travail (Sainsaulieu, 1988).

Comprendre comment les individus se perçoivent dans leur environnement professionnel et comment ils communiquent cette perception est essentiel. L'identité professionnelle contribue à la qualité de vie au travail et est particulièrement influencée par la pression de l'hyper compétitivité, où les nouvelles générations ne sont pas prêtes à sacrifier leur identité personnelle

sans raison valable.

Pour aborder cette thématique, nous commencerons par définir et caractériser l'identité professionnelle, avant d'explorer le processus de construction identitaire et son impact sur le secteur bancaire, un domaine soumis à des pressions éthiques, juridiques et d'image.

2.1.2.1 Conceptualisation de l'identité professionnelle : définitions et perspectives

L'identité professionnelle, qui fait partie intégrante de l'identité individuelle, est un concept complexe souvent difficile à définir dans les sciences sociales (Dubar, 2015). Renaud Sainsaulieu, dans son ouvrage de référence « L'identité au travail » (1977), définit l'identité professionnelle comme la manière dont les individus s'identifient à des groupes et à des rôles au sein de leur milieu professionnel. D'autres chercheurs, comme Dubar (2015), distinguent les formes identitaires communautaires de celles sociétaires, qui sont influencées par l'appartenance à divers groupes professionnels.

Fray (2010) considère que l'identité professionnelle résulte d'un processus d'identification à des collectifs. Ce processus est à la fois personnel et structurel, impliquant une reconnaissance des compétences au sein de l'organisation (Sainsaulieu, 1988). Selon Fray et Piccolo (2010), trois éléments essentiels constituent l'identité professionnelle : la perception objective du monde du travail, les relations interpersonnelles et l'histoire professionnelle de l'individu.

La légitimité professionnelle, souvent liée à l'identité, est la reconnaissance de la capacité d'un individu à agir dans un cadre donné. Cette légitimité repose sur la reconnaissance sociale et le respect des normes de la profession (Bouquet, 2014). En effet, la légitimité d'une identité professionnelle dépend de la reconnaissance par les pairs et des attributs personnels de l'individu (Guéguen, 2014).

Pour mieux comprendre la formation de l'identité professionnelle, il est essentiel d'explorer le rôle déterminant de la socialisation dans ce processus.

2.1.2.2 L'impact de la socialisation sur la formation de l'identité professionnelle

La construction de l'identité est un processus dynamique qui débute dès l'enfance et se poursuit tout au long de la vie. La socialisation, tant primaire que secondaire, joue un rôle crucial dans cette évolution (Dubar, 2015).

La socialisation primaire, au sein de la famille et des groupes d'enfants, façonne les premières perceptions de soi, tandis que la socialisation secondaire, en milieu professionnel, enrichit l'identité en intégrant de nouvelles normes et valeurs. Dans le contexte professionnel, la socialisation implique l'acquisition des caractéristiques sociales d'un groupe (Dubar, 2015). Hughes identifie trois mécanismes de la socialisation professionnelle : l'immersion dans la culture professionnelle, l'opposition entre modèle idéal et réalité du travail, et l'ajustement de

soi face aux choix de carrière. Cette socialisation est réciproque, les interactions modifiant continuellement les postures des individus (Bordes, 2013).

Une fois ces bases posées, il est pertinent d'examiner comment le processus de catégorisation et d'identification influence l'émergence d'une identité positive.

2.1.2.3 Processus de catégorisation et d'identification : implications pour l'émergence d'une identité positive

L'identité est façonnée par un processus de catégorisation qui permet aux individus de se situer dans leur environnement social (Tajfel, 1986). La catégorisation permet à l'individu de donner un sens à l'environnement social et de se faire une place en son sein (Walsh, 2008).

Cette catégorisation facilite l'identification de soi et des autres, en utilisant des classifications fournies par la société (Dubar, 2015).

Les individus s'auto-catégorisent à différents niveaux, ce qui influence leur identité sociale. La théorie de l'identité sociale postule que les individus construisent leur identité en se comparant à d'autres groupes, ce qui les incite à rechercher des appartenances qui renforcent leur estime de soi (Tajfel, 1986). Dans ce cadre, l'identité professionnelle est construite à partir de l'appartenance à des groupes qui permettent d'atteindre une identité sociale positive (Walsh, 2008). Les études montrent que la construction d'une identité professionnelle positive repose sur divers critères : des qualités éthiques, une évaluation subjective favorable, et une complémentarité des multiples facettes de l'identité (Dutton, 2010).

Cette recherche d'identité positive est essentielle pour naviguer dans les transitions professionnelles et maintenir une image de soi cohérente et valorisée. Pour approfondir cette dynamique, nous examinerons comment l'identité professionnelle est le résultat d'une double transaction entre l'individu et son environnement.

2.1.2.4 L'identité professionnelle comme résultat d'une double transaction

Erikson (1993) décrit l'identité comme un processus complexe, ancré à la fois dans l'individu et sa culture, façonné par des crises et des ruptures, surtout durant l'enfance. L'identité ne se limite pas à une simple accumulation d'identifications, mais évolue également durant l'adolescence, période où des identifications sont abandonnées au profit de nouvelles. Il souligne que le sentiment d'identité repose sur le soutien d'un groupe social, qu'il s'agisse de la classe, de la nation ou de la culture, et que l'identité se construit à travers l'interaction entre l'individu et les perceptions collectives.

Mead (1999) renforce cette perspective en affirmant que le Soi est constitué d'une composante sociologique (le Moi) et d'une composante personnelle (le Je), dont l'interaction définit l'identité. La formation de l'identité s'opère dans le cadre des interactions sociales, chaque

individu se définissant en rapport avec les autres.

Dubar (2015) considère l'identité comme un processus en constante évolution, influencé par des socialisations successives et par les jugements d'autrui. Il met en avant la coexistence de deux processus de socialisation : le processus biographique, qui lie l'identité à l'histoire personnelle, et le processus relationnel, qui la connecte aux interactions significatives. Cette approche de la double transaction suggère que l'identité professionnelle émerge à l'intersection de ces deux dimensions, qui, bien que distinctes, sont inextricablement liées. La dimension biographique renvoie à l'identité pour soi, c'est-à-dire à la façon dont l'individu se perçoit, influencée par son histoire personnelle et les identités héritées. En revanche, la dimension relationnelle concerne l'identité pour autrui, définie par les perceptions et les étiquetages sociaux. Erving Goffman (Goffman, 1975) évoque l'identité virtuelle, notion qui reflète comment autrui peut caractériser une personne à partir de ses attributs. Les interactions professionnelles créent un cadre où l'individu doit naviguer entre son identité incorporée et celle attribuée par les autres, souvent influencée par des relations de pouvoir au sein des institutions (Dubar, 2015).

Ainsi, la construction de l'identité professionnelle se caractérise par une double transaction entre l'individu et son environnement, mêlant passé et avenir dans un contexte en constante évolution. L'identité se construit donc à travers une dynamique de négociation entre l'image personnelle, l'image souhaitée et l'image renvoyée par autrui, illustrant un processus identitaire complexe qui englobe le Moi, le Nous et les autres (Fray, 2010).

Nous soulignerons que l'identité pour soi et l'identité pour autrui peuvent diverger et même être contradictoires. En effet, le concept d'identité englobe les relations humaines dans lesquelles l'individu cherche à établir une synthèse entre sa perception personnelle et celle qu'en ont les autres. Dans cette perspective, que nous adoptons pour notre recherche, la construction de l'identité apparaît comme un processus de négociation continu entre l'identité personnelle et les identités attribuées par autrui. Il convient d'explorer les modèles et les formes identitaires qui en résultent pour appréhender les implications de ces dynamiques.

2.1.2.5 Les modèles et les formes identitaires

Sainsaulieu (1988) introduit un modèle d'identités au travail basé sur ses recherches dans diverses organisations, identifiant quatre types d'identités professionnelles. Cette typologie souligne que l'accès au pouvoir et les stratégies d'action varient d'un individu à l'autre :

- Modèle fusionnel : renvoie aux travailleurs à faible pouvoir, caractérisés par une forte solidarité et une dépendance envers l'autorité.
- Modèle de négociation : s'applique aux professionnels qualifiés qui peuvent négocier leurs positions et leur reconnaissance.

- Modèle des affinités : se concentre sur les jeunes travailleurs en quête de mobilité socioprofessionnelle rapide, souvent en dehors des structures traditionnelles.
- Modèle de retrait : décrit les travailleurs peu qualifiés, souvent désengagés et ne considérant pas le travail comme une priorité.

Dubar (2015) élargit cette compréhension en définissant les formes identitaires comme des constructions qui permettent aux individus de se définir et d'interagir avec autrui. Ces formes sont influencées par les transactions subjectives et objectives, qui articulent l'identité héritée et l'identité visée, ainsi que l'identité attribuée par autrui.

Tableau 2 : les quatre processus identitaires typiques

Source : la socialisation : construction des identités sociales et professionnelles (Dubar C., 2015, p. 233)

Identité pour soi	**Identité pour autrui**	**Transaction objective**	
		Reconnaissance	**Non-reconnaissance**
Transaction subjective	Continuité	*Promotion (interne) identité d'entreprise*	*Blocage (interne) identité de métier*
	Rupture	*Conversion (externe) identité de réseau*	*Exclusion (externe) identité de hors-travail*

Dans son étude de 2015, Dubar réévalue et élabore son analyse des quatre identités professionnelles typiques (cf. tableau 2), initialement présentée en 1992. Chaque forme identitaire est liée à des processus distincts : promotion, blocage, conversion ou exclusion, et ces configurations sont influencées par les types de relations professionnelles et les acteurs impliqués, qu'ils soient internes ou externes.

Les processus d'identité se manifestent à travers des interactions diverses, permettant de naviguer entre continuité et rupture, promotion ou exclusion. Les institutions jouent un rôle crucial en validant ou non les identités revendiquées, façonnant ainsi le parcours professionnel de l'individu.

Cette dynamique souligne l'importance de la socialisation dans la construction des identités professionnelles, où l'interaction entre trajectoires individuelles et systèmes d'emploi est essentielle.

Ces formes identitaires peuvent s'interpréter à partir des modes d'articulation entre transaction objective et transaction subjective, comme des résultats de compromis « intérieurs » entre identité héritée et identité visée mais aussi de négociations « extérieures » entre identité attribuée par autrui et identité incorporée par soi. (Dubar, 2015, p. 231).

Pour mieux comprendre la dynamique de ces modèles, examinons comment l'identité professionnelle se relie à l'insertion professionnelle.

2.1.2.6 Identité professionnelle et insertion professionnelle

L'identité professionnelle se définit par le sentiment d'appartenance d'un individu à sa profession, engendrant un engagement envers ses exigences et ses valeurs éthiques (Broberg, 2018). Il est crucial de distinguer cette identité du professionnalisme, ce dernier se référant davantage à l'affichage du comportement professionnel, tandis que l'identité professionnelle concerne la perception personnelle d'un rôle, comme l'explique Wilson (2013) avec l'exemple de la médecine.

La construction de l'identité professionnelle est un processus complexe et dynamique, influencé par divers facteurs tout au long de la vie. Prenons l'exemple d'un stagiaire en comptabilité: son parcours de formation l'amène à développer son identité professionnelle, un processus interactif où l'identité et la formation se nourrissent mutuellement. L'identité professionnelle est ainsi perçue comme une construction sociale, évoluant en fonction du contexte historique et des interactions sociales. Par conséquent, l'identité d'un comptable, par exemple, ne se résume pas à des compétences techniques, mais englobe des valeurs et un engagement envers la profession (Hamilton, 2013).

Cela situe l'individu au sein d'une communauté professionnelle. Il est désormais pertinent d'explorer comment l'identité professionnelle peut à la fois être à l'origine de conflits et favoriser la coopération interprofessionnelle

2.1.2.7 L'identité professionnelle : clé de compréhension des conflits et de la coopération interprofessionnelle

Les conflits interprofessionnels, comme ceux observés entre auditeurs internes et responsables informatiques concernant la cybersécurité, illustrent comment les identités professionnelles peuvent entrer en compétition. Chaque groupe, en raison de ses convictions identitaires, peut percevoir sa responsabilité différemment, entraînant des tensions. Les stratégies d'auto-vérification identitaire peuvent jouer un rôle crucial dans la résolution de ces conflits, en aidant à harmoniser des identités professionnelles concurrentes (Gunz, 2007).

Lorsqu'un individu détient plusieurs identités professionnelles, comme un avocat agissant en tant que consultant interne, la saillance de ces identités influence ses décisions dans des

situations conflictuelles. Des recherches montrent que les avocats peuvent parfois ignorer les tensions éthiques liées à leurs différentes identités, gérant ainsi la dissonance identitaire de manière inconsciente (Costello, 2004).

Dans des environnements organisationnels complexes, il est fréquent que des professionnels négligent leur indépendance au profit de l'identité organisationnelle, créant des risques éthiques. Les organisations peuvent atténuer ces risques en renforçant l'identité professionnelle de leurs employés par des structures et des opportunités qui favorisent l'auto-évaluation de cette identité (Robertson, 2011).

En agissant ainsi, elles contribuent à maintenir des normes éthiques élevées et à prévenir des comportements problématiques, comme en témoigne le cas de la faillite d'Enron. En conclusion, il est important de considérer comment les conflits interprofessionnels peuvent évoluer vers des opportunités de coopération. Par exemple, dans une banque française, un auditeur interne a remis en question la mise en œuvre des protocoles de cybersécurité. Cette remise en question a généré des tensions avec les responsables de sécurité informatique, car chaque groupe percevait sa propre responsabilité et compétence comme prioritaire, révélant ainsi des identités professionnelles en concurrence (Power, 2007).

2.1.2.8 Des conflits interprofessionnels vers une coopération

Les conflits, qu'ils soient entre individus ou organisations, soulèvent des questions d'identité professionnelle et peuvent mener à des comportements conflictuels. Un conflit au travail peut être perçu comme une crise d'identité professionnelle, menaçant la crédibilité et le professionnalisme des employés (Webb, 2015).

Par exemple, Warren et Alzola (2009) démontrent que la force de l'identité professionnelle de l'auditeur est cruciale pour garantir son indépendance dans la prise de décision.

La théorie de l'identité sociale indique que l'appartenance à un groupe façonne les attitudes et comportements, influençant ainsi les conflits intergroupes. Dans ce contexte, une identité professionnelle solide favorise une approche coopérative face aux désaccords, tandis qu'une identité moins affirmée peut mener à la confrontation (Ivanova, 2017).

L'identité professionnelle joue un rôle déterminant dans la transformation des conflits en opportunités de coopération, soulignant l'importance d'un engagement fort envers ses valeurs et son rôle au sein de la communauté professionnelle.

2.1.3 Le rôle des juridictions pour comprendre les conflits et la coopération

Dans la dynamique des organisations, le débat sur l'audit interne et la cybersécurité peut mener à des conflits d'identité entre les auditeurs internes et les responsables de la sécurité

informatique. Ces tensions découlent souvent de la répartition des rôles et des responsabilités, chaque groupe revendiquant son autorité basée sur son expertise. Par exemple, un avocat agissant en tant que consultant interne peut naviguer entre son identité professionnelle d'employé et celle d'expert neutre, tout comme un auditeur interne peut osciller entre le rôle de décideur et de consultant.

Les conflits interprofessionnels résultent donc de perceptions contradictoires des identités professionnelles. Nous avons observé que, dans certaines circonstances, les professionnels peuvent ne pas réaliser ce qui constitue un comportement éthique. Ces comportements sont souvent influencés par des normes identitaires ancrées, et les professionnels de haut niveau peuvent valoriser leur indépendance, tandis que ceux de niveau inférieur peuvent privilégier la conformité. Ainsi, les entreprises ont un rôle crucial à jouer pour renforcer l'identité professionnelle des individus exerçant des fonctions doubles, en les intégrant pleinement dans la culture organisationnelle.

Ces crises identitaires, manifestées dans les tensions interprofessionnelles, soulignent la nécessité de définir plus clairement les responsabilités à travers des mécanismes formels, tels que les juridictions.

2.1.3.1 Des conflits interprofessionnels vers une coopération

L'identité professionnelle peut être un levier essentiel pour transformer les conflits en opportunités de coopération. Dans le milieu de travail, ces conflits sont souvent liés à des crises identitaires, affectant le recrutement et la rétention des talents. Dans de nombreux cas, les conflits interprofessionnels liés à l'identité peuvent se transformer en opportunités de coopération, surtout lorsque les employés parviennent à dépasser les crises identitaires initiales. Ces dynamiques nous poussent à explorer le rôle des juridictions dans la résolution de tels conflits (Abbott, 2003).

2.1.3.2 Le rôle des juridictions pour comprendre les conflits et la coopération

La cybersécurité, territoire souvent disputé entre auditeurs internes et responsables de la sécurité informatique, illustre ce phénomène. Selon Susan Hamilton (2013), la notion de juridiction décrit la relation entre une profession et son domaine d'activité. La concurrence pour la juridiction émerge particulièrement lors de l'introduction de nouvelles responsabilités, comme c'est le cas avec la cybersécurité dans le secteur bancaire.

Les professions cherchent à s'approprier des domaines d'activité en revendiquant leur légitimité à travers des savoirs et des pratiques spécifiques. Ces luttes pour le contrôle, souvent exacerbées par des échecs d'autres professions, sont soumises à la réaction de divers auditoires, incluant l'État et le public. Ainsi, les organisations deviennent le théâtre de ces luttes de juridiction, où

chaque profession cherche à consolider son rôle et sa légitimité face aux autres, surtout dans des domaines critiques comme la cybersécurité (Abbott, 2003).

2.1.3.3 Les conflits interprofessionnels et la professionnalisation

Le développement des professions s'inscrit dans un système où chaque groupe cherche à établir et défendre sa juridiction. Abbott (1988) souligne que les luttes pour la juridiction sont fondamentales pour comprendre l'évolution des professions. Dans ce cadre, les professions tentent de revendiquer des champs d'activité laissés vacants par d'autres. Par exemple, dans le conflit entre la dentisterie et l'hygiène dentaire en Ontario, l'hygiène dentaire a su s'approprier des tâches traditionnellement réservées aux dentistes, élargissant ainsi son champ d'action. Dans le secteur bancaire, la cybersécurité reste un domaine contesté où auditeurs internes et professionnels de l'informatique rivalisent pour affirmer leur juridiction, illustrant un cas classique de lutte interprofessionnelle pour la responsabilité.

Ces conflits soulignent l'importance, pour les organisations, d'établir des frontières de responsabilité claires afin de minimiser les tensions et de favoriser une coopération efficace.

2.1.3.4 L’impact de l'identité sociale sur l'évolution de la juridiction

Dans les environnements de travail, la notion de juridiction se réfère à la capacité de contrôler et de superviser certaines tâches. Les questions fondamentales concernent qui est habilité à effectuer quel type de travail. Selon Strauss et al. (1963), chaque organisation possède un ordre professionnel négocié qui influence la capacité des individus à développer de nouvelles compétences. Haslam (2001) ajoute que les individus portent plusieurs identités qui varient en fonction du contexte, affectant ainsi leur influence sur les juridictions au sein de l'organisation.

Hughes (1984) a souligné que les groupes professionnels établis obtiennent une reconnaissance officielle pour certaines tâches, mais Abbott (1988) soutient que les véritables divisions de travail sont souvent définies par la négociation et la coutume, ce qui les rend vulnérables aux changements organisationnels.

Alors que les divisions interprofessionnelles opposent traditionnellement des groupes distincts, les divisions intra-organisationnelles reflètent des changements dans la répartition des tâches au sein même de l’organisation, obligeant les professionnels à élargir leur champ d’action (Abbott, 1988).

2.1.3.4.1 Des frontières dépassées

Les frontières entre les professions engendrent des dynamiques complexes. Abbott (1988) démontre que ces frontières sont souvent franchies, par exemple lorsque des professionnels incompétents sont remplacés par des non-professionnels pour accomplir des tâches essentielles. Dans divers secteurs, comme la cybersécurité bancaire, les frontières entre professions

deviennent floues, car les impératifs de prévention des cyberattaques transcendent les distinctions traditionnelles, illustrant la dynamique changeante des juridictions professionnelles.

2.1.3.4.2 La juridiction liée à l'identité professionnelle

L'identité professionnelle joue un rôle déterminant dans la négociation des juridictions au sein des organisations. La distinction entre professionnels et non-professionnels repose sur deux critères : la compétence technique et l'adhésion à un code éthique (Chapoulie, 1973).

Historiquement, certaines professions, comme les soins infirmiers, avaient une identité bien définie, mais cette clarté s'est atténuée avec la diversification des rôles et des responsabilités. Cependant, l'élargissement des rôles peut aussi renforcer l'identité professionnelle, comme le montrent Petrakaki, Klecun et Cornford (2014), où les infirmières ont étendu leur champ d'action pour inclure des responsabilités en matière de gestion des données des patients. En revanche, la dilution des responsabilités peut menacer cette identité, comme l'indiquent Borthwick (2009) et Musselbrook (2013).

Dans le secteur bancaire, le maintien de la cybersécurité ne repose pas sur une juridiction managériale claire, mais plutôt sur des compétences qui varient d'une institution à l'autre. Pour revendiquer leur juridiction en matière de cybersécurité, les auditeurs internes doivent élargir leur identité professionnelle en intégrant de nouvelles compétences techniques.

2.1.3.5 La juridiction au cœur des identités professionnelles

Dans les approches néo-wébériennes, les professions se définissent par leur capacité à monopoliser un segment du marché du travail, à légitimer leurs compétences juridiques et à s'imposer sur des domaines spécifiques. Cependant, cette quête de monopole génère également des conflits interprofessionnels. Ces professions sont des constructions sociales et historiques, constituées de groupes qui mobilisent des ressources culturelles pour valider leur vision du monde. Pour accroître leur prestige, ces groupes mettent en place des stratégies politiques, élaborant des systèmes de justification qui les opposent à d'autres professions concurrentes. L'analyse d'Andrew Abbott sur les systèmes professionnels et l'écologie professionnelle offre un cadre pertinent pour explorer les luttes entre professions, notamment celles liées à la comptabilité, ainsi que celles opposant la comptabilité à d'autres disciplines. Ce travail favorise des études inductives et comparatives, permettant de comprendre les mécanismes de l'autonomisation professionnelle et les interrelations entre groupes dans l'exercice de leurs activités. (Sebti, 2016).

2.1.3.5.1 Une théorie des juridictions professionnelles institutionnalisées

La sociologie des professions s'est récemment concentrée sur la concurrence entre groupes dans

la constitution d'une juridiction par le contrôle d'un système de connaissances. (Tolbert, 1990)

Abbott (1988) souligne qu'un groupe doit maîtriser son système de connaissances pour revendiquer une légitimité professionnelle, ce qui lui permet de redéfinir les problèmes sociétaux qu'il traite et de défendre sa position face à des professions concurrentes. Le contrôle des connaissances est donc plus crucial que le comportement éthique dans l'acquisition de prestige et de récompenses financières.

Abbott identifie trois processus historiques fondamentaux qui contribuent à l'évolution des professions : la perturbation, le déplacement des revendications et la modification des systèmes de connaissances. Les conflits de juridiction génèrent des politiques d'expertise, particulièrement intenses en périodes de transformation professionnelle. Reed (1996) propose que ces conflits se manifestent principalement aux frontières entre trois types de professions : libérales, organisationnelles et entrepreneuriales, chacune adoptant des stratégies distinctes pour défendre sa juridiction.

Au niveau de la revendication de la juridiction, elle repose sur le diagnostic, le traitement, l'inférence et le travail académique. En exigeant la reconnaissance de ses droits exclusifs, une profession cherche à imposer sa structure cognitive et son autorité dans divers contextes, notamment légal, public et organisationnel. En milieu de travail, la complexité des rôles professionnels peut mener à des chevauchements juridictionnels, rendant difficile la délimitation des responsabilités. (Abbott, 1988)

Au niveau des luttes pour gagner la juridiction, Abbott (1988) affirme que les professions s'engagent constamment dans des luttes pour protéger ou acquérir des juridictions, les définissant comme des domaines de pouvoir où elles peuvent revendiquer leur expertise. Cette dynamique est influencée par la nécessité de codifier des connaissances et de maintenir une reconnaissance par les pairs, essentielle pour préserver le statut d'expert.

Gendron (2007) souligne que la lutte pour la juridiction implique la réclamation de domaines d'expertise déjà occupés par d'autres. L'approche d'Abbott s'applique particulièrement bien à l'analyse des conflits de juridiction, comme celui entre auditeurs internes et responsables de la sécurité informatique, que nous examinerons en détail.

Abbott (1988) propose différentes configurations pour résoudre les conflits de juridiction. Dans le cas de la pleine juridiction, un groupe exerce un contrôle total sur la juridiction. La juridiction subordonnée se manifeste lorsqu'une profession est placée sous l'autorité d'une autre. La prééminence intellectuelle implique un partage des connaissances entre différents groupes. La juridiction divisée est caractérisée par une collaboration entre professions pour résoudre des problèmes complexes. Avec la juridiction consultative, un groupe exerce un rôle de contrôle

consultatif sur un autre. Enfin, la juridiction peut être différenciée par clients, avec une division des professions en fonction du type de clientèle qu'elles desservent.

Ce modèle sera utilisé pour analyser la relation entre l'audit interne et externe, que nous synthétiserons dans le tableau suivant.

Tableau 3 : la relation entre l'audit interne et l'audit externe selon Abbott

La relation entre l'audit interne et l'audit externe selon Abbott					
Définition	Pleine Juridiction	Juridiction Subordonnée	Juridiction Intellectuelle	Juridiction Consultative	Juridiction Partagée
	Une profession contrôle la juridiction et exclut les concurrents.	La profession supérieure contrôle le travail de la profession subordonnée.	La profession supérieure contrôle la base de connaissances, mais permet à d'autres professions de pratiquer plus ou moins libre.	Une profession retient le droit d'interpréter ou modifier le travail d'un autre métier.	La juridiction est divisée entre deux professions.
Appliqué à la relation Audit I/E	L'audit externe contrôle entièrement le travail d'audit interne et exclut toute personne, sauf les professionnels de l'audit externe disposant d'une licence complète, de la pratiquer.	L'audit externe est la profession supérieure qui délègue le travail d'audit interne à la profession subordonnée d'auditeur interne tout en conservant un contrôle direct sur le travail effectué.	L'audit externe contrôle la base de connaissances de l'audit interne mais permet aux auditeurs internes de l'exercer comme ils le souhaitent.	L'audit externe et interne existe en deux professions égales, mais l'audit externe conserve le droit d'interpréter le travail de l'audit interne.	L'audit externe et interne existe sous la forme de deux professions de différentes juridictions. Les deux juridictions peuvent être interdépendantes.
Connaissance de base	L'audit interne est un audit financier.	L'audit interne est la tâche de routine de l'audit financier.	L'audit interne est en théorie un audit financier, alors qu'en pratique, il peut s'agir d'autre chose.	L'audit interne est l'audit opérationnel ou de gestion des risques. Auditeurs externes Interprètent les résultats de ces audits du point de vue de l'audit financier.	L'audit interne est l'audit opérationnel et de gestion des risques. L'audit externe est un audit financier.

Au niveau des sources de perturbations de la juridiction, les changements dans les juridictions résultent souvent de concours interprofessionnels. Ces perturbations peuvent être engendrées par des forces externes, qui ouvrent de nouveaux domaines de compétence, ou par des

changements internes qui renforcent les juridictions existantes. Par exemple, de nouvelles technologies peuvent créer des opportunités ou des menaces pour les professions établies, tandis que les changements organisationnels peuvent mener à la formation de nouvelles professions. Les professions doivent naviguer ces dynamiques pour maintenir et revendiquer leur autorité dans un paysage professionnel en constante évolution (Abbott, 1988). La figure 11 ci-dessous, résume la théorie d'Abbott par une représentation graphique.

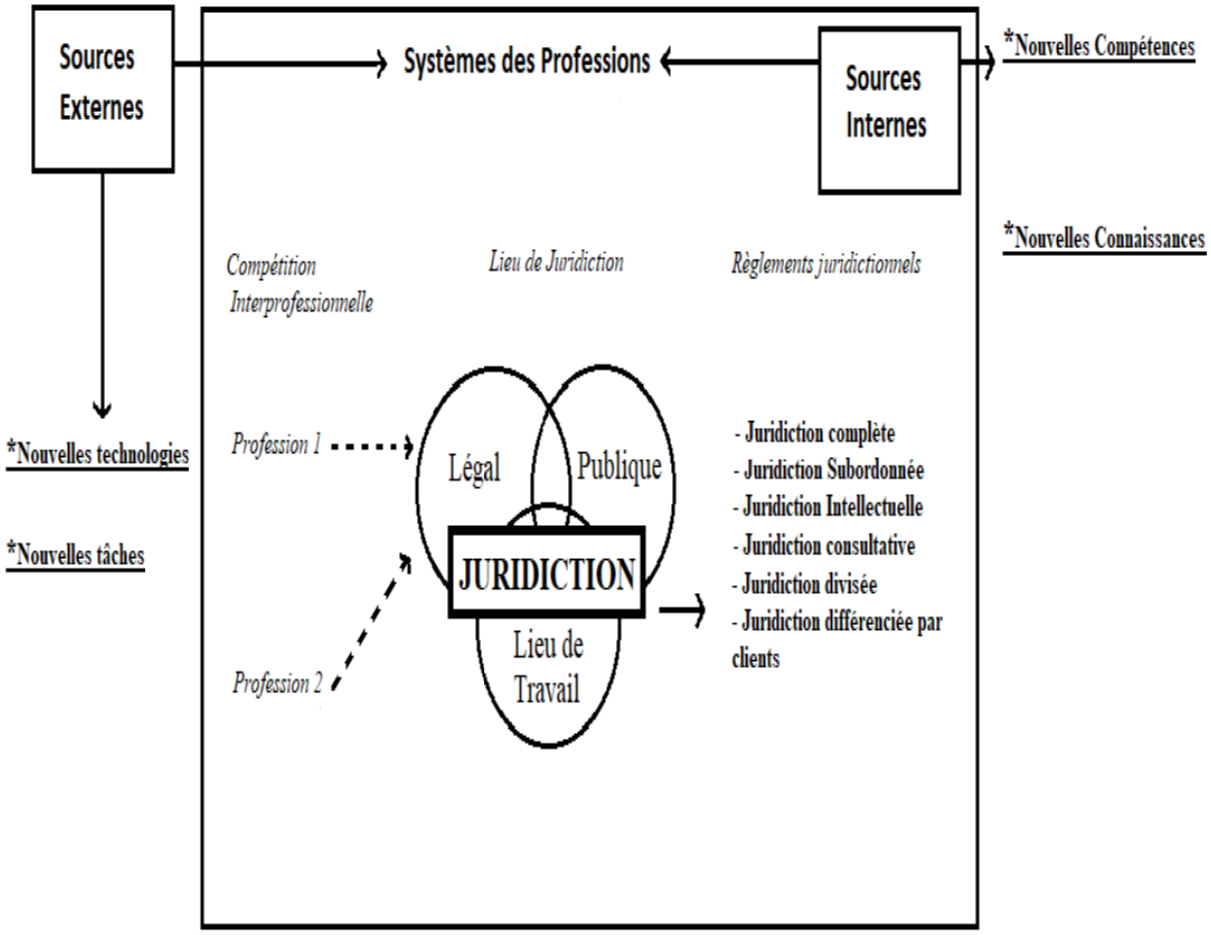


Figure 11 : représentation graphique et partielle de la théorie d'Abbott

Source: the system of professions : An essay of the division of expert labor (Abbott A. , 1988).

En clôture, la lutte pour la juridiction professionnelle, que ce soit dans le domaine de la cybersécurité ou d'autres secteurs, reflète la quête des professions pour légitimer et sécuriser leur champ d'action. Cette dynamique met en lumière les défis organisationnels liés à la clarification des rôles et responsabilités pour assurer une meilleure coopération.

Conclusion intermédiaire

L’identité professionnelle, en tant que notion complexe et multidimensionnelle, joue un rôle fondamental dans la dynamique des conflits et de la coopération au sein des organisations, en particulier dans le domaine de la cybersécurité bancaire. Les professionnels, tels que les auditeurs internes et les responsables de la sécurité informatique, sont souvent appelés à endosser des rôles multiples. Cela peut entraîner des conflits d'identité, notamment lorsque des responsabilités concurrentes en matière de cybersécurité leur sont attribuées.

Dans cette partie, nous avons souligné comment des tensions peuvent émerger lorsque, par exemple, un auditeur interne se perçoit comme le gardien de l'organisation, tandis qu'un responsable de la sécurité informatique se considère comme l'expert technique responsable de la protection des systèmes. Cette divergence d'identités professionnelles peut engendrer des désaccords sur les meilleures stratégies à adopter pour assurer la cybersécurité.

Les juridictions professionnelles jouent un rôle crucial dans la définition et la défense de ces identités. Chaque groupe professionnel cherche à établir sa légitimité dans un domaine spécifique, ce qui peut créer des conflits de responsabilité. Dans le secteur bancaire, par exemple, les auditeurs internes et les responsables de la sécurité informatique se disputent souvent le contrôle de la cybersécurité, chacun souhaitant définir son rôle prépondérant.

Cependant, il est essentiel de reconnaître que ces conflits d'identité et de compétence ne sont pas intrinsèquement négatifs. Ils peuvent donner lieu à des dialogues constructifs, à une clarification des responsabilités et, en fin de compte, à un renforcement de la cybersécurité au sein de l'organisation. Une gestion adéquate de ces conflits est cruciale pour favoriser une collaboration efficace entre les professionnels, tous engagés vers l’objectif commun de protéger les actifs informatiques et de prévenir les cyberattaques.

En somme, comprendre les identités professionnelles, les conflits de juridiction et leurs interactions est indispensable pour relever les défis complexes de la cybersécurité dans le secteur bancaire. Une approche efficace de ces enjeux contribuera à accroître la résilience des entreprises face aux menaces croissantes du monde numérique.

2.2 L’identité professionnelle des auditeurs internes : enjeux et transformations contemporaines

Dans la partie précédente, nous avons exploré la notion d’identité professionnelle et son rôle dans le cadre des conflits identitaires au sein des organisations, notamment dans le contexte de la cybersécurité bancaire. Cette partie se concentre spécifiquement sur la construction de l’identité professionnelle des auditeurs internes dans ce secteur. Pour ce faire, nous examinerons la définition, les responsabilités, les normes et l'évolution de la fonction d'audit interne, ainsi que son impact sur la cybersécurité. Face à ces conflits identitaires, la construction de l’identité professionnelle des auditeurs internes, en particulier dans le contexte de la cybersécurité, devient essentielle pour garantir l'efficacité de leur intervention (Cunliffe, 2021).

2.2.1 Le rôle de l’auditeur interne dans l’organisation : fondements et évolutions

L’audit interne n'est pas un emploi à vie, mais plutôt une fonction dynamique qui évolue rapidement avec les besoins des organisations, s'adaptant à la montée en puissance des technologies, des régulations et des menaces nouvelles telles que les cyberattaques. Les auditeurs internes, grâce à leur expérience et leurs compétences, peuvent évoluer vers des rôles de management ou devenir des leaders au sein de l'organisation, assurant ainsi une supervision stratégique des risques.

2.2.1.1 Les éléments essentiels de la fonction d’audit interne : cadre conceptuel et méthodologique

L’audit interne est né de la nécessité pour les directions générales de maîtriser les risques liés à l'augmentation du volume d'informations et à la complexité croissante des entreprises. Aujourd'hui, il ne s'agit plus d'une simple activité de vérification, mais d'un processus qui contribue activement à la performance de l'organisation (Mandzila, 2011).

La définition de l’audit interne par l’Institute of Internal Auditors (2020) souligne son rôle indépendant et objectif, orienté vers l'amélioration des processus de gestion des risques et la création de valeur ajoutée.

2.2.1.2 Objectifs de l’auditeur interne et enjeux de la cybersécurité

Les objectifs de l’audit interne s'articulent autour de la supervision des dispositifs de contrôle interne, de l'examen des données financières et opérationnelles, ainsi que de l'évaluation des risques, tels que les failles potentielles dans les systèmes de gestion de l'information ou la conformité aux réglementations en matière de cybersécurité. Dans le cadre de la cybersécurité, l’audit interne revêt une importance primordiale, en permettant l’identification des risques liés à la sécurité de l’information et en participant activement à l’optimisation des mécanismes de

contrôle (IIA, 2011).

Le modèle des trois lignes de défense, ci-dessous, définit la position de l'audit interne comme la dernière ligne, garantissant une assurance objective sur l'efficacité des contrôles de cybersécurité en place.

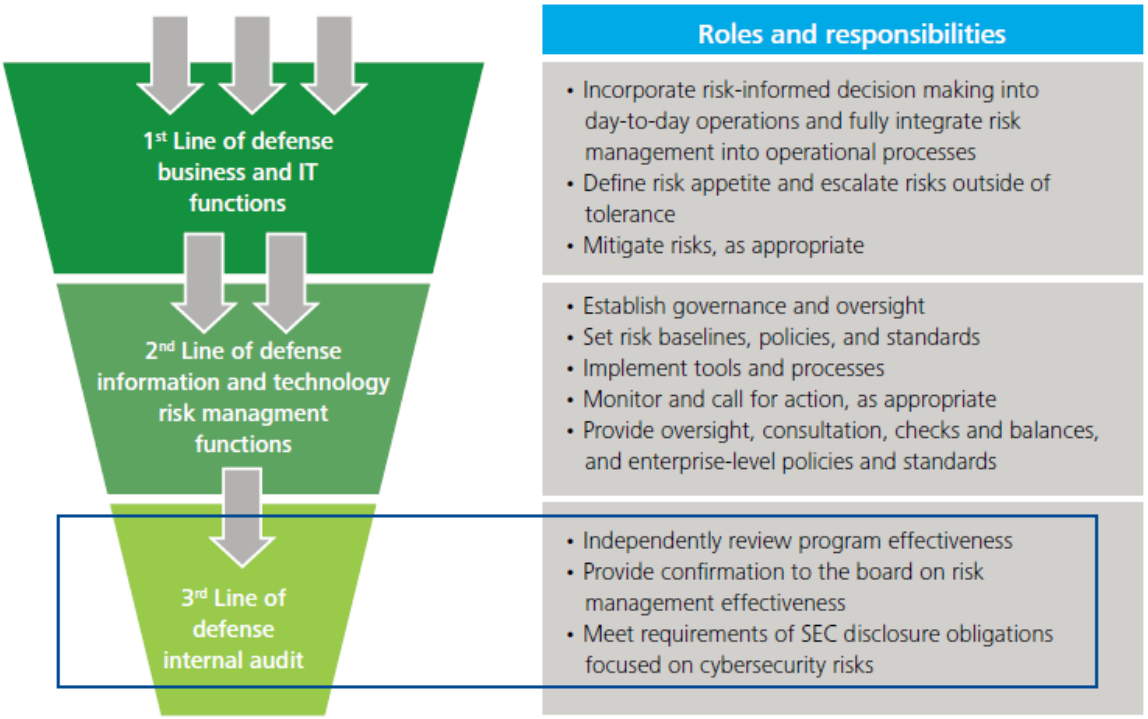


Figure 12 : modèle de trois lignes de défense

Source: rôles des trois lignes de défense pour la sécurité de l'information et la gouvernance (Ho, 2018).

2.2.1.3 Les normes d'audit interne : définition et impact sur les pratiques professionnelles

Les normes professionnelles guident les pratiques d'audit interne, assurant que les auditeurs exercent avec compétence et éthique. Ces normes incluent celles promulguées par l'IIA (Institute of Internal Auditors) et la norme ISO 27001, particulièrement pertinente dans le cadre des audits de cybersécurité. Le Code de Déontologie et les différents types de normes (qualification, fonctionnement et mise en œuvre) définissent les principes et les critères d'évaluation de la qualité des missions d'audit. Ces normes sont essentielles pour établir la légitimité et l'efficacité de la fonction d'audit interne (Renard, 2017).

2.2.1.4 La reconnaissance de la profession d'audit interne

L'audit interne n'est pas un emploi à vie : constat définitif qui situe bien là fonction hors du champ des professions. Mais également constat optimiste puisqu'il situe les auditeurs internes parmi ceux qui, ayant acquis expérience et connaissance, vont pouvoir être demain des

managers efficaces et performants. Cette perspective est en train de se réaliser dans trois directions : spécialisation, certification, mondialisation.

L'identité professionnelle des auditeurs internes est renforcée par leur spécialisation croissante, la certification de leurs compétences et l'adoption de normes mondiales. La spécialisation permet aux auditeurs de maîtriser des domaines complexes, tandis que la certification, comme le *CIA* (Certified Internal Auditor), ou des certifications spécifiques à la cybersécurité telles que le *CISA* (Certified Information Systems Auditor), deviennent des gages de qualité reconnus à l'échelle internationale. La mondialisation des pratiques d'audit favorise une standardisation et une reconnaissance internationales, renforçant ainsi le statut et l'importance de la fonction (Renard, 2017).

L'identité professionnelle des auditeurs internes se construit à travers l'acquisition d'expérience, de spécialisation et de reconnaissance, ce qui les positionne comme des acteurs clés dans la cybersécurité au sein des organisations.

2.2.1.5 Le comité d'audit et les auditeurs internes

L'audit interne est supervisé par le Comité d'audit, garantissant ainsi l'objectivité de l'auditeur interne, qui ne doit exercer aucune autre fonction au sein de l'organisation. Cela permet de maintenir une séparation claire des responsabilités et d'assurer l'intégrité des processus d'audit (Renard, 2017).

La supervision d'un programme de cyber sécurité réussi nécessite un engagement fréquent et proactif du conseil d'administration et du comité d'audit. Le comité d'audit, en sa capacité de superviser les activités de gestion des risques et de surveiller les politiques et procédures de la direction, joue un rôle stratégique important dans la coordination des initiatives et des politiques relatives aux cybers risques et dans la confirmation de leur efficacité. Ces responsabilités comprennent la définition des attentes et de la responsabilité de la gestion, ainsi que l'évaluation de l'adéquation des ressources, du financement et de la concentration des activités de cybersécurité. Le président du comité d'audit peut être une liaison particulièrement efficace avec d'autres groupes pour faire respecter et communiquer les attentes en matière de sécurité et d'atténuation des risques. Le comité d'audit devrait confirmer que la fonction d'audit interne examine régulièrement les contrôles relatifs à la cybersécurité, est à jour sur les derniers développements et inclut les questions connexes de manière visible et régulière à son ordre du jour (Leong, 2017).

2.2.1.6 Une profession mal définie : défis et perceptions contradictoires

La fonction d'audit interne peine à trouver sa légitimité au sein des entreprises. Selon Benabid (1995), plusieurs raisons expliquent cette situation. D'abord, de nombreux dirigeants ne

comprennent pas bien le rôle de l'audit interne, souvent confondu avec d'autres fonctions comme le contrôle de gestion. Une meilleure communication sur la spécificité des objectifs de l'audit interne, en particulier dans la gestion des risques liés à la cybersécurité, pourrait améliorer cette compréhension. Benabid souligne également que les auditeurs internes sont souvent perçus uniquement comme des *« hommes de chiffres »*, limitant ainsi leur reconnaissance. Pour améliorer cette image, il est crucial de revoir les méthodes de recrutement et d'adopter une approche centrée sur la gestion des risques, qui aidera à identifier les zones critiques et à clarifier les compétences requises dès le départ.

La réputation de l'auditeur, tant sur le fond que sur la forme, est primordiale. Cette nécessité d'autocontrôle peut mener à une crainte de nuire à sa réputation, poussant ainsi l'auditeur à un engagement maximal dans son travail (Garnier, 2014).

Cependant, cette perception floue de son rôle peut créer des tensions avec d'autres acteurs de la cybersécurité, entraînant des problèmes de légitimité et de territorialité dans la gestion des risques liés à la sécurité informatique. Ces défis soulignent l'importance d'une clarification des rôles et des responsabilités, essentielle pour renforcer la collaboration entre les différentes fonctions au sein des organisations.

2.2.2 La légitimité professionnelle des auditeurs internes : défis, opportunités et perspectives

L'essor des technologies numériques et la montée des cybermenaces ont placé la cybersécurité au cœur des préoccupations commerciales. Les coûts liés à la protection des actifs numériques, aux temps d'arrêt opérationnels et aux obligations réglementaires augmentent rapidement, rendant le rôle de l'audit interne crucial. Ce dernier fournit aux conseils d'administration une assurance indépendante sur l'efficacité de la gestion des risques (*la première et la deuxième ligne de défense*[2]*)* en matière de cybersécurité, évaluant comment les fonctions de cybersécurité protègent les actifs d'une organisation (Federation of European Risk Management Associations, 2019).

Pour que l'audit interne soit efficace, il doit réaliser une évaluation complète et opportune, conforme aux normes professionnelles et aux attentes des parties prenantes. Traditionnellement centré sur les risques financiers et opérationnels, l'intégration de la cybersécurité dans ses missions pose de nouveaux défis (Chambers, 2015).

Les auditeurs internes se heurtent à des problèmes de juridiction, car la sécurité de l'information est souvent perçue comme une fonction distincte et les conseils d'administration peinent à

[2] Figure 14 : Modèle de trois lignes de défense, p 55.

définir des attentes claires pour atténuer les cyberrisques (Islam, 2018).

De plus, l'insuffisance des compétences et des ressources disponibles limite leur capacité à évaluer efficacement ce domaine émergent (IIA, 2020).

2.2.2.1 Optimisation des pratiques d'audit en cybersécurité : vers une méthodologie efficiente

Une étude menée auprès de 183 auditeurs informatiques, renforcée par une documentation de l'ISACA[3], a révélé que les facteurs normatifs, tels que les certifications en cybersécurité, ainsi que le soutien des conseils et la coopération entre les lignes de défense, sont déterminants pour l'efficacité de l'audit de cybersécurité. Par exemple, la collaboration entre les auditeurs et les équipes IT permet une meilleure identification des vulnérabilités, tandis que les audits réguliers assurent une mise à jour continue des contrôles de sécurité. Bien que de nombreux éléments influençant l'audit interne global soient également applicables ici, les spécificités de la cybersécurité requièrent des compétences techniques distinctes et un soutien actif de la direction (Jamison, 2018).

L'efficacité de l'audit est également liée à sa capacité à répondre aux besoins des audités, mesurée par la satisfaction des audités et le taux de mise en œuvre des recommandations (IIA, 2020).

Cependant, de nombreux dirigeants ne comprennent pas bien l'organisation de leurs entreprises pour faire face aux cyberattaques, compliquant ainsi l'évaluation de l'audit de cybersécurité. Pour être efficace, un audit doit fournir un avis objectif sur l'efficacité des contrôles en place, soutenu par une légitimité établie par les compétences des auditeurs (Vuko, 2021).

2.2.2.2 Les critères de légitimité dans l'audit des systèmes d'information et de cybersécurité

La légitimité des auditeurs internes repose sur plusieurs facteurs, dont l'efficacité des audits eux-mêmes. Un audit de cybersécurité est considéré comme légitime s'il s'appuie sur des normes professionnelles, un référentiel déontologique clair et des pratiques de rapport standardisées. Ces éléments renforcent la reconnaissance professionnelle des auditeurs dans leurs interactions avec les parties prenantes (Power, 1995).

De plus, le discours institutionnel autour des technologies de cybersécurité, associé à l'autorité de l'institution professionnelle, constitue un autre fondement de leur légitimité (Sarfatti-Larson, 1988).

[3] Anciennement connue sous le nom d'*Information Systems Audit and Control Association*®, l'ISACA n'utilise désormais que son acronyme pour refléter le large éventail de professionnels de la gouvernance informatique qu'elle dessert.

La capacité des auditeurs à s'adapter à l'évolution des technologies et à se repositionner par rapport aux défis contemporains est essentielle pour maintenir cette légitimité. Pour les auditeurs internes, la légitimité se traduit par le soutien des parties prenantes, obtenu en démontrant leur utilité et leur efficacité (Lenz et al. 2018).

Ainsi, l'efficacité de l'audit de cybersécurité découle d'un équilibre entre les forces institutionnelles, les contraintes organisationnelles et le soutien du conseil d'administration, tout en interagissant de manière constructive avec les autres lignes de défense.

L'audit interne doit se conformer à un corpus de connaissances professionnelles, façonné par la formation académique et les certifications en cybersécurité, pour renforcer sa légitimité (Lenz et al. 2018). Bien que peu de preuves empiriques existent quant à l'efficacité des approches d'audit en cybersécurité, l'adhésion aux normes et l'émulation des meilleures pratiques confèrent une légitimité à ces pratiques (Vuko, 2021).

La légitimité des auditeurs internes repose sur leur indépendance, leur compétence et leur intégration au sein de la structure organisationnelle. Cependant, il est essentiel de reconnaître que la légitimité n'est pas un acquis ; elle doit être continuellement renforcée par des aptitudes et des normes appropriées.

2.2.2.3 La légitimité des pratiques professionnelles en audit interne

La légitimité de la profession d'audit interne repose sur le cadre de gouvernance et les revendications qui en légitiment les pratiques. Ce cadre est ancré dans des valeurs fondamentales telles que la rationalité et l'efficacité, essentielles pour l'acceptation sociale de la fonction (Abbott, 1988).

2.2.2.3.1 Pratiques et structuration de la fonction d'audit interne : étendue des services et audit en sécurité informatique

La littérature sur le rôle de l'audit interne dans la production de légitimité est abondante, mais peu traite de l'acquisition et du maintien de cette légitimité dans le contexte de la cybersécurité. Face à un environnement commercial en constante mutation, l'audit interne doit s'adapter aux exigences évolutives, devenant ainsi un enjeu de survie pour la profession (Kagermann, 2008).

Les changements récents dans les rôles et pratiques d'audit interne, notamment en matière de cybersécurité, soulignent la nécessité d'une réévaluation continue des compétences et des responsabilités (Selim, 2009).

Pour répondre aux attentes croissantes des parties prenantes, les auditeurs internes doivent fournir une assurance raisonnable et pertinente (Cattrysse, 2005).

2.2.2.3.2 Compétences et outils technologiques de l'audit interne : une revue critique

L'intégration des compétences en cybersécurité au sein des équipes d'audit interne est primordiale pour aligner leurs activités avec les priorités de l'entreprise. PwC (2009) souligne l'importance d'une formation adéquate et d'une collaboration étroite avec les départements de sécurité informatique. Bien que des initiatives existent pour renforcer ces compétences, de nombreux auditeurs internes manquent encore de préparation face aux défis technologiques actuels (Sarens, 2009). Cette lacune en compétences techniques rend souvent nécessaire le recours à des experts externes, ce qui pose des questions sur la légitimité et l'efficacité des audits internes (Abdolmohammadi, 2010).

2.2.2.3.3 L'externalisation de l'audit de cybersécurité : une approche controversée

L'externalisation des audits de cybersécurité peut sembler attrayante, notamment en raison de la rareté des compétences nécessaires. Cependant, elle peut limiter la continuité des processus internes, nuisant ainsi à la gestion proactive des risques cybernétiques (Munro et Stewart, 2010). Cependant, cette approche présente des risques, notamment une perte de connaissance organisationnelle et un risque accru de détection insuffisante des fraudes ou des cyberattaques (Colin et Robyn, 2008). Bien que l'externalisation puisse offrir des compétences spécialisées, il est souvent plus efficace de maintenir une fonction d'audit interne compétente, capable de travailler en collaboration avec les équipes de sécurité informatique.

2.2.2.3.4 Relations interservices : l'audit interne et le département de sécurité informatique

La relation entre les auditeurs internes et les responsables de la sécurité informatique est cruciale pour l'efficacité des audits. Ces deux fonctions doivent collaborer étroitement tout en naviguant des responsabilités parfois conflictuelles. Les auditeurs ont besoin d'un accès rapide aux données pour fournir des assurances adéquates, tandis que les responsables de la sécurité se concentrent sur la protection de ces mêmes données (Lewis, 2010).

Les tensions qui émergent de cette dynamique peuvent nuire à la légitimité des deux parties et à la cybersécurité globale de l'organisation.

2.2.2.3.5 Maintien et renforcement de la légitimité de la fonction d'audit interne

Dans le domaine de la cybersécurité, l'audit interne doit faire face à des exigences contradictoires qui menacent sa légitimité. Pour maintenir leur pertinence, les auditeurs doivent non seulement acquérir des compétences techniques, mais aussi démontrer comment leur expertise peut bénéficier à l'organisation (Robson, 2007).

Les tensions entre les anciennes logiques institutionnelles, axées sur la gestion financière traditionnelle, et les nouvelles logiques orientées vers la sécurité informatique, peuvent

compliquer l'adoption de nouvelles pratiques, exacerbant ainsi les conflits identitaires et de légitimité au sein des équipes d'audit interne (Thornton, 2002).

2.2.2.4 La réévaluation de la légitimité des auditeurs internes : vers une nouvelle juridiction

L'auditeur interne fonde sa légitimité et sa crédibilité sur les normes internationales d'audit, sur son indépendance. Il doit être rattaché au plus haut niveau de l'organisation pour lui assurer ces objectifs et l'accès à toute information nécessaire à l'accomplissement de la mission (Lamarque, 2016).

L'auditeur interne, par son indépendance et son rattachement aux niveaux les plus élevés de l'organisation, peut renforcer sa légitimité en matière de cybersécurité. Ce processus implique un contrôle légitime sur des activités auparavant réservées aux responsables de la sécurité informatique (Abbott A. , 1988).

En maîtrisant des savoirs techniques essentiels, les auditeurs internes étendent leur autorité, mais cela peut également engendrer des conflits d'identité professionnelle, nécessitant une clarification des rôles et des responsabilités dans ce nouvel environnement. Un cadre de collaboration structuré avec les responsables de la sécurité informatique pourrait atténuer ces tensions.

2.2.3 Identités professionnelles des auditeurs internes : construction, conflits et transformations

L'audit interne, peu préparé à la transformation numérique, se trouve confronté à des défis spécifiques, notamment dans le domaine de la cybersécurité. Ce terrain relativement nouveau, en particulier dans le secteur bancaire, souligne l'évolution rapide de la profession. En effet, de nombreuses études révèlent que le métier d'auditeur interne a connu des changements significatifs au cours des 25 dernières années. Face à ces nouveaux défis, tels que la cybersécurité, la profession des auditeurs internes évolue rapidement, ce qui transforme leur identité professionnelle (Broberg, 2018).

Cette partie se penche sur la dynamique de construction identitaire des auditeurs internes, une évolution qui éclaire les problèmes de juridiction rencontrés avec les responsables de la sécurité informatique.

2.2.3.1 Évolution de l'identité professionnelle des auditeurs internes au fils du temps

L'introduction de nouveaux services au sein des cabinets d'audit a été identifiée comme un facteur clé d'accélération du changement dans cette profession. Des chercheurs soutiennent que cette diversification a contribué à une renaissance de l'industrie de l'audit. Ce phénomène a

suscité un intérêt croissant dans la littérature, car la concurrence sur le marché non réglementé, notamment en matière de cybersécurité, engendre des tensions quant aux valeurs professionnelles et menace l'indépendance des auditeurs (Broberg, 2018).

La réputation des cabinets d'audit a également été mise à mal par divers scandales financiers, tels que ceux d'Enron et de WorldCom, qui ont remis en question l'efficacité de l'audit interne. Ces événements ont soulevé des préoccupations quant à la crédibilité des auditeurs et à leur rôle en tant que garants de l'intérêt public. Les attentes croissantes des parties prenantes concernant l'accès à des informations financières précises et rapides alimentent cette évolution de la profession (Ialy, 2014).

En réponse à ces défis, la profession d'audit interne est en pleine réinvention. Face à une demande croissante pour des services financiers plus complexes, les auditeurs doivent adapter leurs pratiques. Cependant, cette transformation pose des questions sur l'intégrité des auditeurs, comme l'indique Levitt (2000), l'ancien président de la SEC, qui est mis en garde contre l'affaiblissement de l'indépendance des auditeurs face à la pression croissante pour des résultats plus rapides et efficaces. Il avertit que la réingénierie de l'audit pourrait compromettre l'objectivité au profit de l'efficacité. Au fil des années, les auditeurs internes ont évolué, passant de leur image de contrôleurs à celle de consultants, visant à protéger les actifs de l'entreprise tout en maîtrisant les risques (Ialy, 2014).

2.2.3.2 Les processus de construction identitaire chez les auditeurs internes

La construction identitaire des auditeurs internes a fait l'objet de recherches approfondies au cours des deux dernières décennies (Grey, 1998). La littérature souligne que l'identité de ces professionnels est le résultat d'un développement continu, en interaction avec deux formes d'identité : l'identité sociale, ancrée dans les normes de groupe, et l'identité personnelle, centrée sur l'introspection (Watson, 2009 ; Lambert, 2016).

Ce processus de construction identitaire, souvent positif, se manifeste par une définition claire des rôles et responsabilités des auditeurs internes, contribuant ainsi à leur image professionnelle (Grey, 1998).

Tandis que l'identité sociale se construit en interaction avec l'environnement collectif, l'identité personnelle est le fruit d'un processus introspectif, où l'individu réconcilie ses expériences professionnelles avec ses valeurs personnelles. L'identité sociale des auditeurs, point central de cette recherche, reflète les normes comportementales qui sont internalisées dans les dispositifs de gestion des entreprises (Anderson-Gough, 2006).

Cependant, la construction de cette identité est confrontée à des défis. Les auditeurs internes doivent gérer des relations complexes avec leurs interlocuteurs, souvent accaparés par des

plannings surchargés et la désorganisation des documents comptables.

La peur de commettre des erreurs, pouvant entraîner des conséquences financières graves, renforce cette pression (Lambert, 2016).

Sur le terrain, ils font face à des limitations et à des rejets, qu'ils doivent parfois affronter avec cynisme (Kosmala, 2006).

Cette lutte pour maintenir une cohérence entre leur vision idéalisée de leur rôle et les réalités rencontrées peut engendrer un sentiment de dévalorisation chez les auditeurs, surtout lorsqu'ils ne parviennent pas à aligner leur mission avec les défis du quotidien (Morales, 2013). Parallèlement, les épreuves professionnelles, telles que les rites de passage et les jeux politiques, jalonnent leur parcours au sein de l'organisation (Kornberger, 2011).

2.2.3.3 Identité sociale et professionnelle des auditeurs internes : facteurs de saillance

L'identité sociale est définie comme la perception d'appartenance à un groupe. La théorie de l'identité sociale suggère que les individus, par le biais de comparaisons sociales, cherchent à établir une affiliation privilégiée avec leur groupe (Ian Burt, 2016). Les auditeurs, comme tout autre employé, s'identifient à divers groupes, tant à l'intérieur qu'à l'extérieur de leur organisation, ce qui influence leurs décisions et leur indépendance.

Ashforth et Mael (1989) ont développé cette notion, expliquant que l'identification à un groupe professionnel peut engendrer un sentiment de succès ou d'échec en fonction des résultats de ce groupe. Cette identification peut également affecter les interactions entre les auditeurs et leurs collègues, exacerbant les biais dans les jugements et menaçant leur indépendance. Ainsi, l'identité sociale des auditeurs internes émerge d'une quête de reconnaissance dans l'organisation, souvent en concurrence avec d'autres expertises (Lambert, 2016). Cette quête est en miroir avec leur identité personnelle, qui est définie comme la compréhension réflexive de soi, intégrant les expériences de vie individuelles (Giddens, 1991 ; Watson, 2009). Ces deux identités interagissent constamment, influençant le comportement et la prise de décision des auditeurs.

2.2.3.4 Identité professionnelle et conflits interprofessionnels : défis de positionnement

Les conflits interprofessionnels se manifestent généralement lorsque des professionnels, comme les auditeurs internes, ressentent une perte de reconnaissance de leur rôle au sein de l'organisation (Oandasan, 2006). La montée en puissance de la cybersécurité exacerbe ces conflits, car les auditeurs internes doivent désormais composer avec des professionnels de la sécurité informatique, dont le rôle chevauche parfois celui de l'auditeur en termes de protection des actifs de l'entreprise.

Ce défi nécessite une réflexion sur les antécédents et les dynamiques interprofessionnelles qui influencent l'identité sociale des auditeurs internes.

2.2.3.4.1 L'image professionnelle de l'auditeur interne : entre perception et réalité

Les membres d'un groupe s'intéressent souvent à l'image externe de leur profession. Par exemple, Dutton et al (1994) expliquent que le lien cognitif que les membres établissent avec leur organisation est influencé par ce que pensent les autres de cette dernière. Nous supposons donc que la perception qu'ont les auditeurs de l'image de leur profession est positivement liée à leur identification à celle-ci.

2.2.3.4.2 L'autonomie professionnelle des auditeurs internes : analyse critique

L'autonomie est un élément crucial pour les auditeurs, en raison de la nécessité d'adhérer aux normes professionnelles. Norris et Niebuhr (1984) ont trouvé une corrélation positive entre l'autonomie professionnelle et le professionnalisme dans leur étude d'un cabinet comptable. De même, Fogarty et Kalbers (2000) concluent que l'autonomie professionnelle est l'une des étapes les plus importantes que les entreprises peuvent entreprendre pour améliorer le professionnalisme des auditeurs internes. Par conséquent, nous émettons l'hypothèse que l'autonomie professionnelle est positivement liée à l'identité professionnelle. Des recherches connexes (Aranya, 1984) suggèrent également que l'autonomie professionnelle sera négativement liée aux conflits interprofessionnels.

2.2.3.4.3 L'efficacité des audits internes : une approche comparative des méthodologies

Les exigences des investisseurs en matière d'informations financières fiables et le besoin des auditeurs de répondre aux normes professionnelles sont des caractéristiques marquantes de l'audit. La théorie de l'identité sociale (Tajfel, 1985) suggère que l'estime de soi et le sentiment d'appartenance des auditeurs à leur profession devraient être améliorés par leur capacité à effectuer des audits de qualité. Par conséquent, nous émettons l'hypothèse qu'il existe une relation positive entre la perception qu'ont les auditeurs de l'efficacité de l'audit dans leur entreprise et leur identité professionnelle. Comme pour l'autonomie professionnelle, nous postulons également une relation négative entre l'efficacité de l'audit et les conflits interprofessionnels.

2.2.3.4.4 Le mode d'occupation professionnelle : redéfinir les pratiques de l'audit

Plusieurs études ont analysé l'influence de la durée et du progrès de carrière sur l'identification organisationnelle des professionnels de l'audit interne (Mael, 1992). Nous validons également que la carrière des auditeurs est positivement liée à leur identité professionnelle. Nous retenons le mode d'occupation comme variable exogène, sans relation hypothétique avec l'identification

professionnelle.

2.2.3.5 Identité professionnelle et saillance des auditeurs internes : enjeux de reconnaissance

La recherche sur l'audit se concentre généralement sur le niveau d'analyse individuel (auditeur) ou organisationnel (cabinet d'audit). Sans diminuer l'importance de ce dernier, et conformément à la théorie comportementale du cabinet d'audit (Cyert, 1963) et à certains écrits en audit (Johansson, 2005), nous supposons que les organisations reflètent les décisions prises par des individus au sein du service d'audit. Dans ce contexte, étant donné qu'il s'agit de bureaucraties professionnelles, les auditeurs professionnels constituent le noyau opérationnel de ces organisations. Les identités de ces individus sont supposées être construites en interaction, ou même à travers le choc des forces externes et internes représentées respectivement par la profession et l'organisation (Lui, 2001). En d'autres termes, l'identité professionnelle des auditeurs, largement étudiée dans la recherche en audit, représente les forces de l'environnement interne et externe qui influencent le comportement de l'auditeur au sein de l'organisation (Johnson, 2006).

L'identité professionnelle désigne la mesure dans laquelle un employé éprouve un sentiment d'unité avec sa profession (Heckman, 2009).

L'individu se sent impliqué dans sa profession et accepte les exigences d'indépendance et les valeurs éthiques qui la caractérisent. L'identité professionnelle des auditeurs se distingue par son absence de contribution visible aux profits de l'entreprise ; au lieu de cela, l'accent est mis sur la fourniture d'un service de haute qualité aux parties prenantes (Freidson, 2001).

Mintzberg (1980) explique que l'appartenance des auditeurs à la profession d'audit favorise l'émergence d'une identité professionnelle. Cette identité au niveau de l'auditeur individuel a été soulignée dans de nombreuses études. Ces recherches soutiennent également que ces identités servent de proxy pour les influences des forces externes et internes qui construisent l'auditeur individuel (Johnson, 2006).

L'identité professionnelle des auditeurs, influencée par des forces internes et externes, façonne directement leurs décisions dans l'exercice de leurs fonctions.

Surmontant la vision de l'auditeur purement expert, Power (1991) comme Grey (1998) envisagent le savoir technique comme une précondition basique, le minimum requis pour la pratique professionnelle. Cette condition, assurée par un diplôme ou un contrat de travail, n'est finalement pas suffisante pour définir l'identité de l'auditeur. Les auteurs cherchent à montrer la nature socialement construite des professions, notamment en déchiffrant une attitude constitutive d'un processus identitaire qui conduit à définir l'auditeur comme professionnel.

Être auditeur serait donc avant tout adopter un comportement approprié (Alvesson, 1994).

Pour Grey (1998), être un professionnel de l'audit est plus une attitude, une façon de se comporter qu'une possession ou la maîtrise d'un savoir technique. Pour étayer son propos, il mène une étude de cas dans un cabinet Big Six et conclut que les composantes qui évaluent l'auditeur pour être considéré comme professionnel incluent : la capacité technique, la relation avec le client, la qualité du travail fourni, la gestion du temps et de la mission, ainsi que les attributs personnels et professionnels.

Grey souligne également des notions telles que l'équité, le genre, la hiérarchie, l'apparence physique ou la sexualité pour définir l'auditeur comme professionnel, respectant des normes qui ne sont pas strictement professionnelles mais qui sont avant tout produites et reproduites au sein de la firme : *« Being a professional emerges as being embedded in a series of issues such as fairness, appearance, gender, sexuality and hierarchy »* (Grey 1998, p. 570).

La présentation de soi, au sens de Goffman, est ainsi particulièrement importante pour être considéré comme un professionnel de l'audit : les individus doivent adopter les bonnes manières et se comporter de manière appropriée aux circonstances, avec une autodiscipline rigoureuse (Anderson-Gough, 1998).

Dans ce sens, Grey (1994) et Anderson-Gough (2001) identifient les caractéristiques des auditeurs internes : être vêtu de façon appropriée, utiliser un langage adapté tant au cabinet que face aux clients, être ponctuel… Ils ajoutent que les auditeurs internes, pour être considérés comme professionnels, doivent aussi posséder certaines caractéristiques personnelles, comme le fait d'être compétitifs, travailleurs, jeunes…

Nous postulons donc qu'être auditeur semble se définir davantage par le comportement que par la maîtrise d'un savoir complexe. L'auditeur se définit, en tant que professionnel, par son comportement ou par ses valeurs et son engagement, plutôt que par son expertise. Kosmala et Herrbach (2006) introduisent trois indices clés de l'identité de l'auditeur :

- La conscience professionnelle ou *professional conscientiousness ;*
- La résistance professionnelle ou *professional hardiness ;*
- Le sens de la collectivité ou *collective office mode.*

Ces valeurs se sont dégagées des réponses fournies par des auditeurs à la question : *« Qu'est-ce que ça fait d'être auditeur ? »*. Selon leur étude sur l'identité des auditeurs, l'autonomie et la liberté d'organisation dans le travail sont possibles car elles se fondent sur la conscience professionnelle inhérente à la profession. Les auditeurs ont la volonté de bien faire et retirent une satisfaction personnelle du travail bien accompli.

Des études récentes signalent que les clients influencent la construction de l'identité professionnelle des auditeurs internes. Le client devient alors un autrui significatif influençant la construction de l'identité professionnelle des auditeurs. Les auditeurs acquièrent et reproduisent ainsi différents comportements en se justifiant par les attentes des clients à leur égard (Grey, 1998).

Kosmala et Herrbach (2006) expliquent que l'identité professionnelle de l'auditeur est ainsi formatée sur un modèle de progression idéal.

2.2.3.6 Vers une identité négative de l'auditeur interne : défis d'image et de perception

Deux points essentiels contribuent à transformer l'identité professionnelle de l'auditeur interne en une identité négative. En premier lieu, sous son image de professionnel de chiffre, l'un des stéréotypes comptables les plus répandus dépeint l'auditeur comme un acteur qui est presque entièrement dépourvu de sentiment. (Dimnika, 2006)

Cette identité ou image est renforcée par le *travail émotionnel* dans lequel la plupart des auditeurs sont invités à s'engager afin de projeter et de maintenir une aura de professionnalisme au travail. (Hochschild, 1983)

Comme le travail d'audit est interpersonnel, l'adoption d'une attitude non émotionnelle fait en fait partie du travail. Le terme *non émotionnel* est une expression impropre pour une orientation émotionnelle particulière, celle d'une fraîcheur d'apparence professionnelle compatible avec la technocratie. (Gill, 2009)

Francis (1994) se fonde sur les normes d'audit professionnelles en affirmant que le travail d'audit ne semble impliquer que des méthodes de raisonnement algorithmique sans émotion.

Huberty (2019) explique selon l'expérience de ces auditeurs que le mot « audit » induit principalement la peur. Elle affirme qu'un audit peut susciter des sentiments d'anxiété parce que quelqu'un pourrait vérifier votre travail, ou vous devrez peut-être accomplir un travail supplémentaire pour l'auditeur. Elle ajoute que la peur accompagne l'audit, et que les audits peuvent souvent ressembler à une punition, un peu comme une amende, une réprimande ou pire.

Cette perception négative, renforcée par la peur de l'audit, découle non seulement de la stricte technicité du travail, mais aussi de l'image d'un auditeur perçu comme un 'contrôleur froid et distant'. Ce stéréotype nuit à la collaboration efficace entre auditeur et audité, instaurant une barrière psychologique.

Ainsi, l'identité de l'auditeur interne se trouve tiraillée entre sa mission de contrôle et l'image négative qui l'accompagne, posant un défi majeur pour l'avenir de la profession.

2.2.3.7 Impact des nouvelles technologies sur l'identité professionnelle des auditeurs internes : une transformation inévitable

L'émergence de technologies telles que l'IA, l'analyse de données avancée et l'automatisation transforme profondément le métier d'auditeur interne, redéfinissant ainsi son identité professionnelle. Ces innovations imposent une évolution rapide des compétences, où les auditeurs ne sont plus uniquement des experts en matière de contrôle et de conformité, mais doivent également maîtriser des outils numériques sophistiqués. Selon PwC (2020), les auditeurs internes sont désormais confrontés à la nécessité d'intégrer ces nouvelles technologies pour mieux identifier les risques et améliorer l'efficacité des processus d'audit.

Cette transformation technologique a une incidence majeure sur la perception qu'ont les auditeurs de leur propre rôle, mais également sur leurs interactions avec les parties prenantes, qu'il s'agisse de collègues ou de clients. En intégrant des outils comme l'intelligence artificielle, les auditeurs peuvent traiter des volumes massifs de données en un temps réduit, augmentant ainsi leur capacité à fournir des recommandations précises et rapides. Toutefois, ce changement demande une adaptation culturelle et organisationnelle, car les auditeurs doivent adopter une approche plus flexible et collaborative. Velte et Stawinoga (2021) soulignent que ces nouvelles exigences augmentent la pression sur les auditeurs internes pour qu'ils deviennent à la fois des experts techniques et des consultants stratégiques.

En outre, la transition numérique ne modifie pas uniquement les compétences techniques requises, mais influence également la dynamique relationnelle au sein des organisations. Les auditeurs internes sont de plus en plus sollicités pour collaborer avec des départements tels que l'informatique ou la cybersécurité, ce qui peut entraîner des frictions interprofessionnelles mais aussi des synergies potentielles. Morales et Lambert (2022) suggèrent que cette réorganisation des rôles au sein de l'entreprise redéfinit les frontières de la juridiction professionnelle des auditeurs, nécessitant une redéfinition de leur autonomie et de leur indépendance.

Ainsi, l'intégration de l'intelligence artificielle et des outils numériques dans la pratique de l'audit contribue non seulement à la transformation des pratiques professionnelles, mais également à la redéfinition de l'identité professionnelle des auditeurs internes. L'évolution technologique exige une reformulation de leur rôle, allant au-delà de la simple conformité pour inclure des capacités d'analyse stratégique et de gestion des risques dans un environnement numérique complexe.

Conclusion intermédiaire

La partie 2.2 a permis de mettre en lumière la construction de l'identité professionnelle des auditeurs internes en soulignant les défis auxquels ces derniers sont confrontés dans un environnement professionnel en perpétuelle transformation, notamment sous l'influence croissante de la cybersécurité.

L'identité professionnelle des auditeurs internes émerge comme un processus à la fois complexe et dynamique, marqué par une adaptation constante aux évolutions technologiques et aux nouvelles attentes des organisations. Plus spécifiquement, la montée en puissance des enjeux liés à la cybersécurité bouleverse les pratiques traditionnelles et redéfinit les contours de leur légitimité et de leur champ de compétences. Alors que la fonction d'audit interne, telle que décrite par l'IIA, consiste traditionnellement à offrir une assurance indépendante sur la gouvernance et les processus de contrôle d'une organisation, les auditeurs internes sont désormais appelés à intégrer la cybersécurité au cœur de leurs missions.

Cette évolution engendre des tensions interprofessionnelles, notamment avec les départements de sécurité informatique, où les responsables de ces services se perçoivent comme plus légitimes pour traiter des enjeux techniques liés à la cybersécurité. Face à cette concurrence, les auditeurs internes doivent affirmer leur rôle stratégique auprès de la direction tout en développant les compétences techniques nécessaires à la maîtrise des risques informatiques.

Ainsi, l'auditeur interne se voit contraint de redéfinir son identité professionnelle en intégrant ces nouvelles responsabilités sans compromettre son indépendance ni son autorité. Ce rééquilibrage identitaire impose aux auditeurs de maintenir leur légitimité au sein des organisations tout en élargissant leur expertise, en particulier dans des secteurs en transformation rapide comme celui des banques, où la cybersécurité est un enjeu prioritaire.

En conclusion, la construction de l'identité professionnelle des auditeurs internes est en constante mutation, façonnée par l'accélération des innovations technologiques et les exigences croissantes en matière de sécurité. Bien que ces transformations puissent générer des tensions intersectorielles, elles sont également porteuses d'opportunités pour renforcer le rôle stratégique des auditeurs internes dans la protection des systèmes d'information et la préservation de la résilience organisationnelle.

2.3 L'identité professionnelle des responsables de la sécurité informatique : une dynamique émergente

La transition vers l'analyse du rôle et de l'identité professionnelle des responsables de la sécurité informatique est essentielle pour comprendre les dynamiques interprofessionnelles à l'ère de la transformation numérique. Contrairement aux secteurs tels que le droit ou la médecine, les recherches sur les identités professionnelles dans le domaine des technologies de l'information (TI) demeurent limitées. Tout comme les auditeurs internes, les responsables de la sécurité informatique doivent naviguer dans un environnement marqué par des risques croissants liés à la cybersécurité, ce qui influence profondément la construction et la légitimation de leur identité professionnelle

En continuité avec l'analyse des auditeurs internes, cette section explore la construction de l'identité professionnelle des responsables de la sécurité informatique, un rôle qui, bien que relativement récent, fait face à des défis similaires de légitimité et d'adaptation dans un environnement numérique en perpétuelle mutation. Comme pour les auditeurs, ces professionnels évoluent dans un cadre interdisciplinaire où les responsabilités techniques se combinent de plus en plus avec des compétences managériales et des impératifs stratégiques.

2.3.1 Une fonction en constante évolution : de la technique à la gestion stratégique

Historiquement, la fonction de sécurité informatique était centrée sur la protection des systèmes et des actifs informationnels, avec un accent particulier sur la conformité réglementaire et la gestion des risques techniques (Basie, 2005). Cependant, à l'ère de la mondialisation et de l'innovation technologique, la cybersécurité a pris une ampleur inédite. Les RSSI jouent désormais un rôle critique dans la continuité des affaires et dans la gestion globale des risques (Yaping, 2018).

Cette évolution a modifié les contours du métier. De simples experts techniques, les RSSI sont aujourd'hui des acteurs stratégiques impliqués dans les décisions organisationnelles (Krotov, 2015). Ils doivent ainsi naviguer entre des compétences techniques approfondies et un leadership managérial nécessaire pour gérer les menaces numériques complexes, tout en assurant la conformité avec des normes de sécurité en constante évolution (Weiss et Adams, 2010 ; Krotov, 2015).

Nous détaillons dans le tableau 4 suivant les représentations du rôle du responsable de la sécurité de l'information dans le management de l'entreprise selon différentes injonctions.

Tableau 4: les injonctions relatives à la gestion de la sécurité informatique

Nature de l'injonction	Auteur (s) et Année	Résultats
Injonction Structurelle	(Chang, 2006)	Les entreprises doivent établir des structures de gestion solides pour la sécurité de l'information.
Injonction Directoriale	(Knapp, 2006) ; (Ezingeard, 2007) ; (Hu, 2012) ; (Whitman, 2012) ; (Kwon, 2012)	Le soutien et l'implication de la direction influencent fortement la sécurité de l'information.
Injonction technique	(Ma, 2009)	Le soutien à la gestion est essentiel pour une sécurité informatique efficace.
Injonction Praxéologique	(Phillips, 2013)	Les pratiques managériales jouent un rôle crucial dans l'efficacité des systèmes de sécurité.

De plus, les études montrent que le facteur humain reste l'un des éléments les plus critiques de la cybersécurité. Les comportements des employés, qu'ils soient malveillants ou résultant de négligences, représentent souvent des menaces significatives pour la sécurité des informations (Vance, 2013). Le tableau 5 synthétise la littérature sur le rôle humain dans le travail de sécurité de l'information.

Tableau 5 : l'importance du facteur humain dans la gestion de la sécurité informatique

Nature	Auteur (s) et Année	Etude plus analytique
Focalisation humaine	(Loster, 2005)	Le facteur humain est central dans la sécurité de l'information.
Interaction homme/technologie	(Trcek, 2007) ; (Rhee, 2012)	L'interaction entre les employés et la technologie est complexe et essentielle à la sécurité.
Psychologie de l'utilisateur	(Yeniman, 2011), (Jaeger, 2013)	Les erreurs humaines sont souvent à l'origine des failles de sécurité.
Compétences des malveillants	(Vance, 2013)	Les initiés malveillants constituent une menace importante.

En conclusion, la gestion de la sécurité informatique nécessite une approche globale intégrant non seulement des compétences techniques, mais aussi un leadership managérial fort. Les responsables de la sécurité doivent acquérir une légitimité accrue en assumant des rôles stratégiques et en renforçant les capacités humaines et organisationnelles pour faire face aux menaces de plus en plus sophistiquées qui pèsent sur les systèmes d'information.

2.3.2 La légitimité des RSSI : un enjeu central

L'un des défis majeurs pour les RSSI est la quête de légitimité professionnelle. Contrairement

à des domaines bien établis comme le droit ou la médecine, la sécurité informatique est un secteur émergent, ce qui limite parfois la reconnaissance de ces professionnels au sein des organisations (Denis, 2009). La légitimité des RSSI se fonde non seulement sur leur expertise technique, mais aussi sur leur capacité à intégrer des compétences managériales et à influencer les stratégies de gouvernance des risques (Suddaby, 2019).

La cybersécurité est généralement confiée à des services hautement techniques, composés d'experts dont le jugement professionnel est crucial pour fournir aux dirigeants des entreprises une sécurité adéquate, une approbation réglementaire ou une évaluation de la valeur de leurs infrastructures. Andrew Abbott (1988, p. 184) souligne que ce jugement professionnel représente un travail de légitimation qui relie le diagnostic et le traitement aux valeurs culturelles dominantes.

Les dirigeants renforcent la légitimité du département informatique, non seulement en s'appuyant sur les compétences techniques des experts, mais aussi en valorisant les certifications et références qui solidifient l'autorité de ces derniers. Par exemple, une certification comme la CISSP est un atout clé pour légitimer les prétentions des responsables informatiques dans le domaine de la cybersécurité (Covaleski, 2003).

Trois formes de légitimité influencent leur reconnaissance : la légitimité pragmatique, liée aux compétences techniques ; la légitimité morale, qui repose sur la conformité aux normes éthiques et réglementaires ; et la légitimité cognitive, qui dépend de la reconnaissance culturelle et professionnelle des compétences (Suchman, 1995).

Les RSSI doivent travailler en étroite collaboration avec les autres départements de l'entreprise, notamment les ressources humaines et l'audit interne, pour asseoir leur légitimité et garantir la résilience des systèmes face aux cyberattaques (Shaikh, 2019).

La légitimité des responsables de sécurité informatique ne repose pas uniquement sur leurs compétences techniques, mais également sur leur capacité à naviguer dans les dynamiques organisationnelles et sociales pour établir leur crédibilité. La gestion efficace de cette légitimité, notamment via une légitimité pragmatique, est primordiale pour renforcer la sécurité de l'information tout en minimisant les risques organisationnels.

2.3.3 L'identité professionnelle des responsables de sécurité informatique

L'identité professionnelle des RSSI est un enjeu fondamental pour leur efficacité et leur adaptation aux exigences d'un environnement en constante évolution. Cette identité, en évolution continue, se construit autour de plusieurs éléments clés : l'expertise technique, la gestion stratégique et l'interaction avec les autres acteurs organisationnels (Schwartz, 2011 ;

Eatough, 2014).

Selon Tajfel (1978), l'identité sociale et professionnelle est renforcée par l'appartenance à un groupe valorisé. Pour les RSSI, cette identité est double : d'une part, leur rôle technique les identifie comme des experts en cybersécurité, d'autre part, ils doivent assumer des responsabilités de plus en plus stratégiques, ce qui peut créer des tensions dans la définition de leur identité professionnelle (Skorikov, 2011 ; Fuller, 2013).

2.3.3.1 Le stress lié à l'identité professionnelle

Le domaine de la cybersécurité est hautement stressant en raison de l'évolution rapide des menaces, combinée à une pression constante pour protéger les systèmes d'information. Philipe Trouchaud (2018) souligne que les responsables de sécurité informatique (RSSI) sont souvent perçus comme les boucs émissaires en cas de cyberattaque, peu importe la réussite ou l'échec des systèmes de défense. Cette charge mentale, accentuée par une équipe souvent sous-dimensionnée, engendre une grande source de stress pour les RSSI, qui sont constamment sous pression pour anticiper et répondre aux cybermenaces. La tension entre les exigences de performance et la perception de culpabilité dans le cas d'une attaque ratée alimente un stress continu dans ce métier, souvent perçu comme un fardeau psychologique (Bochman, 2019).

2.3.3.2 Une identité professionnelle en mutation

Le rôle de responsable de la sécurité informatique est en constante évolution. Autrefois centré sur des compétences techniques traditionnelles, il s'étend aujourd'hui à la gestion stratégique et à la diplomatie inter-organisationnelle. Cette évolution est encore plus visible dans les entreprises où le RSSI provient souvent d'horizons professionnels éloignés, tels que la gestion des services généraux ou la sécurité physique, ce qui peut nuire à la reconnaissance de leur compétence dans le domaine cybernétique (Trouchaud, 2018).

Il devient ainsi crucial pour ces professionnels de développer non seulement leurs compétences techniques, mais aussi des compétences managériales et stratégiques pour répondre aux exigences contemporaines de la cybersécurité.

2.3.3.3 L'évolution de la profession de RSSI : entre technique et gestion

La profession de la sécurité informatique ne partage pas encore pleinement les caractéristiques des professions établies, notamment en raison des barrières relativement faibles à l'entrée (Donnelly, 2011).

Cependant, à mesure que le secteur évolue, il devient nécessaire pour les professionnels de la sécurité de développer un ensemble diversifié de compétences, allant de la maîtrise des outils techniques à des compétences en gestion de projets et en relations interpersonnelles (Marks, 2007).

Une telle évolution est essentielle pour que les RSSI soient perçus non seulement comme des techniciens experts, mais aussi comme des leaders capables de naviguer dans des environnements organisationnels complexes.

2.3.3.4 Le conflit d'identité des RSSI

Ce passage du rôle technique à un rôle plus managérial peut provoquer un conflit d'identité. En effet, certains RSSI peuvent ressentir une dévalorisation de leurs compétences techniques lorsqu'ils sont promus à des postes de direction ou se voient confier des responsabilités administratives (Hotho, 2008).

Un conflit d'identité a été observé lorsque les participants étaient seuls responsables de l'informatique avec peu d'intérêt manifesté par les supérieurs hiérarchiques ou quand ils ne se sentaient pas reconnus. L'identité a également été jugée problématique lorsque l'investissement informatique devait être justifié et que l'identité organisationnelle des responsables informatiques était mise à l'épreuve dans ce processus. Sally Smith (2016, p. 68) a observé que ce conflit est particulièrement présent chez les professionnels qui, après avoir acquis une expertise technique avancée, sont promus à des postes de direction, mais ressentent une perte de leur identité technique. Il devient ainsi crucial pour les RSSI de trouver un équilibre entre leurs responsabilités techniques et managériales, afin de surmonter ces tensions identitaires et de s'adapter aux besoins stratégiques de l'organisation. L'identité professionnelle des RSSI est une composante cruciale de leur efficacité dans un environnement où les cybermenaces évoluent rapidement. La maîtrise de compétences techniques, associée à des aptitudes managériales, permet de renforcer cette identité, tout en réduisant les conflits qui peuvent surgir entre les différentes facettes de leur rôle. Pour améliorer leur bien-être professionnel et garantir une gestion optimale de la cybersécurité, il est essentiel que les RSSI soient mieux intégrés dans les processus décisionnels stratégiques des entreprises et qu'ils bénéficient d'un soutien organisationnel adéquat.

2.3.4 Revalorisation des RSSI : dynamiques identitaires et organisationnelles à l'ère de la cybersécurité stratégique

Malgré leur rôle clé dans la sécurisation des infrastructures numériques, les RSSI restent souvent sous-évalués au sein des organigrammes d'entreprise (Trouchaud, 2018). Les entreprises doivent repenser la place de la cybersécurité dans leur hiérarchie, en intégrant davantage les RSSI dans les décisions stratégiques. Une meilleure reconnaissance de la fonction passe par une revalorisation de leur expertise et par une plus grande légitimité au sein des comités de direction. Pour surmonter les tensions identitaires, il est crucial que les RSSI

bénéficient de formations continues et d'un soutien organisationnel fort, leur permettant de naviguer entre leurs rôles techniques et managériaux, et d'assurer une gestion proactive des risques cyber. La profession de responsable de la sécurité informatique se trouve à la croisée de plusieurs dynamiques identitaires et organisationnelles. Alors que les RSSI sont de plus en plus intégrés dans les processus décisionnels stratégiques, leur identité professionnelle évolue, entre technicité, gestion des risques et leadership managérial. La reconnaissance de leur légitimité, tant au niveau technique que managérial, est cruciale pour assurer une cybersécurité efficace et pérenne au sein des organisations. Pour renforcer cette identité, il est nécessaire que les RSSI continuent à développer des compétences diversifiées et à asseoir leur rôle stratégique dans la gestion des risques cyber.

Conclusion intermédiaire

Cette partie 2.3 a permis d'explorer les différentes dimensions de l'identité professionnelle des RSSI et les défis spécifiques auxquels ils sont confrontés dans un contexte technologique en évolution rapide. Alors que la cybersécurité s'impose comme une priorité stratégique pour les entreprises, l'identité professionnelle des RSSI se complexifie, nécessitant une adaptation constante. Tout d'abord, la transformation de leur rôle, qui s'étend au-delà des compétences techniques, implique désormais des responsabilités managériales et stratégiques croissantes. Les RSSI sont devenus des acteurs clés de la gouvernance des risques numériques, appelés à naviguer entre la protection des infrastructures techniques et la prise de décisions stratégiques (Schwartz, 2011 ; Eatough, 2014). Cette extension de leurs attributions illustre l'évolution vers un rôle davantage axé sur le leadership et la gestion des risques organisationnels. Ensuite, la quête de légitimité professionnelle constitue un enjeu crucial pour les RSSI. Si leur expertise technique reste au cœur de leur reconnaissance, ils doivent également développer des compétences managériales afin de gagner la confiance des décideurs et de s'imposer comme des leaders dans la gestion globale de la cybersécurité (Covaleski, 2003). Cette dualité dans leur identité professionnelle — entre technicité et leadership — alimente une tension permanente qui peut entraîner des conflits identitaires, en particulier lorsque les professionnels doivent s'éloigner de leurs compétences techniques pour assumer des fonctions managériales (Hotho, 2008 ; Smith, 2016). Par ailleurs, le stress professionnel exacerbé par la pression constante de la prévention des cybermenaces contribue à des tensions identitaires. Ce fardeau psychologique, amplifié par la nécessité d'anticiper et de répondre rapidement aux cyberattaques, souligne l'importance de soutenir les RSSI pour qu'ils puissent concilier leur expertise technique avec leurs nouvelles responsabilités stratégiques (Trouchaud, 2018). Il est indispensable pour les RSSI de renforcer leurs compétences en leadership. La gestion des équipes, la coordination

inter-fonctionnelle et la collaboration avec les autres départements de l'organisation deviennent des composantes essentielles de leur rôle (Marks, 2007). Ce développement de compétences transversales est nécessaire pour répondre aux exigences contemporaines de la cybersécurité, qui repose de plus en plus sur des stratégies globales et une approche organisationnelle intégrée. L'identité professionnelle des RSSI évolue en parallèle de l'importance accrue de la cybersécurité pour les entreprises. Leur efficacité dépend de leur capacité à allier expertise technique et compétences en gestion, tout en surmontant les tensions identitaires liées à cette transition. À mesure que leur rôle se diversifie, il devient impératif de mieux les intégrer dans les processus décisionnels stratégiques et de leur offrir un soutien organisationnel adapté, garantissant ainsi une gestion proactive et holistique des risques cyber.

2.4 Le conflit juridictionnel a priori des auditeurs internes et des RSSI

Cette partie examine le conflit potentiel de juridiction entre les auditeurs internes et les responsables de la sécurité informatique, en s'appuyant sur les notions d'identité professionnelle et de légitimité propres à chaque fonction. Alors que l'identité professionnelle des auditeurs internes repose sur des valeurs telles que le comportement et l'engagement, celle des responsables de sécurité informatique se fonde principalement sur leur expertise technique et leurs compétences.

Nous utiliserons la notion de juridiction développée par Abbott (1988) pour éclairer ce conflit.

2.4.1 La notion de juridiction

Abbott (1988) a avancé que le contrôle d'un groupe sur son système de connaissances est crucial pour revendiquer une stature professionnelle. Ce contrôle permet à une profession de définir et redéfinir les problèmes sociétaux qu'elle traite, d'élaborer des solutions adaptées, et de défendre ses prérogatives face à d'autres professions concurrentes. Il est donc essentiel de comprendre comment les auditeurs internes et les responsables de la sécurité informatique cherchent à établir et à maintenir leur légitimité respective. Dans cette perspective, Dubar (2015) explique que *« les professions, reconnues comme telles, sont celles qui sont parvenues à monopoliser un segment du marché du travail, à faire reconnaitre leurs compétences juridiques et à légitimer leurs privilèges sociaux ».*

Cette dynamique est à l'œuvre entre l'audit interne, qui se fonde sur la rationalité et l'efficacité, et la sécurité informatique, qui est pragmatique et dépend de l'acquisition de ressources techniques (Payette, 2014).

2.4.2 La lutte pour le contrôle des connaissances

Il est nécessaire pour une profession de recréer continuellement son système abstrait de connaissances, d'étendre ainsi sa juridiction pour empiéter éventuellement sur celle des professions adjacentes. (Reed, 1996)

Le conflit entre ces deux groupes professionnels s'intensifie lorsque des changements organisationnels surviennent, comme l'introduction d'un nouvel outil de gestion ou l'adoption d'une nouvelle stratégie (Briers, 2001). Dans ce cadre, chaque profession cherche à définir les problèmes qui affectent son domaine et à revendiquer des compétences spécifiques.

Pour illustrer ce phénomène, Ezzamel (2005) souligne que la position d'un groupe dépend de sa capacité à formuler des définitions favorables à ses intérêts. Les auditeurs internes, en cherchant à établir leur expertise en cybersécurité, tentent d'étendre leur juridiction sur un

domaine qui relève historiquement des responsables de la sécurité informatique. Cette dynamique est exacerbée par la tendance de chaque groupe à protéger son territoire et à revendiquer une expertise spécifique, créant ainsi une compétition pour la légitimité.

2.4.3 L'échec de la revendication juridictionnelle

Malgré leurs efforts, les auditeurs internes rencontrent des obstacles dans leur tentative d'étendre leur juridiction au domaine de la cybersécurité. Abbott (1988) indique que la force d'une revendication juridictionnelle diminue lorsque les connaissances d'un groupe deviennent trop vagues. Ce manque de précision est particulièrement problématique dans le contexte actuel où les compétences techniques en sécurité informatique sont primordiales.

Les résultats d'une enquête menée par la Fondation indiquent que seulement 20 % des auditeurs internes sont impliqués dès les phases de conception des projets informatiques, ce qui reflète leur position marginale dans les décisions stratégiques liées à la cybersécurité (Jamison, 2018). Cette situation souligne que, sans un soutien significatif de la direction et des parties prenantes, l'audit interne risque de ne pas être en mesure de revendiquer une juridiction effective en cybersécurité.

2.4.4 Le rôle des parties prenantes et de l'environnement juridique

La cybersécurité est un territoire de dispute entre les auditeurs internes et les responsables de la sécurité informatique. Cette concurrence se manifeste lorsque des conflits surgissent lors de changements clairement identifiés, comme l'apparition d'une nouvelle orientation stratégique ou organisationnelle. Le fait que la cybersécurité devienne, dans les banques, un problème central, a aiguisé ce jeu concurrentiel. Pour élargir ou défendre leur juridiction, les professions revendiquent une expertise ou des connaissances sur la problématique. De telles revendications peuvent être faites dans l'arène publique pour persuader l'opinion publique. Elles peuvent être faites dans l'arène juridique pour gagner la reconnaissance et la protection de la juridiction d'une profession, ou elles peuvent être effectuées sur le lieu de travail en effectuant certains types de travaux *(Légitimité par la preuve)* (Abbott, 1988, pp. 59-69).

Dans ce contexte concurrentiel, la perception du public joue un rôle crucial dans la légitimation des revendications professionnelles. Selon Abbott (2003), les groupes professionnels doivent non seulement répondre à leurs propres objectifs, mais aussi tenir compte des attentes des auditoires, qui incluent clients, gestionnaires et partenaires. Les auditeurs internes doivent naviguer entre les attentes de leurs parties prenantes tout en essayant de formuler des revendications de légitimité basées sur une expertise en cybersécurité. Cependant, leur manque de compétences techniques spécifiques en informatique et leur absence de soutien

organisationnel limitent leur capacité à étendre leur juridiction sur ce domaine.

2.4.5 Dynamique des sources internes et externes

Selon Abbott (1988), la concurrence entre professions agit comme un moteur de développement. Les professions sont définies par les travaux qu'elles accomplissent, et leur capacité à établir des juridictions est essentielle pour leur évolution. Les perturbations du système peuvent être de deux types : externes et internes.

2.4.5.1 Les sources externes de perturbation

Les forces externes modifient directement le système en ouvrant de nouvelles zones de compétence. Par exemple, l'émergence de nouvelles technologies et la montée des cybermenaces ont créé une nécessité pressante d'expertise en cybersécurité, redéfinissant ainsi les compétences requises dans le secteur bancaire. Robert Mueller, ancien directeur du FBI, a déclaré en 2020 : *« Il n'y a que deux types d'entreprises : celles qui ont été piratées et celles qui le seront »*. Cette évolution met en lumière l'importance d'une vigilance accrue des équipes informatiques face à la montée des cybermenaces (Forrest, 2020).

La perturbation des professions d'audit interne et de responsables informatiques dans le secteur bancaire résulte des facteurs externes comme la naissance d'une nouvelle technologie (Internet) et d'une nouvelle tâche (l'assurance de la cybersécurité) dans le secteur bancaire. Ces deux facteurs ont entrainé une création et une destruction des juridictions dans la banque pour assurer la cybersécurité.

2.4.5.2 Les sources internes de perturbation

Les perturbations internes sont des forces qui changent le système de l'intérieur, souvent en renforçant ou en redéfinissant les juridictions existantes. Les avancées dans les connaissances ou les pratiques peuvent consolider la légitimité d'une profession, mais elles peuvent également provoquer des expansions aux dépens d'autres. Par exemple, l'expérience accumulée par les auditeurs internes au fil de leurs missions peut, à terme, perturber les juridictions des autres professions auditées (Abbott, 1988). L'audit interne a cette particularité d'investir, le temps d'une mission, les juridictions des professions auditées. Mais, dans le long terme, l'expérience cumulée de l'audit interne peut perturber la juridiction des professions auditées.

2.4.6 Règlements juridictionnels

Les règlements juridictionnels, tels que définis par Abbott (1988), incluent la pleine juridiction, la juridiction subordonnée, la juridiction intellectuelle, la juridiction consultative, la juridiction divisée et la juridiction différenciée par clients. Nous examinerons ci-dessous comment ces règlements se manifestent dans la relation entre auditeurs internes et responsables de la sécurité

informatique.

La pleine juridiction est souvent revendiquée à travers diverses méthodes, généralement appuyées par des cadres juridiques. Dans le contexte de la cybersécurité, bien que cette compétence relève principalement des responsables informatiques, les auditeurs internes peuvent également prétendre à ce domaine en raison de leur indépendance professionnelle, leur permettant d'analyser et de formuler des avis sur ces questions (Abbott, 2003).

En ce qui concerne la juridiction subordonnée, elle se manifeste lorsque des groupes non-professionnels sont autorisés à exécuter certaines tâches, autrefois réservées à une profession spécifique. Par exemple, lorsqu'une fonction de cybersécurité est instaurée suite aux recommandations des auditeurs internes, cela introduit une dynamique de subordination entre les responsables informatiques et les auditeurs, générant ainsi des tensions quant à leurs champs d'autorité respectifs (Arena, 2010).

En matière de juridiction intellectuelle, elle se produit lorsque la profession dominante cherche à contrôler la base de connaissances d'une profession subalterne. Dans le domaine de la cybersécurité, bien que les auditeurs internes puissent proposer des protocoles de sécurité, leur légitimité à le faire est souvent remise en question par leur manque de compétence technique spécifique à la cybersécurité (Abbott, 2003).

Par ailleurs, la juridiction consultative se manifeste lorsque la profession dominante revendique le droit de modifier ou d'interpréter les actions d'une profession subalterne. Dans ce contexte, les auditeurs internes, bien qu'ils travaillent aux côtés des responsables de la sécurité informatique, conservent le droit d'interpréter les actions relatives à l'assurance de la cybersécurité (Abbott, 1988).

La juridiction divisée se retrouve lorsque la responsabilité de la cybersécurité est partagée entre les auditeurs internes et les responsables de la sécurité informatique. Cette répartition des responsabilités reflète l'indépendance des deux professions et souligne la collaboration requise pour une gestion efficace de la cybersécurité. Enfin, la juridiction différenciée par clients fait référence aux divisions qui peuvent émerger dans l'organisation, souvent en désaccord avec les structures juridictionnelles officielles. Les conseils d'administration et les parties prenantes jouent ici un rôle essentiel dans la légitimation des revendications juridictionnelles, bien que la littérature ne fournisse pas de réponses claires quant aux choix opérés dans ce domaine spécifique de l'audit interne et de la cybersécurité (Abbott, 1988).

Nous présentons ci-dessous un schéma illustrant les principaux éléments de la théorie d'Abbott appliqués au système des professions d'audit interne et de sécurité informatique dans le cadre de la cybersécurité. Ce schéma explicite les règlements juridictionnels, les sources internes et

externes, ainsi que les lieux de juridiction existant entre ces deux fonction

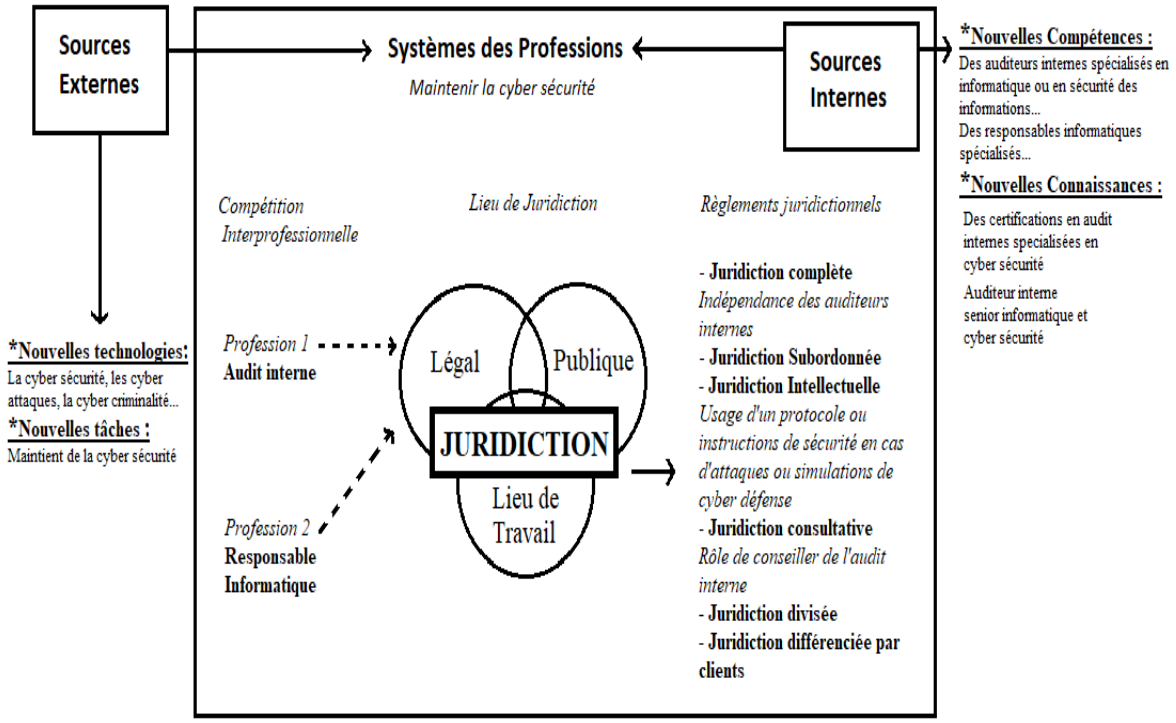


Figure 13: le schéma d'ABBOT appliqué à l'audit interne et à la RSSI

Source: the system of professions : an essay of the division of expert labor (Abbott, 1988).

Conclusion intermédiaire

Les responsabilités conflictuelles des auditeurs internes et des responsables de la sécurité informatique dans le domaine de la cybersécurité constituent une problématique complexe et multiforme. Pour appréhender cette contradiction, nous avons mobilisé la théorie des systèmes professionnels formulée par Abbott. Sur le plan de la légitimité professionnelle, les auditeurs internes fondent leur légitimité sur un engagement envers l'expertise et les valeurs d'audit, tandis que les responsables de la sécurité informatique s'appuient sur leurs compétences techniques pour justifier leur rôle. Cette divergence se manifeste dans la manière dont chaque profession revendique un contrôle sur le système de connaissances liées à la cybersécurité. Selon Abbott, la capacité à définir les problèmes, développer des techniques et maintenir un contrôle formel sur les définitions clés du service professionnel est essentielle pour revendiquer une stature professionnelle.

Il est notable que chaque groupe professionnel cherche à élargir son domaine de compétence en formulant activement des problèmes spécifiques à son champ d'expertise. En ce qui concerne

la cybersécurité, les auditeurs internes expriment une volonté d'élargir leur expertise dans ce domaine. Cependant, leur manque de compétences techniques complique leur capacité à revendiquer la responsabilité des questions de cybersécurité. Dans ce contexte, la capacité de convaincre les parties prenantes et de créer une justification tant morale que pratique s'avère cruciale. Les évolutions technologiques, telles que l'essor d'Internet, ainsi que les changements de rôles au sein du secteur bancaire, influencent également les responsabilités des auditeurs internes et des responsables de la sécurité informatique, particulièrement en matière de cybersécurité. Nous avons exposé les différents règlements de juridiction entre ces deux professions, allant de la pleine juridiction, où les deux groupes sont en concurrence, à des formes plus subordonnées, intellectuelles, consultatives, partagées ou différenciées, selon la capacité de chaque groupe à influencer et à contrôler certaines dimensions du travail en cybersécurité.

Le conflit de juridiction qui émerge entre auditeurs internes et responsables de la sécurité informatique résulte donc d'une lutte pour le contrôle des connaissances et de la légitimité professionnelle. Bien que les règles juridictionnelles varient en fonction des circonstances et des évolutions, il est crucial de comprendre comment ces deux professions se positionnent dans un environnement en constante mutation. La capacité à influencer les parties prenantes et à démontrer la pertinence de son expertise est essentielle pour chaque groupe professionnel.

Cette partie vise à structurer les idées de manière plus fluide et à accentuer certains points clés tout en conservant l'essence de votre synthèse originale.

Synthèse du chapitre 2 : relations et dynamiques identitaires au sein de la cybersécurité

Au long de ce chapitre, nous avons examiné la complexité de l'identité professionnelle et les conflits de juridiction dans le domaine de la cybersécurité bancaire, en mettant en exergue les rôles des auditeurs internes et des responsables de la sécurité des systèmes d'information (RSSI). En premier lieu, nous mettons en évidence la manière dont des conflits d'identité peuvent émerger lorsque des professionnels se voient confier des responsabilités divergentes ou concurrentes en matière de cybersécurité. Les auditeurs internes, en tant que gardiens de l'intégrité organisationnelle, peuvent entrer en tension avec les RSSI, ces derniers se percevant comme les spécialistes techniques chargés de protéger les infrastructures numériques. Cette dynamique de rivalité identitaire peut générer des désaccords sur les meilleures pratiques à adopter pour assurer la cybersécurité.

Par ailleurs, nous soulignons l'importance des « tribunaux professionnels », concept qui renvoie à la manière dont les experts cherchent à définir et à légitimer leur propre juridiction pour affirmer leur autorité sur un domaine donné. Dans le contexte de la cybersécurité bancaire, cela se traduit souvent par des conflits de responsabilité entre les auditeurs internes et les RSSI, chacun cherchant à établir son rôle comme central. Toutefois, il est important de noter que ces conflits identitaires et de compétences ne sont pas nécessairement négatifs. Ils peuvent favoriser des échanges constructifs, clarifier les responsabilités respectives, et aboutir à une meilleure collaboration, renforçant ainsi la cybersécurité des organisations. Cependant, une gestion appropriée de ces tensions est indispensable pour que la coopération soit véritablement efficace.

Ce chapitre a également permis d'explorer la construction de l'identité professionnelle des auditeurs internes et des RSSI. Les auditeurs internes se voient confrontés à de nouvelles responsabilités liées à la sécurité informatique, soulevant des questions sur leur légitimité et leur compétence dans ce domaine en perpétuelle mutation. De leur côté, les RSSI élargissent leurs fonctions pour inclure des aspects stratégiques et managériaux, en complément de leurs compétences techniques traditionnelles.

Enfin, nous avons analysé les conflits de juridiction à la lumière de la théorie des systèmes professionnels développée par Abbott. Ces conflits découlent de la lutte pour le contrôle des connaissances et de la légitimité professionnelle, et leur résolution peut prendre diverses formes, allant de la juridiction exclusive à des compromis partagés, selon le contexte organisationnel et professionnel.

PARTIE 2.

METHODOLOGIE DE LA RECHERCHE ET RESULTATS EMPIRIQUES

CHAPITRE 3.

CADRE METHODOLOGIQUE ET DESIGN DE RECHERCHE

Sommaire du chapitre 3. Cadre méthodologique et design de recherche

3.5 Codage des récits et des données

3.5.1 L'intérêt du codage conçu par Dubar et Demazière

3.5.2 La conception du codage selon Dubar et Demazière

3.5.3 La démarche de codage

3.5.4 Les questions d'analyse et de collecte

Conclusion intermédiaire

3.6 Analyse inter-cas : faire sens d'expériences contrastées

3.6.1 L'intérêt de l'analyse inter-cas

3.6.2 Les modalités de l'analyse inter-cas

Conclusion intermédiaire

Synthèse du chapitre 3 : évaluation des méthodes et perspectives de recherche

3. Cadre méthodologique et design de recherche

Ce chapitre a pour objet de retracer la méthodologie de recherche utilisée pour étudier le rôle de l'audit interne dans la cybersécurité d'établissements bancaires en France et au Liban et répondre à nos questions de recherche. Nous explicitons ainsi les choix qui ont été opérés tout au long de notre recherche.

Le design de recherche confère à la phase empirique le statut d'une étape diagnostique, utilisée pour comprendre et analyser un problème ou situation spécifique (De Robertis, 2014).

Nous avons choisi cette démarche pour analyser comment les banques libanaises et françaises gèrent la cybersécurité, ainsi que pour évaluer le niveau de collaboration entre les auditeurs internes et les RSSI.

La démarche diagnostique consiste à définir et clarifier les objectifs spécifiques comme comprendre comment les banques gèrent la cybersécurité et évaluer le niveau de collaboration entre les auditeurs internes et les RSSI. Ensuite, les informations pertinentes sur les pratiques de cybersécurité des banques - leurs structures organisationnelles, les politiques et procédures en place, ainsi que les interactions entre les auditeurs internes et les RSSI – sont rassemblées. Cette analyse est effectuée sous l'angle des identités professionnelles à l'œuvre. A travers les résultats de recherche, prenons la mesure des forces et faiblesses de la gestion de la cybersécurité, notamment celles qui dépendent des relations interprofessionnelles entre les auditeurs internes et les RSSI. Cette analyse articule des monographies puis une approche inter-cas entre les pratiques des banques libanaises et françaises.

Ce chapitre se divise en cinq sous parties. Nous évoquons les problèmes confrontés sur les terrains bancaires libanais et français en expliquant le concept de dynamique identitaire qui ressort à travers la méthodologie d'analyse des entretiens biographiques proposée par Dubar et Demazière (1999). Nous complétons par une démarche diagnostique de compréhension de la manière dont les établissements s'organisent pour gérer la cybersécurité et de leur degré de prise en compte des relations interprofessionnelles. Nous privilégions une méthodologie interprétativiste et une approche qualitative sur le terrain. Nous détaillons notre méthode de collecte de données et de codage. Nous concluons ce chapitre par une analyse inter cas entre la BPVF et les banques libanaises qui nous permet de mieux comprendre les différences et les similitudes entre les cas et de produire des connaissances approfondies sur le rôle de l'audit interne dans la gestion de la cybersécurité bancaire.

3.1 Contexte de la recherche et accès au terrain : un rapport contrasté et évolutif à la cybersécurité dans les établissements bancaires

Le secteur bancaire et financier a besoin de systèmes sûrs, résilients et fiables pour assurer des opérations transparentes et maintenir la confiance du public dans les systèmes monétaires. De nombreuses institutions financières sont à l'avant-garde du développement des meilleures pratiques et du déploiement de technologies avancées pour sécuriser leurs systèmes et leurs actifs. (Abend, 2008)

Plus important encore, la cybersécurité fournit une assurance de sécurité et constitue aujourd'hui un fondement de la confiance dans les établissements bancaires. Dans ce sens, Trouchaud (2018) affirme que la mise en place d'une cybersécurité raisonnée et humaine peut faire naître les chemins d'une *« nouvelle confiance »*. La cybersécurité raisonnée peut restaurer la confiance aux clients dans le secteur bancaire et créer la réassurance dans ce climat de confiance. Mais la sécurité de l'information reste une préoccupation importante pour toutes les institutions du secteur bancaire et financier. Les institutions financières sont constamment ciblées par des criminels et d'autres personnes aux intentions malveillantes. Nous citons par exemple la crise de grande ampleur engendrée par WannaCry. Ce n'est plus seulement un problème de cybersécurité, ni de sécurité, c'est non seulement un problème économique mais aussi un problème de confiance.

Pour résoudre ces problèmes et faire face aux cyberattaques, les banques investissent constamment dans ce monde évolutif et risqué. Le secteur bancaire fait face à de nombreux défis et travaille en permanence pour améliorer les défenses contre les attaques, renforcer la résilience et maintenir la confiance du public dans des relations bancaires de confiance. Le secteur financier s'appuie fortement sur les systèmes d'information pour les entreprises. Le secteur perçoit des cybermenaces contre l'infrastructure financière sous-jacente, ainsi que contre la disponibilité des services informatiques et la confidentialité des données, en plus du vol financier. Le secteur est particulièrement préoccupé par le potentiel de perte de réputation dû aux cyberattaques. La menace interne suscite également des inquiétudes particulières.

Nous pouvons faire l'hypothèse qu'une cybersécurité réfléchie et axée sur l'humain peut rétablir et renforcer la confiance des clients dans le secteur bancaire. Dans le secteur bancaire, les clients font plus de confiance au capital de marque qu'à la technologie elle-même. Sans cybersécurité, les banques détruiront leur capital de marque. La cybersécurité est l'un des outils des banques pour restaurer cette confiance. Dans l'émotion, globalement, les employés agissent

dans la précipitation et oublient souvent les bases de leur métier. Ce n'est pas surprenant, la responsabilisée de la question cyber reposant généralement sur une personne. (Trouchaud, 2018)

La cybersécurité n'est pas une question purement technologique, mais elle est liée à l'organisation et aux facteurs humains. La cybersécurité, dans le secteur bancaire en particulier, demande des compétences humaines, des investissements financiers, mais aussi et surtout une organisation nouvelle. Seule cette nouvelle approche tant managériale qu'organisationnelle permettra aux banques une gestion sereine du cyberrisque, sans pic d'émotion.

3.1.1 Un accès au terrain contrasté

Il faut noter que dans le secteur bancaire, il existe des divergences entre les défenseurs du renforcement de la régulation et ceux qui sont contre. Les premiers visent en effet à empêcher les écarts ainsi que les actions abusives, tandis que les derniers estiment que la régulation est à l'origine d'un rigorisme contraignant et qu'elle n'est pas toujours à jour. En d'autres termes, l'objet de notre étude, la banque de détail, s'inscrit pleinement dans cette ère de risque qui caractérise la banque et le secteur bancaire au sens général.

3.1.1.1 Le terrain bancaire libanais

La cybersécurité est un domaine sensible plein de risques et constitue une problématique essentielle afin de lutter contre les fraudes et les cyberattaques. Nous avons rencontré plusieurs problèmes durant la phase de collecte de données, particulièrement sur le secteur bancaire libanais. La crise sanitaire engendrée par le COVID-19 ainsi que le début de la crise économique et la manifestation du 17 octobre 2019 ont renforcé la pression sur les systèmes informatiques des banques libanaises. La crise sanitaire liée au Coronavirus a accéléré l'évolution des usages bancaires numériques : transactions sans contact, achats en ligne, travail à distance. La manifestation du 17 octobre a touché les banques libanaises qui sont restés fermées pendant deux semaines et des mesures illégales de contrôle des capitaux ont été appliquées. Il y a eu plusieurs manifestations à la Banque centrale et au siège de plusieurs banques pour dénoncer la fraude et la corruption du système bancaire, et en même temps, plusieurs routes principales ont été fermées. (Babin, 2022)

Le secteur bancaire demeure un secteur particulier où les banques sont en concurrence permanente. Nous étions aussi en difficulté d'obtenir des informations qui relèvent du secret professionnel.

Pour ces raisons, nous avons essayé d'augmenter le nombre de banques étudiées dans le but

d'aboutir à des résultats diversifiés. En ce qui concerne les informations et les statistiques spécifiques au Liban, il était difficile de trouver des chiffres à jour voire plus simplement d'obtenir des données. De ce fait, nous avons réalisé plusieurs entretiens avec les acteurs principaux (auditeurs internes ou directeur d'audit interne, RSSI ou Responsables informatiques) qui ont enrichi notre thèse, et grâce à qui nous avons pu recueillir des informations significatives. Le manque de documentation, notamment de recherche scientifique, est particulièrement prononcé en ce qui concerne les aspects informels, le commerce illégal et l'aide économique non déclarée au Liban. De plus, les tabous liés aux équilibres socio-politiques et sécuritaires rendent impossible l'accès aux données et statistiques sur des partis politiques spécifiques ou des individus spécifiques appartenant à des groupes politiques considérés comme des organisations terroristes ou de financement du terrorisme. L'accès aux données était presque impossible. Certaines personnes ont refusé de répondre à nos questions relatives à la cybersécurité pour des raisons de sécurité, car le sujet de la cybersécurité est sensible et concerne toutes les données. De plus, ceux qui nous ont fourni des informations ont préféré rester anonymes et ne pas être enregistrés ou filmés afin que nos conversations ne puissent pas être retracées. De plus, divulguer ces informations est en soi risqué, car l'aspect informel affecte les dirigeants de partis politiques et des personnalités publiques qui veulent cacher leurs sources de financement illicites et leur rôle dans le secteur bancaire.

Précisons de surcroît qu'il est difficile de recueillir des informations approfondies sur les pratiques, car peu de recherches ont été réalisées à ce sujet au Liban. Notre travail analysera les informations qualitatives et se concentrera sur le rôle de l'audit interne dans la cybersécurité des banques. Les établissements sollicités se situent dans le premier groupe du marché bancaire libanais : Banque Audi, BLOM Banque, Byblos Banque, Fransabank, Société générale de banque au Liban (SGBL), Banque of Beirut, Bank Med, Banque Libano-Française (BLF).

3.1.1.2 Le terrain bancaire français

L'économie française s'appuie sur l'un des moteurs fondamentaux de sa croissance et de son indépendance : un système bancaire doté d'un cadre clair et concurrentiel qui doit inspirer confiance aux usagers. Depuis 2008[4], il était impératif pour les banques de restaurer et de renforcer la stabilité financière tout en assurant une reprise robuste et durable et en créant des

[4] La crise bancaire et financière de la fin de l'été 2008, aussi connue comme la crise estivale de 2008, est la seconde phase de la crise financière mondiale de 2007-2008, après la crise des subprimes de l'été 2007 et le temps fort de la crise économique mondiale des années 2007-2012. (Wikipédia 2022, Crise bancaire et financière de l'automne 2008.)

emplois. Un bilan récent des progrès des banques françaises montre qu'elles n'ont pas failli à cette mission. (Prot, 2022)

Afin de connaître les résultats de la cybersécurité dans les banques françaises, nous avons choisi de mener huit entretiens auprès d'une banque française : la BPVF, Banque Populaire Val-de-France. Nous exposons les motifs de ce choix dans la suite. Nous avons mené ces entretiens avec les employés les plus concernés par notre problématique. Nous avons fait face à divers problèmes lors de la collecte de données puisque le secteur bancaire français, comme le secteur bancaire libanais, est un domaine sensible porteur de risques plus précisément, en cybersécurité. Nous ne devons pas non plus oublier l'impact de la crise sanitaire engendrée par le COVID-19 sur le terrain bancaire français.

3.1.1.3 Analyse contextuelle des enjeux de cybersécurité bancaire : une comparaison des dynamiques libanaises et françaises

Les contextes libanais et français présentent des contrastes significatifs en matière de cybersécurité bancaire, notamment en ce qui concerne les conditions d'accès au terrain et les enjeux spécifiques à chaque environnement. D'une part, le secteur bancaire libanais est caractérisé par une instabilité économique et politique prononcée, ainsi qu'une opacité des données, rendant l'accès aux informations à la fois complexe et sensible. Les dynamiques socio-politiques et la crise économique exercent une influence directe sur les pratiques de cybersécurité et la coopération entre les différents acteurs. D'autre part, bien que plus stable et structuré, le secteur bancaire français fait face à des défis distincts, notamment en termes de confidentialité des données, de risques réputationnels et des impacts de la crise sanitaire.

Ces divergences mettent en évidence la nécessité de considérer les dynamiques contextuelles propres à chaque environnement pour analyser les pratiques de cybersécurité et les interactions professionnelles entre auditeurs internes et RSSI. Cette approche comparative prépare le terrain pour une analyse approfondie des "matériaux sensibles" recueillis et de la méthodologie employée, permettant ainsi de dégager des enseignements pertinents pour chaque cas étudié.

3.1.2 Des matériaux chauds offerts à l'analyse

Adopter un point de vue d'extériorité par rapport au terrain étudié est souvent perçu comme gage de scientificité. Dans cette optique, le chercheur est tenté de se fonder sur des matériaux « froids » sans lien avec la pratique comme par exemple les statistiques, les rapports, les données existantes… (Aggeri, 2016).

Nous privilégions au contraire, une étude des matériaux « chauds » des problèmes et des enjeux

d'actualité qui s'accordent au sujet de la cybersécurité dans les établissements bancaires. Nos sources doivent donc s'appuyer sur des entretiens et observations. En effet, dans le contexte de la cybersécurité bancaire, les relations interprofessionnelles, la culture organisationnelle et les perceptions des acteurs jouent un rôle primordial dans la manière dont les politiques et pratiques de sécurité sont mises en œuvre et acceptées. Notre choix vers une approche interventionnelle et qualitative, centrée sur des « matériaux chauds », nous permet d'aller au-delà des cadres rigides pour explorer la complexité des interactions humaines. Cette approche est particulièrement pertinente car elle permet de révéler les subtilités des rapports de pouvoir, des conflits identitaires et des stratégies d'adaptation au sein des organisations. En nous concentrant sur les discours, les représentations et les pratiques des acteurs clés – auditeurs internes, RSSI, responsables informatiques –, nous capturons des données riches et nuancées, souvent négligées par les analyses technocentriques. Notre choix méthodologique s'inscrit donc dans une perspective holistique, où les dimensions humaines et techniques de la cybersécurité sont intégrées, offrant ainsi une compréhension plus globale et réaliste des enjeux en jeu.

Pour illustrer la pratique de la cybersécurité et mieux comprendre son rôle et ses apports dans les établissements bancaires françaises et libanaises, nous avons opté pour des entretiens sur le terrain d'étude bancaire. Cette démarche nous a permis de produire des analyses lorsque nous étions confrontés à des données chaudes, en l'occurrence à une crise organisationnelle et un terrain évolutif qui se sont manifestés dans les banques autour des problématiques de cybersécurité.

Au regard de l'évolution continue et des défis qui font face à la cybersécurité, nous nous penchons vers une recherche-intervention ou recherche collaborative. A l'inverse d'autres démarches, la recherche-intervention se fonde sur une immersion dans l'organisation en vue de conduire une intervention, c'est-à-dire d'accompagner ou de susciter une transformation des organisations (Aggeri, 2016).

3.1.3 Une légitimité de la recherche et du chercheur à construire

Les interlocuteurs ayant un très haut niveau de connaissances en cybersécurité imposaient des exigences élevées et techniques quant au cadre et au déroulé de l'entretien. Pour répondre à ces attentes, il est rapidement devenu indispensable de développer et affiner nos compétences en la matière, en nous tenant informés des dernières actualités via des séminaires spécialisés, tels que les « Lundis de la cybersécurité », ou en consultant des ouvrages scientifiques de référence comme ceux de la Harvard Business Review. Ces efforts visaient à créer un climat de confiance

propice à des échanges ouverts avec les experts, qu'il s'agisse de RSSI ou de leaders en cybersécurité.

Au cours de nos entretiens, nous avons observé que l'évocation de termes techniques spécifiques (comme « Application Level Gateway Firewall », « Anomaly Detection Model », ou encore « Dark Web ») suscitait parfois des réactions de surprise de la part de nos interlocuteurs. Néanmoins, cela a souvent ouvert la voie à des explications plus personnalisées et détaillées de leur vision de la cybersécurité, non seulement pour leur propre organisation, mais aussi à l'échelle nationale, tant en France qu'au Liban. Notre objectif n'était pas de parvenir à une définition standardisée de la cybersécurité, mais plutôt de saisir comment ces experts se représentaient ce concept, dans un cadre à la fois organisationnel et culturel.

La construction de notre légitimité en tant que chercheurs dans ce domaine technique s'est révélée être un processus évolutif et déterminant pour le succès de notre démarche. Participer à des événements spécialisés, tels que des conférences sur la sécurité informatique ou des ateliers de sensibilisation, nous a permis de non seulement acquérir des connaissances techniques, mais aussi de nous familiariser avec les préoccupations et le langage des professionnels du secteur. Lors de nos interactions, une démarche itérative alliant écoute active et questionnements ciblés a progressivement renforcé la confiance des experts interrogés. Certains d'entre eux, initialement sceptiques, ont été convaincus par notre engagement à approfondir les concepts complexes qu'ils abordaient, et ce, à travers des retours réguliers et des échanges de plus en plus pointus.

Au fur et à mesure que la recherche progressait, cette légitimité s'est consolidée, facilitant l'accès à des données sensibles et encourageant des discussions plus riches et nuancées. En contextualisant les retours des experts dans une perspective intégrant à la fois les dimensions techniques et organisationnelles, nous avons pu recueillir des témoignages essentiels pour une analyse fine des dynamiques humaines au cœur de la cybersécurité bancaire. Finalement, c'est cette approche mêlant expertise technique, compréhension organisationnelle et ouverture presque « psychanalytique » dans nos entretiens biographiques qui a permis à la plupart de nos interviewés de s'exprimer aussi librement que possible.

Conclusion intermédiaire

Cette partie explore le contexte complexe et évolutif de la cybersécurité dans le secteur bancaire, en mettant en évidence les défis rencontrés et la méthodologie adoptée dans l'étude. Les secteurs bancaires libanais et français sont confrontés à des défis importants liés à la

cybersécurité, essentielle pour assurer la protection des systèmes et des données et maintenir la confiance du public. Une cybersécurité solide et résiliente aux crises est essentielle pour restaurer et maintenir cette confiance dans un environnement en constante évolution. L'accès aux données et à l'information différait considérablement dans les deux contextes étudiés. Au Liban, l'instabilité politique et économique pose des défis importants, rendant particulièrement complexe l'obtention de données fiables et d'informations pertinentes. En revanche, en France, bien que le cadre soit plus stable, des défis liés à la confidentialité et aux impacts de la crise sanitaire ont également été rencontrés. Ces contrastes soulignent l'importance d'adapter les méthodes de recherche aux spécificités locales pour obtenir des résultats significatifs.

La méthodologie employée privilégie l'analyse des matériaux « chauds » à travers des entretiens et des observations directes, permettant d'obtenir une vue plus complète et nuancée des pratiques de cybersécurité. Cette approche offre une compréhension approfondie des interactions humaines et des dynamiques organisationnelles, allant au-delà des perspectives purement technologiques.

La construction de la légitimité du chercheur dans ce domaine technique a été essentielle pour accéder à des données sensibles et obtenir des témoignages détaillés. Les efforts pour acquérir des connaissances spécialisées et participer à des événements du secteur ont renforcé la confiance des experts, facilitant des échanges enrichissants.

Nous avons établi un cadre solide pour analyser les dynamiques de cybersécurité dans les établissements bancaires, en tenant compte des défis contextuels et méthodologiques spécifiques à chaque environnement. Cette base permettra de poursuivre l'exploration des dimensions identitaires et organisationnelles en lien avec la cybersécurité bancaire.

3.2 Objet de la recherche : la construction identitaire abordée à partir de la méthodologie de Dubar et Demazière[5]

La méthode de Dubar et Demazière nous conduit à examiner le concept de dynamique identitaire pour mieux comprendre ce qui est en question dans les récits que les différents acteurs de la banque font de leur insertion dans un domaine de cybersécurité. Nous joignons ce terme à celui de trajectoire subjective c'est-à-dire la manière dont les auditeurs internes et les RSSI pensent de leur parcours en domaine cyber et comment ils prévoient assurer la cybersécurité dans la banques dans l'avenir.

3.2.1 Formes identitaires et identités : des distinctions élémentaires à la base de la méthodologie

Nous proposons ici de saisir les distinctions nécessaires pour cerner la notion d'identité à partir de la contribution de Dubar :

« Le premier obstacle épistémologique inhérent au concept d'identité demeure l'essentialisme. Parler d'identité, ethnique, nationale, sexuelle ou professionnelle, par rapport à un ensemble de phénomènes, c'est toujours risquer qu'il y ait des essences, des permanences constitutives, des personnes affectées ou des groupes désignés et qu'il suffit de les prononcer avec l'autorité de la science pour expliquer les faits. » (Dubar, 2015)

Durkheim avait à sa manière souligné le risque essentialiste :

« Lorsqu'il s'agit d'identité collective, le risque associé à l'utilisation non critique du terme identité est d'évoquer l'idée que la culture du groupe auquel on est étiqueté est une réalité en soi, une totalité autonome, un noyau culturel qui structure les personnalités des membres d'un groupe considéré comme une sorte de communauté. » (Durkheim, 1985)

Pour autant, l'identité ne peut être cernée de manière décontextualisée :

« Le concept d'identité véhicule souvent l'idée que la subjectivité est une entité qui peut être définie à partir de certains traits qui caractérisent un individu, quels que soient le contexte, la situation, les relations avec les autres... Ainsi, tout type de personne présente un risque d'étiquetage. Dès lors que l'on néglige le contexte, et surtout le contexte relationnel, on adopte une position épistémologique redoutable : celle qui suppose que le comportement que nous étudions n'est pas le produit de l'interaction du sujet et du contexte (situations, relations,

[5] Demazière, D. et Dubar, C., Analyser les entretiens biographiques. L'exemple de récits d'insertion. Paris : Nathan, 1999

institutions...), mais en exprimant le sujet lui-même, et donc aussi son identité. Prendre tout comportement d'une personne comme l'expression de cette supposée entité (une identité souvent qualifiée de personnelle) revient donc à risquer de réduire cette personne à une étiquette qu'on lui colle et qu'on légitime par toute sorte d'expertise... » (Dubar et Demazière, 1999).

L'invitation de Dubar et Demazière est donc d'aborder l'identité comme un fait à la fois individuel et collectif, contextualisé sans être déterminé :

« Cette position n'est pas la seule position sociologique possible. Nier toute pertinence sociologique aux manifestations individuelles (Durkheim, 1985) et ne considérer le social que comme extérieur aux individus et saisissable par des outils statistiques n'est pas la seule ni peut-être la meilleure façon d'aborder les faits sociaux. »

Veyne (1971) propose d'inscrire tout fait social dans son contexte spatio-temporel, défini globalement, c'est-à-dire dans les formes symboliques sous lesquelles il apparaît, et surtout ses formes langagières classificatoires. Durkheim et Simmel (1987) parlent de l'importance des formes symboliques dans la vie sociale et la démarche sociologique. Dans l'expression de la forme d'identité, la notion de forme est au moins aussi importante, sinon plus, que la notion d'identité. L'objectif n'est pas la personnalité des sujets concernés, mais la forme symbolique et surtout linguistique (langagière) à laquelle ils se réfèrent, argumentent et expliquent. Nous admettons comme Dubar et Demazière que l'identité est un processus de construction et de reconnaissance d'une définition de soi (Dubar, 2015) à la fois satisfaisante pour le sujet lui-même et validée par les institutions qui l'encadrent et l'ancrent socialement en les catégorisant. Cette définition est de moins en moins donnée par l'héritage familial ou même culturel et de plus en plus construite, vécue, reconstruite au cours du dialogue et de la confrontation avec les autres. Elle est le produit de la socialisation, mais aussi de la constitution de l'expérimentation sociale (Dubar, 2015) et de l'expérimentation progressive (Galland, 2011) à travers le passage dans les institutions, mais aussi dans les rencontres avec les autres. C'est pourquoi la mise en récit *(Storytelling)* est un mécanisme identitaire particulièrement intéressant à étudier.

3.2.2 Formes identitaires et double transaction : une théorisation

Les récits biographiques portent des traces de transactions qui font l'objet et l'enjeu de processus identitaires. Nous les appelons ainsi parce qu'ils se rapportent aux classements et aux affiliations, aux compétences et aux appartenances, aux préférences et aux évaluations, et impliquent des relations informelles avec les autres et avec soi-même (Strauss, 1989). Une transaction biographique est une transaction qui peut être identifiée par des traits narratifs.

Pour les RSSI, l'opposition entre « je suis responsable » (fortes connaissances informatiques, responsable de la sécurité informatique, conscience que la cybersécurité est un risque majeur...) et « je fais recours à des prestataires externes » (nous ne sommes pas experts en cybersécurité, nous n'avons pas les compétences requises, notre rôle est limité à la sensibilisation et la supervision…) met en mots la préférence pour une assurance par des prestataires externes de la cybersécurité contre le risque d'anticiper les cyberattaques et de mal gérer la cybersécurité (pour un manque de compétence), ce qui est dégradant pour l'image de soi. Cette transaction là est le fait de celles et ceux dont la forme identitaire (externaliser la cybersécurité) se construit dans une relation entre la formation universitaire (Diplômes et certifications) et le monde du travail (le milieu cyber). D'où leur double insistance, dans leur argumentaire, sur le fait qu'ils n'ont pas les compétences techniques spécialisés en cybersécurité, et qu'ils sont déçus de l'absence de lien entre leur formation et leur emploi, qu'ils n'ont pas été formés pour faire face aux cyberattaques, un domaine nouveau pour eux. En revanche, les oppositions entre le travail des informaticiens « je sais tout » fondé sur leurs expériences informatiques, leur compétence informatique de métier et assurer la cybersécurité exige des compétences techniques spécialisés, mettent en récit une autre forme identitaire (référence au monde des vrais métiers de cybersécurité) pour laquelle l'image de soi valorisante est celle de l'indépendance, de la mise à son compte et de la pratique en fondant une expérience cyber. Mais ces croyances subjectives issues des expériences biographiques (contexte fort informatique, expérience sur des systèmes informatiques et codage, respect de la sécurité informatique) ne suffisent pas à construire l'une ou l'autre des deux formes précédentes. Il faut la validation d'un tiers, une reconnaissance minimale des prétentions à être responsable de l'assurance-cybersécurité ou à l'externaliser. C'est l'objet d'une transaction relationnelle toujours incertaine, jamais achevée. Il peut s'agir de trouver une formation universitaire qui prépare au exigences et défis de la cybersécurité ou avoir un apprentissage spécifique en cybersécurité ou avoir une formation technique ou un accompagnement en cybersécurité durant les premières années d'emploi sont des conditions de validation des formes identitaires précédentes. Même s'il s'agit d'ambition voire de rêve en raison de contraintes budgétaires, cet autrui significatif (Mead, 1933) est l'instance qui rend possible une catégorisation crédible. C'est pourquoi la mise en évidence de cette transaction s'effectue à travers l'analyse des acteurs du récit et la confirmation de la pertinence des catégorisations précédentes résulte de l'homologie structurelle entre l'organisation des séquences narratives et la mise en scène de ses actants. Les RSSI et les responsables de sécurité s'identifient aux opérateurs informatiques technique en cybersécurité ou aux prestataires

externes spécialisés en cybersécurité qui sont les meilleurs représentants ou les prototypes dans leur environnement et dans leur organisation. Ainsi, les formes d'identité sont indissociables de l'identification à des types d'Autrui qui représentent des figures sociales (Weber, 1909) ou des rôles attractifs (Kaufman, 1994) ou des acteurs clés (Sainsaulieu, 1994).

Ces deux transactions s'articulent nécessairement comme une identité que l'on revendique pour soi à partir de son expérience biographique et une identité que vous reconnait Autrui à partir des critères et normes de gouvernance et de fonctionnement. Cependant, ils mettent en jeu des mécanismes différents pour rendre compte de la dualité des processus identitaires (Dubar C. , 2015). La double transaction s'exprime à travers le dialogue des interviewés (RSI, auditeurs...), dans les arguments échangés et la restitution du récit considéré comme parole (Barthes, 1967).

Les formes d'identité sont donc des concepts typologiques destinés à différencier les manières de parler du travail, de décrire sa vie professionnelle et d'envisager son avenir, et d'assurer la cybersécurité dans les banques. Cette façon de catégoriser les situations de travail, les positions dans l'espace de travail sont constitutives d'un monde socioprofessionnel. Pour notre recherche, nous avons supposé a priori la coexistence de plusieurs catégories qui se fondent sur de nouveaux types de parcours et de récits relatifs à l'assurance-cybersécurité. Ces catégories ou scénarios peuvent être liés à la vision individuelle d'un directeur d'entreprise ou d'un conseil d'administration ou d'un CEO pour gérer la cybersécurité. Or chaque banque (monde socioprofessionnel) articule une architecture de catégories et un système de préférences et de valorisation pour assurer la cybersécurité.

3.2.3 Analyses des dynamiques identitaires des RSSI et des auditeurs internes

Notre analyse des entretiens biographiques repose en partie sur des formes argumentaires par lesquelles les RSSI et les auditeurs internes s'efforcent de justifier leurs parcours métier, de légitimer leurs compétences et évoquent leur contribution possible à la cybersécurité dans le présent et l'avenir. Théorisés comme une double transaction avec eux-mêmes et avec Autrui significatifs de leur situation ou de leur parcours, ces argumentaires sont analysés comme des stratégies discursives lors des entretiens. Cette analyse peut servir d'analyse complémentaire à l'analyse structurale, car elle avance probablement la clarification des stratégies identitaires associées aux formes que nous avons identifiées.

Nous nous appuyons ainsi sur :

- L'énonciation et la subjectivité dans le langage ;
- La relation dialogique et les discours de référence ;

- Le contrat de communication et stratégie discursive.

L’analyse des dynamiques identitaires des RSSI et des auditeurs internes, basée sur les entretiens biographiques, met en évidence plusieurs impacts clés sur notre recherche :

- La clarification des stratégies identitaires : l'analyse des argumentaires permet de comprendre en profondeur les stratégies identitaires que les professionnels déploient pour se positionner dans leur rôle. Elle éclaire les motivations et les justifications qui sous-tendent les formes d'identité identifiées, enrichissant ainsi l’analyse structurale en offrant des insights sur la manière dont ces identités émergent et se manifestent dans les discours des RSSI et des auditeurs internes ;
- La légitimation des compétences : les argumentaires révèlent comment ces professionnels légitiment leurs compétences dans un domaine en constante évolution. Cette analyse permet de saisir les dynamiques de reconnaissance et de validation de leurs expertises, influençant ainsi leur perception de leur rôle et de leur contribution à la cybersécurité.
- L’impact sur la contribution à la cybersécurité : en examinant les perceptions des RSSI et des auditeurs internes concernant leur contribution à la cybersécurité, l'analyse permet d'identifier leurs aspirations et leurs visions pour l'avenir. Cela offre un aperçu sur comment ils intègrent les évolutions technologiques et les enjeux émergents dans leurs argumentaires identitaires.
- Stratégies discursives comme outil d’analyse complémentaire : l'analyse des stratégies discursives met en lumière les nuances des récits biographiques et les choix argumentatifs des professionnels. Cela permet de dégager des tendances et des patterns dans la construction des identités professionnelles, apportant une dimension contextuelle et subjective à l’étude des dynamiques identitaires.

Conclusion intermédiaire

Nous avons exploré la construction identitaire des acteurs dans le secteur bancaire de la cybersécurité en s'appuyant sur les méthodologies de Dubar et Demazière. Elle se concentre sur les dynamiques identitaires des Responsables de la Sécurité des Systèmes d'Information (RSSI) et des auditeurs internes à travers l'analyse de leurs récits biographiques.

La méthodologie utilisée repose sur les théories de Dubar, qui soulignent les limites de l'approche essentialiste de l'identité. Selon Dubar, l'identité ne doit pas être réduite à des caractéristiques fixes ou immuables, mais doit être vue comme un processus de construction et

de reconnaissance influencé par le contexte social et les interactions. Les contributions de Durkheim et Simmel, quant à elles, mettent en avant l'importance des formes symboliques dans la définition de l'identité, suggérant que les identités doivent être comprises comme des constructions sociales contextualisées.

Les perceptions des RSSI et des auditeurs internes influencent non seulement leur définition des rôles et des compétences, mais aussi leurs approches stratégiques en matière de sécurité. Les RSSI qui se perçoivent comme des experts techniques sont souvent plus susceptibles de promouvoir des stratégies internes robustes, tandis que ceux qui se positionnent comme superviseurs externalisant la cybersécurité peuvent privilégier des solutions de sécurité gérées par des prestataires externes. Cette distinction affecte la manière dont les stratégies de sécurité sont mises en œuvre et intégrées dans les pratiques organisationnelles. La légitimation des compétences joue également un rôle clé dans l'acceptation des mesures de cybersécurité, car les professionnels qui réussissent à affirmer leur expertise influencent davantage les décisions et les politiques de sécurité. Les dynamiques identitaires déterminent aussi comment les professionnels intègrent les évolutions technologiques et les défis émergents dans leurs stratégies, avec les experts techniques étant plus enclins à adopter des solutions innovantes. En outre, les stratégies discursives adoptées reflètent les perceptions identitaires et influencent les pratiques de sécurité, les discours valorisant l'expertise technique favorisant des approches plus intégrées et rigoureuses.

Cette étude enrichit la compréhension des dynamiques identitaires en offrant des perspectives sur la manière dont les RSSI et les auditeurs internes construisent et légitiment leur identité professionnelle. Elle montre également comment leurs stratégies discursives reflètent des tendances et des motivations individuelles et professionnelles, ajoutant ainsi une dimension contextuelle à l'analyse des identités dans le domaine de la cybersécurité bancaire.

3.3 Démarche de recherche empirique : interprétation et abduction

Dans le cadre de notre communication, nous explorerons la démarche méthodologique adoptée pour notre recherche, mettant en lumière notre posture interprétativiste et l'utilisation du raisonnement abductif. Nous détaillerons également comment ces approches ont guidé la collecte et l'analyse des données qualitatives, ainsi que les principales découvertes concernant les dynamiques de cybersécurité et les conflits juridictionnels entre les acteurs impliqués.

3.3.1 Une posture méthodologique interprétativiste

Au regard de notre recherche, nous faisons le choix d'un positionnement interprétativiste, inscrit dans une démarche abductive, fondée sur des données qualitatives tirées de cas singuliers et comparés.

3.3.1.1 L'interprétativisme

En cela qu'il s'intéresse en priorité aux acteurs de terrains et à leurs représentations, l'interprétativisme est pertinent au regard de notre sujet dans la mesure où la cybersécurité est un objet en voie de se faire et un sujet d'interprétation de la construction des identités professionnelles. Le travail de Dubar, dont nous nous inspirons fait de la narration le vecteur de l'identité dans un processus transactionnel.

Le paradigme interprétativiste cherche à trouver comment le chercheur établit le sens qu'il donne à la réalité. Selon les interprétivistes, la réalité est multiple et relative quant à la position de l'interprétivisme par rapport à l'épistémologie (Hudson, 1988). Contrairement aux chercheurs positivistes, les chercheurs interprétivistes adoptent des approches d'étude plus flexibles et ouvertes. Ils n'utilisent pas de cadres traditionnels et structurés. La connaissance devient indissociable des chercheurs et de leur actions (Carson, 2001). Donc, le but de la recherche interprétative est de savoir et d'interpréter les significations du comportement humain plutôt que de généraliser et de prédire les causes et les effets (Hudson, 1988) Pour les chercheurs interprétatifs, il est important de comprendre les modèles, les significations, les raisons et d'autres expériences subjectives en relation avec le temps et le contexte (Neuman, 2007). Les approches interprétatives accordent à la recherche l'opportunité et la liberté d'aborder les questions d'influence et d'impact et de poser des questions telles que « pourquoi » et « comment » des trajectoires spécifiques de technologie sont créées (Deetz, 1996).

Nous en retenons l'idée de *faire parler* les résultats en les mettant en lien avec des référents thématiques. Cette démarche nous permet de déborder le strict relevé thématique, de manière à exploiter toutes les menaces et les implications des résultats qui ne seraient pas apparents à

première vue sur le terrain bancaire de cybersécurité (Paillé, 2012).

3.3.1.2 Un mode de raisonnement abductif

L'approche abductive peut représenter une alternative aux deux approches déductives et inductives. Nous avons opté pour ce type de raisonnement abductif puisqu'il s'établit à travers des aller-retours successifs entre les observations empiriques et les lectures académiques. Les approches sur le terrain sont donc nourries par les réflexions théoriques et rencontrent les présupposés philosophiques et épistémologiques du chercheur (Savoie-Zajc, 2000).

Notre démarche de recherche doctorale peut être qualifiée de stratégie hybride (Fillol, 2007) car elle est établie à travers des allers-retours régulier entre la théorie et le terrain, ce qui correspond bien à un objet en voie se faire dans un environnement évolutif. La démarche abductive permet un aller-retour entre la théorie et le terrain ce qui nous a permis de préciser voire de réorienter certains éléments de notre cadre conceptuel et, au final, d'enrichir les résultats de la recherche.

L'adoption d'une démarche abductive favorise l'ajustement permanent de la recherche et le rapprochement systématique des éléments théoriques et empiriques. La recherche n'en est que plus cohérente, cela permettant d'intégrer des éléments non-prévus théoriquement, mais émergeant directement des terrains étudiés. Comme le mentionne Wacheux (1996), les aller-retour permanents entre théories et faits sont une source d'enrichissement. Cette démarche de va-et-vient entre la collecte des données et leur analyse, d'une part, et les composantes d'analyse elles-mêmes, d'autre part, apporte une contribution significative en termes de qualité et de profondeur des données collectées et de plausibilité des interprétations faites spécialement sur le terrain évolutif bancaire. Premièrement, les données manquantes peuvent être trouvées à temps pour préparer la prochaine collecte de données. Cette approche peut alors obtenir les détails nécessaires pour mieux comprendre les processus impliqués et valider les premières conclusions à partir des données pour assurer leur plausibilité (Deslauriers, 1991).

Enfin, selon nous, il s'agit également d'une démarche nécessaire pour assurer la saturation des données, faute de quoi la crédibilité de l'étude sera remise en question. C'est ainsi que nous avons abouti à une deuxième vague d'entretiens avec les leaders de cybersécurité pour saturer nos données par rapport à notre problématique et nos questions de recherche.

3.3.1.3 Une approche comparative

En ce qui concerne notre positionnement épistémologique, ainsi que pour la nature de notre démarche de recherche utilisée, nous avons choisi de conserver comme fil directeur la volonté

de ne pas nous enfermer dans un design de recherche strict afin de nous adapter plus librement aux contraintes et aléas de la recherche, et notamment à ceux du terrain bancaire et de la cybersécurité. Nous privilégions une épistémologie du quotidien au sens de Wacheux (1997) qui considère que la théorisation n'est pas uniquement une représentation abstraite. Elle se forme aussi d'un encodage des expériences des acteurs et de l'observateur. Wacheux (1997) explique que le chercheur doit réfléchir aux conditions de son intervention pour être légitime sur le terrain. Nous justifions cette intervention par l'étude de l'identité des différents acteurs de proximité (environnement social et identités professionnels) et de l'épistémologie du quotidien (enjeux et évolution constantes de la cybersécurité) qui renforcent cette réflexion.

3.3.2 Une approche qualitative

Notre étude porte sur une recherche qualitative car elle cherche à comprendre et analyser l'identité professionnelle des auditeurs internes et des responsables de sécurité informatique. Cette recherche qualitative permet d'analyser les informations par rapport à la problématique de recherche et les conflits de juridiction éventuels entre les deux professions en charge d'assurer la cybersécurité dans le secteur bancaire. Ces données qualitatives ont été collectées par trois voies complémentaires : observation, entretiens et documents.

Selon Blanchet (2007), les entretiens et les études exploratoires visent à mettre en lumière des aspects du phénomène auquel il se rapporte le chercheur ne peut pas penser spontanément et achever le travail qu'il propose sa lecture. L'entretien devient donc l'instrument privilégié de collecte des récits, notamment lorsqu'ils sont identitaires.

La conduite des entretiens a dû se faire en conscience de la nécessité d'amener les sujets à dépasser ou à oublier les mécanismes de défense qu'ils ont mis en place contre le regard extérieur sur leur comportement ou leurs pensées (Baumard, 2014).

Plus précisément, notre collecte de données est constituée de quarante entretiens biographiques et huit entretiens non directifs et de plusieurs heures d'observation flottante ainsi que de données secondaires enrichis par des rapports d'audit, des statistiques internes et des articles de presse. Notre phase de collecte de données se détaille à travers le tableau ci-dessous où nous avons réalisé un entretien par profession dans chaque organisation :

Tableau 6 : le récapitulatif des entretiens (synthèse, détails par vague infra)

Démarche	Contexte	Organisation	Professions
Phase 1			
Entretiens Biographiques	Banque Française	BPVF	Directeur de l'audit interne
			Directeur général
			Directeur de l'audit interne de l'I-BP
			Directeur de la conformité
			Superviseur de l'audit interne
			Chef de Mission audit interne
			RSSI
			Responsable informatique
	Banques Libanaises	Banque Audi, BLOM Banque, Byblos Banque, Fransabank, Société générale de banque au Liban (SGBL), Banque of Beirut, Bank Med, Banque Libano-Française (BLF)	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
Phase 2			
Entretiens Non directifs	France	ANSSI	Secrétaire général / Chef des Ressources Externes
		ARCSI	Président
		ARCI – AIRBUS - Thomson CGR	Expert sécurité de l'information / Lundi de la cybersécurité
		CLUSIF	Directeur
		KPMG	Associé / Responsable d'activité pour la cybersécurité
		DELOITTE	Associé / Expert en cybersécurité
		PWC	Associé / Responsable activité en cybersécurité France
		Ernest & Young	Directeur en charge d'activité de cybersécurité

Nous avons donc adopté la recherche qualitative pour décrire ce qui a été observé et parfois pour formuler ou créer de nouvelles hypothèses et approches. La recherche qualitative est utilisée lorsque vous en savez peu sur un sujet ou un phénomène et que vous souhaitez découvrir et en savoir plus. Elle est couramment appliquée pour comprendre les expériences des gens et

exprimer leurs opinions (Johnson, 2004).

Nous analysons grâce à une démarche qualitative les identités professionnelles des auditeurs internes et des responsables de sécurité informatique afin de comprendre les problèmes de juridiction qui émergent entre ces deux professions pour assurer la cybersécurité dans le terrain bancaire.

3.3.3 Chronologie de l'approche-terrain dans une démarche abductive

Le secteur bancaire a toujours été intrinsèquement porteur de risques informationnels au-delà des risques financiers. Les données bancaires sont qualifiées comme des données sensibles auxquelles il est nécessaire de porter une attention particulière. De fait, la cybersécurité dans les banques demeure une question de sécurité nationale (Kempf, 2012).

3.3.3.1 La première phase de terrain

Notre première phase de terrain regroupe quarante entretiens biographiques dont huit sont réalisés au sein de la BPVF et trente-deux sont réalisés au sein des banques libanaises.

La BPVF est une grande banque de détail, liée à l'I-BP, qui a pour enjeu de protéger l'épargne populaire. Nous avons réalisé en total huit entretiens relatifs aux postes de directrice générale, directeur d'audit, directeur d'audit de l'informatique Banque Populaire I-BP, superviseur d'audit interne, chef de mission d'audit interne, responsable informatique, responsable de la sécurité des systèmes d'information et directeur des risques et de conformité. Nous avons choisi ces interlocuteurs en raison de leur rôle direct ou indirect dans la structuration de l'audit interne et des SSI autour de la cybersécurité d'établissement bancaire.

Malgré la crise économique (crise monétaire et financière) et sanitaire (COVID-19) au Liban, nous avons réussi à réaliser nos entretiens dans les banques les plus réputées dans le secteur bancaire libanais. En total, nous avons effectué trente-deux entretiens biographiques dont quatre entretiens dans chaque banque. Ces entretiens étaient réalisés avec les responsables d'audit interne et les RSSI. Les banques concernées sont : Banque Audi, BLOM Banque, Byblos Banque, Fransabank, Société générale de banque au Liban (SGBL), Banque of Beirut, Bank Med, Banque Libano-Française (BLF). Nous rappelons que nous avons adopté le même guide d'entretien utilisé pour réaliser les entretiens biographiques à la BPVF. Pour compléter les données sur le terrain bancaire libanais, nous avons effectué une prise de notes d'observations effectuées sur plusieurs journées sur les différentes banques libanaises. La durée moyenne par établissement est équivalente à dix journées d'observations.

3.3.3.2 La cybersécurité bancaire en contexte pacifié versus en contexte de crise

Nous adoptons une optique principale. Elle vise à une comparaison internationale entre deux terrains opposés : un terrain pacifié et un terrain conflictuel. Le contexte pacifié est illustré par la BPVF alors que celui conflictuel regroupe les banques libanaises. Le secteur bancaire français est un contexte pacifié toujours en évolution qui a montré sa résistance face à la crise sanitaire et plusieurs crises économiques inédites. Ce secteur a conservé ses principales caractéristiques structurelles or la crise sanitaire n'a pas provoqué de récessions au-delà de la tendance observée à long terme. En effet, sa rentabilité a résisté en dépit d'une hausse significative du coût du risque. Plus généralement, ces dernières années ont été marquée par une croissance des activités de marché (ACPR, 2020).

A l'inverse, le terrain libanais est en crise conflictuelle. Il a mal réagi face à la crise sanitaire, l'explosion du port, et la crise économique de 2020. L'effondrement du secteur bancaire libanais au moment où la crise économique s'aggravait. Selon la banque de France, le Liban fait face à l'une des trois pires crises à l'échelle mondiale depuis 150 ans (Belhache, 2022). La cybersécurité, dans ce contexte, est devenue un sujet « moins urgent », et la mise en place de dispositifs nouveaux pour l'assurer ont été suspendus pendant la période.

3.3.3.3 La nécessité de sortir de la banque

En interrogeant les différents acteurs dans les banques françaises et libanaises, aucune partie n'a reconnu la nécessité d'une nouvelle organisation ou l'émergence d'une nouvelle fonction pour assurer la cybersécurité dans le secteur bancaire. Or nos observations et les entretiens laissaient entendre des lacunes majeures, notamment en termes de savoir-faire, de disponibilité et de processus dans l'administration de la cybersécurité des établissements quels qu'ils soient. Aucune partie n'a assumé ce que pourrait être sa responsabilité en cas de cyberattaques. Tous les acteurs ont reconnu l'importance de la sensibilisation à la cybersécurité et de la coopération entre les départements et les responsables de services. Le seul dispositif envisagé en cas d'attaque est la constitution d'une cellule de crise au périmètre parfois indéfini. A l'occasion de nos analyses et nos observations du terrain, nous nous sommes concentré sur le conflit juridictionnel qui existe entre les responsables de sécurité informatique et les auditeurs internes au lieu de chercher à savoir la raison à laquelle ce conflit s'est mis en place. Nous nous sommes rendu compte que les RSSI profitent du manque d'expertise, de compétence et de la situation de faiblesse de l'auditeur interne dans un milieu technique spécialisé comme celui de la cybersécurité. Les RSSI s'appuient sur leurs expertises techniques et négligent l'importance que peut apporter l'audit interne pour faire face aux cyberattaques. Alors que lorsqu'il s'agit

d'avoir recours à des cabinets externes spécialisés, ils coopèrent en avançant ne pas avoir les compétences techniques nécessaires pour faire face aux cyberattaques. Le choix de confier la juridiction de la cybersécurité à des experts externes nous a interrogé. L'argument des compétences locales limitées se comprend probablement au regard des constructions identitaires, il peut s'expliquer par la recherche d'une certaine facilité, mais il nous semble ne pas devoir se justifier au regard des enjeux. Nous avons donc jugé nécessaire de sortir de la banque pour avoir une approche radicalement différente sur la cybersécurité et examiner comment le problème juridictionnel entre les RSSI et les auditeurs internes peut être abordé, sinon résolu. Nous avons engagé cette démarche à travers des entretiens supplémentaires pour enrichir nos résultats avec des régulateurs, des observateurs et des auditeurs internes qui sont qualifiés par rapport à leur contexte et leur expérience comme les leaders en cybersécurité.

3.3.3.4 La deuxième phase de terrain hors banques : entretiens non directifs

Nos analyses et nos observations du terrain bancaire libanais et français attestent d'un conflit juridictionnel entre les responsables de sécurité informatique et les auditeurs internes. Nous avons relevé le manque d'expertise, de compétence des auditeurs internes dans un milieu technique spécialisé celui de la cybersécurité. Les RSSI se servent de leur expertise technique pour étendre leur juridiction et négligent l'importance que peut apporter l'audit interne pour faire face aux cyberattaques. Ils ont recours à des cabinets externes spécialisés au prétexte de ne pas avoir les compétences techniques nécessaires pour faire face aux cyberattaques. La contrainte de juridiction fondée sur le manque de compétences s'observe chez les RSSI de même que chez les auditeurs internes. Les huit entretiens réalisés dans la seconde phase auprès d'experts nous ont permis d'accéder à une approche radicalement différente de la cybersécurité et d'envisager des réponses au problème juridictionnel entre les RSSI et les auditeurs internes dans un milieu de cybersécurité. Nous avons réalisé ces entretiens supplémentaires à travers une discussion libre avec une orientation sur la question des juridictions *(Comment vous interagissez avec le RSSI ? Comment percevez-vous le RSSI ? Comment envisager vous l'évolution du RSSI ? Que pensez-vous du positionnement du RSSI dans son travail dans l'organisation ?), sur la question qui touchent la vision d'ensemble de la cybersécurité (Les banques sont-elles un cas particulier en cybersécurité ? Les banques doivent-elle faire l'objet de mesures spécifiques ?) et sur la question d'assurance de la cybersécurité (Nos entretiens sur la BPVF envisagent que la banque fait recours à des cabinets externes spécialisés en cybersécurité. Que pensez-vous de cette intervention d'autre expert pour maintenir la cybersécurité dans une banque. Existe-t-il un risque puisque les données sont sensibles ?)*

Conclusion intermédiaire

La démarche de recherche adoptée repose sur une approche interprétativiste et abductive, visant à explorer les dynamiques de construction identitaire des acteurs impliqués dans la cybersécurité bancaire, tant en France qu'au Liban. En privilégiant une posture méthodologique interprétativiste, nous nous efforçons de comprendre les significations et les représentations des acteurs de terrain. Cette approche s'avère particulièrement adaptée au contexte de la cybersécurité, un domaine en constante évolution et en construction, où les identités professionnelles sont façonnées par des interactions complexes et des processus transactionnels.

L'utilisation d'un raisonnement abductif, caractérisé par un aller-retour constant entre les observations empiriques et les théories académiques, permet d'affiner et de réorienter notre cadre conceptuel en fonction des données recueillies. Cette démarche hybride favorise une meilleure compréhension des phénomènes observés et enrichit les résultats de la recherche en intégrant des éléments théoriques non anticipés initialement.

La recherche qualitative menée à travers des entretiens biographiques, des observations et des analyses de documents révèle des conflits juridictionnels entre les RSSI et les auditeurs internes, ainsi que des lacunes dans les compétences et les processus relatifs à la cybersécurité. Les entretiens avec des experts externes, réalisés lors de la seconde phase de la recherche, apportent une perspective complémentaire sur ces problématiques et suggèrent des pistes pour résoudre les tensions entre les RSSI et les auditeurs internes. L'analyse comparative entre les banques françaises et libanaises met en lumière des divergences significatives liées aux contextes pacifiés et conflictuels. En France, malgré des crises économiques et sanitaires, le secteur bancaire maintient une certaine stabilité, alors qu'au Liban, la crise économique et sanitaire a exacerbé les défis en matière de cybersécurité. Cette situation souligne la nécessité d'une approche plus intégrée et stratégique pour la gestion de la cybersécurité, prenant en compte à la fois les spécificités locales et les exigences globales.

Notre recherche démontre l'importance d'une compréhension approfondie des identités professionnelles et des dynamiques de pouvoir dans le domaine de la cybersécurité bancaire. Elle souligne également la nécessité de développer des solutions adaptées aux contextes spécifiques et de renforcer la collaboration entre les différents acteurs impliqués.

3.4 Méthode de collecte des données : récits biographiques et données secondaires dans un contexte spécifique

Notre collecte des données a été effectuée entre avril 2019 et novembre 2022. Elle s'est opérée suivant trois vagues, chacune comportant un ajustement du guide d'entretien et des répondants ciblés.

3.4.1 Le processus de collectes des données

La première vague, la plus exploratoire, s'est déroulée entre février 2019 et mars 2020 en observation de l'organisation et de l'activité journalière des banques libanaises. Cette première vague a permis de fonder le guide d'entretien. Elle a notamment permis de cibler les principaux interlocuteurs associés à la contrainte de la cybersécurité et de l'audit interne dans le secteur bancaire. La seconde vague s'est déroulée entre mars 2020 et avril 2021. Cette vague a constitué le substrat de nos données avec quarante entretiens biographiques, huit entretiens menés sur le terrain bancaire français à travers la banque populaire val de France BPVF et trente-deux entretiens menés sur le terrain bancaire libanais à travers les huit banques les plus réputés sur le terrain bancaire libanais. Enfin, la troisième vague a eu pour but de vérifier si le point de saturation avait été atteint en complétant les données avec huit entretiens de discussion libre avec les leaders de la cybersécurité soit dans les cabinets d'audit internationaux Big Four, soit les agences nationales de sécurité des systèmes informatiques en France et entre mai et novembre 2022. Elle a également permis de constater les relatives carences des pratiques bancaires observées sur le période de recherche.

Nous avons enrichi cette dernière vague avec des données secondaires tels des rapports d'audit fournis, des documents internes et des statistiques pour conforter les résultats obtenus.

Tableau 7 : liste détaillé des entretiens de la première phase

Démarche	Contexte	Organisation	Professions
Phase 1			
Entretiens Biographiques	Banque Française	BPVF	Directeur de l'audit interne
			Directeur général
			Directeur de l'audit interne de l'I-BP
			Directeur de la conformité
			Superviseur de l'audit interne
			Chef de Mission audit interne
			RSSI
			Responsable informatique
Entretiens Biographiques	Banques Libanaises	Banque Audi	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		BLOM Banque	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		Byblos Banque	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		Fransabank	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		SGBL	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		Banque of Beirut	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		Bank Med	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne
		Banque Libano-Française	Auditeurs internes
			RSSI
			Responsable informatique
			Directeur de l'audit interne

Ces entretiens étaient orientés vers la question du rôle de l'audit interne et de la gestion de la cybersécurité dans ce milieu évolutif et risqué. Il ne nous est pas possible de détailler davantage les caractéristiques des banques du fait du caractère très sensible des informations communiquées pendant les entretiens. Chaque entretien a été réalisé avec les répondants clé de l'organisation (par exemple, le Directeur d'audit, le RSSI ou le président de l'association). Tous ont pu aborder la question de la cybersécurité, du rôle de l'audit interne et du fonctionnement de leur organisation. Pour le terrain français, nous avons contacté nos répondants par courrier électronique à travers notre intermédiaire de confiance Mr François M. Les entretiens en totalité étaient réalisés en Visio à cause des contraintes de sécurité de l'information et de sécurité sanitaire (COVID-19) à partir de mars 2020. Une visite des lieux de travail nous a néanmoins permis d'obtenir des informations supplémentaires sur leur organisation et leur environnement technique. Notre prise de contact avec les répondants ainsi que les relance a été rendu difficile pour plusieurs raisons. Premièrement, aborder le sujet de la cybersécurité est un sujet très sensible pour toute organisation, ce qui limitait considérablement le gain de confiance. Deuxièmement, en plus d'être des entretiens longs, le sujet de la recherche était rarement rattaché au cœur d'activité de ces organisations, dont le temps disponible est déjà très limité. Nous nous sommes concentré sur le lien entre l'audit interne et l'assurance de la cybersécurité dans les banques. Nous avons essayé de comprendre les conflits et les contraintes de juridiction au niveau de la gestion de la cybersécurité. Les entretiens ont duré en moyenne 83 minutes (entre 48 et 156 minutes). Nos entretiens réalisés sur le sujet de l'audit interne et de la cybersécurité ont duré en moyenne 76 min (entre 66 min et 88min).

3.4.2 Le processus d'analyse des données

Nous avons alterné analyse et entretiens entre avril 2019 et novembre 2022. Ce qui nous a permis d'éprouver progressivement certains thèmes émergents de nos analyses par études de cas. Notre analyse s'est divisé en deux parties : une analyse thématique réalisé par un codage spécifique après avoir conduit tous nos entretiens et une analyse par étude de cas. Nous détaillerons notre démarche d'analyse dans la partie Codage qui suit.

3.4.3 Des objectifs poursuivis différenciés

Dans les banques, notre objectif était d'éliciter les identités professionnelles des acteurs, spécialement des auditeurs internes et des responsables de la sécurité des systèmes d'information. Hors banque, c'est-à-dire celui des dirigeants d'associations nationales et ceux des cabinets d'audits internationaux qui sont des acteurs majeurs de la cybersécurité en France,

l'objectif était d'appréhender l'évolution des juridictions de ces professions entre les préconisations de ces institutions et les pratiques bancaires mise en place par rapport à la cybersécurité. Dans les deux terrains, des éléments de contextualisation ont été systématiquement recueillis.

Nous n'avons pas souhaité limiter l'analyse contextualisée des pratiques de socialisation organisationnelle à une analyse contingente, c'est-à-dire à une analyse des relations entre les contextes et les contenus des pratiques, ignorant le jeu des acteurs. Nous nous concentrons sur les interrelations entre le contexte et les pratiques de socialisation organisationnelle tout en considérant la perspective politique, c'est-à-dire l'interrelation du jeu des acteurs sur l'une et l'autre de ces dimensions. Ainsi, le cadre théorique du contextualisme est apparu comme le cadre plus pertinent pour expliquer les problèmes de territorialité et de juridiction entre les auditeurs internes et les RSSI.

3.4.4 Les entretiens

L'utilisation des données d'entretien a été faite à partir des transcriptions que nous avons nous-mêmes effectuées. Nous apportons cette précision car en fait la transcription fait aussi partie du travail d'analyse. En cohérence avec notre cadre théorique et notre cadre d'analyse, nous avons exécuté en total quarante-huit entretiens sur le terrain bancaire libanais, français et avec les leaders de la cybersécurité sur deux phases.

La première phase a été réalisée à travers un journal d'entretien qui regroupe les transcriptions des entretiens à travers guide d'entretien spécifique et une prise de notes d'observation sur le terrain. Nous avons appliqué ce guide d'entretien pour faire des entretiens biographiques sur la BPVF et les huit banques libanaises. Ce guide d'entretien permet d'identifier les identités professionnelles des auditeurs internes et des responsables de sécurité informatique afin de comprendre plus le problème de juridiction qui persiste entre ces deux fonctions pour assurer la cybersécurité. Nous présenterons dans la section « codage », la méthodologie utilisée qui est celle de Dubar. Nous l'avons adoptée puisqu'elle consiste à analyser les entretiens biographiques et à faire ressortir les identités des professions en question afin de comprendre le problème de territorialité et de juridiction qu'existe en cybersécurité.

La deuxième phase s'est avérée nécessaire pour atteindre un degré de saturation des données. Nous l'avons donc complétée avec des entretiens non directifs et des discussions libres avec une orientation précise vers la question des juridictions à travers huit entretiens avec les leaders de la cybersécurité.

3.4.4.1 Le déroulement des entretiens

Dans le cadre de notre démarche exploratoire d'approfondissement de notre objet de recherche, nous avons adopté la méthode de l'entretien biographique en premier.

Nous nous sommes donc appuyés sur le guide d'entretien (voir annexe) tout en conservant une certaine souplesse par rapport au guide (ajout de questions, reformulation et adaptation, ajustement de l'ordre des questions)

En effet, comme le précise Alami et al. (2009, p. 86), *« le guide d'entretien reste un canevas souple : il évolue au fur et à mesure des entretiens, en fonction de la pertinence effective des questions et de l'apparition de nouvelles pratiques à découvrir. Le guide d'entretien propose une dynamique, une progression dans les thématiques à aborder, mais l'ordre des questions n'est pas immuable : le chercheur s'adapte à la logique de l'entretien en suivant l'itinéraire des pratiques évoquées ».*

Nous avons abordé la thématique des identités professionnelles des auditeurs internes et des responsables de sécurité informatique au sein des banques.

C'est à travers les identités professionnelles que nous pouvons étudier les relations de l'auditeur interne avec les responsables de sécurité informatique dans la banque pour assurer la cyber sécurité.

L'objectif était de répondre de manière indirecte et détaillée aux questions suivantes : *quel est le degré d'interaction que vous avez avec les réseaux métier en termes de SSI ? Que penser vous lors que vous entendez le terme cybersécurité ? Qui est responsable de maintenir la cyber sécurité dans la banque ? Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ? Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Qu'en pensez-vous ? Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?*

Ces questions ont été adaptées selon la catégorie d'acteurs de notre cadre d'analyse à laquelle la personne interviewée pouvait être rattachée.

Les personnes interrogées ont été sensibles à la confidentialité de leurs notes, ce qui montre que le sujet reste entièrement secret et sensible. Malgré la confidentialité, lors de nos entretiens, nous avons parfois ressenti une réticence à poser des certaines questions, les interviewés préférant rester discrets et précisant qu'il s'agissait d'informations confidentielles pouvant nuire à la cybersécurité et qu'ils ne leur appartenaient pas de le commenter.

3.4.4.2 Les entretiens biographiques

L'entretien de recherche biographique suppose avant tout que l'acteur raconte quelque chose de sa vie ou de certaines dimensions de sa biographie (vie professionnelle, familiale, affective, etc.) dans une interaction ouverte, approfondie, complexe. C'est une combinaison du travail sur soi de la part de l'acteur et de l'écoute inactive de la part du chercheur. En effet, cette forme de conversation vise à favoriser le Storytelling, c'est-à-dire la cohérence d'épisodes biographiques, l'expression d'un récit impliquant une argumentation sur le sens (à la fois direction et sens) donné par son parcours. La narration est donc à la fois introspection et dialogue avec les autres et avec le chercheur. En ce sens, la situation d'entretien représente une forme particulière d'intrusion qui provoque l'attribution d'un rôle et d'une identité du répondant à l'intervieweur, suscitant même parfois une résistance, un discours évasif ou distanciant. Aussi, le chercheur doit manifester sa participation intellectuelle et affective, non seulement par divers signes d'encouragement, d'intérêt, de reconnaissance, mais aussi par ses interventions, son étonnement, ses commentaires : la présence du narrateur, mais aussi ses attitudes, ses comportements, ses interrogations, sont décisif, car en essayant de comprendre, il stimule la production de sens, pousse à développer des arguments, demande des enchaînements, des rapprochements, des explications de formules qui lui paraissent peu claires (Dubar, 1997).

Pour mieux comprendre ce qui est en question dans les récits des divers acteurs, ce codage nous permet d'examiner le concept de dynamique identitaire et celui de trajectoire subjective, c'est-à-dire la façon dont les différents acteurs disent et pensent de leur parcours d'insertion en banque, de l'assurance de la cybersécurité dans le domaine bancaire et des projections cyber dans l'avenir. Ces entretiens biographiques requièrent une certaine proximité relationnelle avec les enquêtés, voire une certaine indulgence si nous recherchons vraiment une communication non violente. La divulgation d'informations personnelles et confidentielles n'est pas courante, mais certains sont prêts à le faire lorsqu'ils sont assurés de garanties minimales et qu'une relation de confiance mutuelle est établie sur la base de ce que nous appelons une entente de confidentialité. Nous avons conduit tous nos entretiens dans les banques en respectant le code de confidentialité des données et des échanges que nous avons menés.

3.4.4.3 Le repérage de Verbatims signifiants

Au cours de nos transcriptions d'entretiens biographiques, nous avons procédé à l'identification préalable de verbatim jugés signifiants. Il peut s'agir de mots, de groupes de mots, de phrases entières ou même de paragraphes et de actions réalisées. Ici aussi, cette démarche a un caractère fortement inductif et, bien sûr, subjectif. Nous avons reproduit à l'annexe pour un extrait de

l'entrevue et relie l'utilisation de verbatim dans le rapport de recherche.

3.4.5 Les données secondaires

Nous avons renforcé notre analyse par des données secondaires pour saturer nos résultats et valider nos résultats de recherche. Ces données secondaires se sont reparties entre des articles de presse, spécialisées ou généralistes traitant de la cybersécurité dans un numéro spéciale (*Harvard business Review, Le Lundi de la cybersécurité, L'usine digitale…*) des documents internes fournis par les différents interlocuteurs (*Enquête KPMG sur le défi du risque cyber à travers des vues croisées d'auditeurs internes et responsables cybersécurité*), rapports d'audit (*Un rapport d'audit interne fournis lors d'une mission d'audit interne sur le département informatique en 2020 dans la BPVF*) et des statistiques internes fournis.

Conclusion intermédiaire

La collecte des données s'est déroulée entre avril 2019 et novembre 2022, se structurant en trois vagues distinctes. La première vague, exploratoire, s'est concentrée sur l'observation des banques libanaises pour affiner le guide d'entretien et identifier les principaux interlocuteurs en matière de cybersécurité et d'audit interne. La seconde vague, couvrant mars 2020 à avril 2021, a impliqué des entretiens biographiques dans des banques françaises et libanaises, ainsi que des entretiens de terrain pour approfondir les données collectées. La troisième vague, entre mai et novembre 2022, visait à vérifier la saturation des données par des discussions libres avec des leaders de la cybersécurité, enrichie par des données secondaires comme des rapports d'audit et des statistiques.

Les entretiens ont été réalisés avec des acteurs clés des banques (auditeurs internes, responsables de la sécurité des systèmes d'information) et des leaders de la cybersécurité en France. Les données ont été recueillies via un guide d'entretien évolutif et transcrites par les chercheurs eux-mêmes, permettant une analyse approfondie des identités professionnelles et des interactions entre les auditeurs internes et les RSSI. L'analyse des données a alterné entre codage thématique et études de cas, avec une attention particulière portée aux dynamiques identitaires et aux enjeux de territorialité et de juridiction en cybersécurité. La démarche a inclus une analyse des verbatim significatifs et une approche contextuelle intégrant les perspectives politiques des acteurs impliqués.

3.5 Codage des récits et des données

Afin de comprendre le rôle de l'audit interne dans la cybersécurité des établissements bancaires à travers une étude détaillée des identités professionnelles et des problèmes de juridiction des professions en question, nous avons procédé à un codage spécifique des données collectées. Nous listons tour à tour les méthodes de codage utilisées pour chacune des données enregistrées.

L'une des difficultés classiques des recherches dites qualitatives en sciences sociales est le caractère souvent très intuitif et rapide des opérations sur lesquelles elles s'appuient. L'intérêt de ce qui peut être extrait d'un corpus d'entretiens ou d'un travail ethnographique est incontestable. *Mais comment a-t-on réussi à extraire ? Quelles sont les éléments qui forgent les identités différentes des divers acteurs ?*

Pour répondre à ces questions de démarches méthodologiques en cohérence avec notre cadre théorique et notre cadre d'analyse, nous avons procédé à une analyse spécifique des entretiens biographiques réalisés sur le terrain bancaire français et libanais par un codage selon Dubar et Demazière.

3.5.1 L'intérêt du codage conçu par Dubar et Demazière

L'ouvrage *« Analyser les entretiens biographiques : l'exemple de récits d'insertion »* de Dubar et Demazière propose une méthode de codage pour analyser les entretiens biographiques. Cette méthode de codage nous semble utile pour étudier le rôle de l'audit interne et des RSSI dans la cybersécurité bancaire.

Nous justifions le recours au codage conçu par la méthode de Dubar et Demazière parce qu'il offre approche systématique et structurée pour analyser les données issues des entretiens biographiques. Il permet d'identifier des thèmes récurrents, des motifs, des relations causales et des significations dans les récits recueillis lors de nos entretiens. En utilisant cette méthode de codage, nous pouvons extraire des informations pertinentes concernant les identités professionnelles des auditeurs internes et des RSSI, ainsi que les enjeux liés à la gestion de la cybersécurité dans le contexte bancaire français et libanais.

L'intérêt du codage réside dans sa capacité à fournir une structure analytique pour interpréter les données qualitatives et à faciliter la comparaison et la synthèse des informations recueillies. Il permet également de repérer les similitudes et les différences entre les récits des auditeurs internes et des RSSI, ce qui peut nous aider à comprendre les dynamiques de pouvoir, les tensions et les conflits qui peuvent exister entre ces deux acteurs dans le contexte de la cybersécurité bancaire.

En résumé, en utilisant le codage conçu par Dubar et Demazière, nous pouvons analyser de manière approfondie les entretiens biographiques pour comprendre les identités professionnelles des auditeurs internes et des RSSI, ainsi que les défis spécifiques liés à la gestion de la cybersécurité dans le domaine bancaire.

3.5.2 La conception du codage selon Dubar et Demazière

Nous avons adopté le codage des entretiens biographiques à travers la méthodologie de Dubar et Demazière qui travaillent sur un corpus d'entretiens réalisés en 1994-1995 auprès de jeunes ayant quitté l'école huit ans auparavant sans diplôme d'études secondaires. Les jeunes ont été invités à dire quel a été leur parcours d'intégration depuis leur sortie de l'école. Les entretiens ont été menés dans le but d'éviter au maximum la forme d'un questionnaire (une enquête de ce type était auparavant réalisée par téléphone auprès de la même population). Il s'agissait ici d'amener les jeunes à se raconter, à s'approprier leur histoire, à parler de leurs expériences et trajectoires dans le monde du travail telles qu'ils les imaginaient, à transmettre ce qui leur tenait à cœur, ce qu'ils vivaient actuellement, ce qu'ils envisagent pour l'avenir. Ce sont ces entretiens, délibérément conçus pour saisir les trajectoires d'encastrement dans leur dimension la plus subjective, qui font la matière de la méthodologie de Dubar et Demazière.

Nous synthétisons donc l’approche proposée par Dubar et Demazière par trois caractéristiques fondamentales :

- Tout d'abord, il est impossible de considérer la conversation comme une simple source d'information sur le monde extérieur. Les conversations étant des faits linguistiques, elles doivent être considérées comme telles, c'est-à-dire en termes sociaux. La question vraiment pertinente à leur poser est donc de savoir ce qu'ils peuvent nous apprendre sur un certain type d'univers de sens et sa logique interne de constitution. Dans le cas de l’assurance de la cybersécurité, notre tâche comme analyste était de reconstituer les catégories de pensée, les jugements de valeur à travers lesquels les auditeurs internes et les responsables de sécurité informatique perçoivent leur trajectoire passée et leur situation actuelle et de définir ce qui serait du bon travail, un vrai travail pour eux pour assurer la cybersécurité.
- Les catégories apprises permettant l'interprétation des entretiens ne seront pas supposées, mais progressivement créées à travers un long processus d'analyse, de comparaison et de typologie, qui doit être exposé au lecteur. Se basant sur Dubar et Demazière, sous le signe de la théorie ancrée de Glaser et Strauss, nous concevons notre

interprétation comme une activité de *théorisation progressive* à partir de matériaux empiriques. Mais comment nous opérerons cette induction dans cette phase spécifique du processus abductif ?

Comment identifions-nous les catégories d'analyse à partir des données d'entretien ? En nous appuyant sur Dubar et Demazière, nous validons le choix de se reposer sur les orientations de la sémantique structurale comme ils les ont développés aussi Barthes et Greimas (1967), surtout dans les années 1960 et 1970. De même, nous avons clairement voulu réactiver cet héritage que les sciences sociales avaient en grande partie laissé en sommeil depuis vingt ans, ce qui apparaît clairement dans deux aspects de notre démarche. D'une part, une forte demande de formalisation dans le travail interprétatif ; d'autre part, une attention privilégiée aux disjonctions, oppositions, relations différentielles et constructives dans le discours des sujets, fondée sur ce postulat commun des méthodes structurales, selon lequel il y a un des mécanismes privilégiés de fonctionnement, et donc la découverte de sens.

3.5.3 La démarche de codage

Nous avons procédé au codage de tous les entretiens biographiques réalisés. Les entretiens font l'objet d'une retranscription complète, suivie d'une présentation complète de l'analyse qui a été effectuée et des résultats qu'elle a produits. Chaque entretien est d'abord codé systématiquement selon trois niveaux d'analyse : séquences, actants et arguments. Les rapports collectés pour chacun sont collectés et regroupés par grands types. Un schéma provisoire de la conversation est créé, représentant les principales classes d'énoncés qu'elle comprend à différents niveaux d'analyse. Ensuite, un point de vue structurel peut être utilisé, qui consiste à trouver les principales dichotomies et conjonctions apparaissant à chaque niveau, les homologies formelles entre différents niveaux, puis à identifier les régularités structurelles qui organisent l'ensemble de l'entretien et créent en quelque sorte son code narratif implicite. La formalisation des opérations n'est pas une fin en soi, mais elle est clairement mise au service d'intérêts sémantiques et sociologiques. Notre objectif selon la méthodologie de Dubar et Demazière est de comprendre ce qu'ils appellent *« l'ordre catégorique »* et *« l'univers des croyances »* à travers lesquels les auditeurs internes et les responsables de sécurité informatique perçoivent leurs expériences et projettent leur avenir pour tout ce qui touche au travail dans le domaine de la cybersécurité. L'analyse structurale, menée jusqu'au bout, aboutit finalement à la construction d'un schéma spécifique pour un entretien donné, qui dans sa logique interne représente un certain point de vue, une perspective à la fois globale et spécifique sur l'expérience

socioprofessionnelle. Un travail comparatif sur l'ensemble de ces schèmes spécifiques nous conduit ensuite à tenter d'élaborer une typologie des principales classes d'univers symboliques mis en évidence. Ce qui nous amène à réaliser :

- Une comparaisons inter cas par contexte d'organisation ou établissement. Nous décrivons les organisations des services, la politique de gestion des risques, la culture de risque… (Comparer le terrain bancaire libanais au terrain bancaire français)
- Une comparaison de contexte à double niveau : dans chaque banque c'est-à-dire les éléments qui forgent les identités des différents acteurs et pour toutes les banques.

3.5.4 Les questions d'analyse et de collecte

Dans le cadre de notre méthodologie, inspirée par les travaux de Dubar et Demazière (1999) sur l'analyse des entretiens biographiques, nous avons adopté une approche rigoureuse et nuancée pour la collecte et l'analyse des données. Notre guide d'entretien, conçu pour intégrer de manière continue les dimensions de collecte et d'analyse, s'appuie principalement sur la technique de l'entretien narratif non directif. Cette méthode est essentielle car elle accorde au locuteur une liberté d'expression qui nous permet de structurer et d'ordonner ses pensées. Ainsi, le processus de mise en mots et de séquençage dirigé par le répondant joue un rôle central dans la construction et la révélation du sens. Nous ne négligeons pas l'importance de revenir sur ces récits à plusieurs reprises au cours de notre analyse, sans pour autant en faire systématiquement l'objet de nos notes initiales. La non-directivité, qui se traduit par une écoute non intrusive et par un contrat de confiance implicite entre nous même en tant qu'enquêteur et le répondant, constitue un pilier fondamental de notre démarche. Cette approche repose sur la notion de construction dialogique du sens, une interaction basée sur la confiance, où nous, bien que placé en position d'extériorité par rapport aux auditeurs internes et aux responsables de la sécurité informatique, facilitons l'expression authentique des vécus et des perceptions.

Par ailleurs, notre méthodologie inclut deux postures complémentaires : d'une part, une attitude inquisitoriale, parfois provocante, qui vise à perturber et à challenger les discours pour en extraire des éléments révélateurs ; d'autre part, une approche psychanalytique qui nous positionne en tant qu'investigateurs psychologiques. Cette dernière nous permet d'explorer les significations inconscientes des comportements, relations et conduites des acteurs impliqués, en particulier les auditeurs internes et les responsables de la sécurité informatique, dans le contexte de la cybersécurité. Cette double posture enrichit notre compréhension des dynamiques sous-jacentes à leur discours et à leurs pratiques (Dubar et Demazière, 1999).

Conclusion intermédiaire

La phase de codage des données est essentielle pour comprendre le rôle de l'audit interne dans la cybersécurité bancaire, en explorant les identités professionnelles et les questions de juridiction. En utilisant la méthodologie de codage proposée par Dubar et Demazière, nous avons pu structurer l'analyse des entretiens biographiques et mettre en lumière les thèmes récurrents, les relations causales et les significations dans les récits des auditeurs internes et des responsables de la sécurité des systèmes d'information.

Cette approche nous permet d'avoir une analyse approfondie des données qualitatives, facilitant la comparaison entre les récits et l'identification des dynamiques de pouvoir et des conflits entre les différents acteurs dans le domaine de la cybersécurité. Le codage a été effectué à travers trois niveaux d'analyse—séquences, actants et arguments—afin de repérer les régularités structurelles et les catégories de pensée spécifiques aux participants.

Nous avons également intégré des éléments de la sémantique structurale pour affiner l'analyse des discours, en mettant l'accent sur les disjonctions et les relations différentielles. Cette méthode permet de construire des typologies des univers symboliques et des contextes organisationnels, offrant une perspective à la fois globale et spécifique sur les expériences socioprofessionnelles des acteurs impliqués.

En combinant une approche narrative non directif avec une posture inquisitoriale et psychanalytique, nous enrichissions notre compréhension des enjeux liés à la cybersécurité et des défis auxquels sont confrontés les auditeurs internes et les RSSI. La méthodologie adoptée assure une exploration rigoureuse et nuancée des récits et des pratiques, en dévoilant les dimensions complexes des rôles et des interactions au sein des établissements bancaires.

3.6 Analyse inter-cas : faire sens d'expériences contrastées

Les recherches empiriques en sciences sociales se fondent sur une approche par cas ou une approche par variables, que le type de données collectées soit qualitatif ou quantitatif (Fiss, 2007).

Nous adoptons une étude de cas comparative abductive entre deux terrains internationaux : le secteur bancaire français et l'autre libanais. Cette approche consiste à identifier les relations observées entre les variables pertinentes du cas.

3.6.1 L'intérêt de l'analyse inter-cas

L'analyse inter-cas constitue une méthodologie essentielle dans notre étude comparative sur le rôle de l'audit interne dans la cybersécurité bancaire, en raison de sa capacité à révéler des dynamiques spécifiques et contextuelles à travers des terrains contrastés. En examinant des banques opérant dans deux environnements distincts — le secteur bancaire français représenté par la BPVF et huit banques « Alpha » libanaises — cette approche permet de comprendre comment des contextes socio-économiques et culturels différents influencent les pratiques de cybersécurité, les identités professionnelles, ainsi que les relations entre auditeurs internes et RSSI.

Notre objectif principal était de dégager des points communs et des divergences significatives entre les deux contextes, en identifiant des modèles récurrents et des tendances émergentes qui caractérisent les rôles et responsabilités des acteurs concernés. Pour ce faire, nous avons structuré notre analyse autour de thématiques spécifiques qui ont émergé de nos entretiens et observations : les identités professionnelles des auditeurs internes et des RSSI, les problèmes juridictionnels, et les dynamiques de territorialité.

Afin de faire dialoguer ces contextes différents et de trouver des points communs aux situations étudiées, nous avons adopté une approche systématique reposant sur un tableau comparatif des thématiques structurantes. Ce tableau a servi de cadre analytique pour comparer les résultats issus des deux terrains, permettant ainsi de mettre en évidence les similitudes et les divergences de manière organisée et cohérente. Par exemple, les différences de réglementation entre les deux pays ont été analysées en parallèle avec les perceptions des auditeurs internes et des RSSI, ce qui a permis de révéler comment ces différences influencent les pratiques de cybersécurité.

En identifiant des modèles récurrents à travers les deux cas, cette analyse nous a permis de tirer des conclusions robustes sur les défis et les opportunités liés à la cybersécurité dans le secteur bancaire. En outre, elle renforce la validité externe de notre étude, puisque les conclusions

issues de la comparaison entre ces deux terrains contrastés peuvent potentiellement être généralisées à d'autres contextes similaires. Enfin, l'approche comparative inter-cas enrichit notre discussion en nous permettant de formuler des recommandations plus nuancées et adaptées aux réalités spécifiques de chaque environnement étudié.

3.6.2 Les modalités de l'analyse inter-cas

Dans notre recherche, l'analyse inter-cas a suivi les étapes suivantes :

- Sélection des cas (pour rappel) : nous avons sélectionné la BPVF pour représenter le terrain bancaire français et huit banques « Alpha » libanaises. Notre choix présente des différences significatives, telles que leur structure organisationnelle, leur taille, leur environnement réglementaire et leurs pratiques en matière de cybersécurité par rapport à chaque banque.
- Collecte des données (pour rappel) : nous cherchons à dégager les identités professionnelles des auditeurs internes et des RSSI dans chaque cas à travers par le guide d'entretien et des observations sur le terrain.
- Analyse des données (pour rappel) : nous utilisons le codage conçu par Dubar et Demazière mentionné précédemment pour structurer notre analyse des entretiens biographiques et identifier les similitudes et les différences entre les banques libanaises et la BPVF en termes d'identités professionnelles et de problèmes juridictionnels liés à la cybersécurité.
- Comparaison des résultats : nous comparons les résultats obtenus pour identifier les modèles, les divergences et les relations entre les identités professionnelles des auditeurs internes et des RSSI, ainsi que les problèmes juridictionnels spécifiques à chaque cas. Nous examinons aussi les facteurs contextuels qui peuvent influencer ces dynamiques.
- Interprétation des résultats : à partir des résultats de notre analyse inter cas, nous tirons des conclusions sur le rôle de l'audit interne dans la cybersécurité bancaire.

Conclusion intermédiaire

L'analyse inter-cas que nous avons présentée dans cette partie 3.5 constitue une étape essentielle pour mieux comprendre le rôle de l'audit interne dans la cybersécurité bancaire. Cette méthodologie comparative entre le secteur bancaire français et libanais offre de nombreux avantages. Tout d'abord, cette approche nous permet d'explorer en profondeur les identités

professionnelles des auditeurs internes et des RSSI, ainsi que les problèmes juridictionnels et de territorialités qui peuvent surgir entre ces acteurs. En considérant la BPVF et huit banques Alpha libanaises comme des cas distincts, nous avez pu analyser les différences contextuelles qui influencent ces dynamiques.

De plus, l'analyse inter cas nous offre la possibilité d'identifier des modèles et des tendances émergents en comparant les résultats des deux terrains. Cette comparaison renforce la validité externe de nos conclusions, les rendant potentiellement généralisables à d'autres contextes similaires.

Enrichissant la discussion et les recommandations, cette approche comparative nous permet de formuler des recommandations plus solides et spécifiques, tenant compte des spécificités de chaque cas. Cela renforce la pertinence pratique de notre étude pour les acteurs de l'industrie de la cybersécurité bancaire.

En résumé, nous menons une analyse inter cas parce qu’elle offre une perspective comparative et approfondie qui contribue à une compréhension nuancée et robuste du rôle de l'audit interne dans la cybersécurité bancaire. Elle tient compte des différences contextuelles, identifie des modèles et des tendances, renforce la validité externe, et enrichit les discussions et les recommandations. Cette approche renforce la qualité et la pertinence de notre recherche.

Synthèse du chapitre 3 : évaluation des méthodes et perspectives de recherche

Ce troisième chapitre a exploré en profondeur le rôle de l'audit interne dans la cybersécurité bancaire à travers une méthodologie rigoureuse et comparative. En suivant une structure analytique détaillée, nous avons abordé successivement les différentes dimensions de notre étude, du cadre théorique aux analyses empiriques. La première partie du chapitre (3.1) a établi le cadre théorique de notre recherche, en définissant les concepts clés liés à l'audit interne et à la cybersécurité. Nous avons articulé les rôles et responsabilités des auditeurs internes et des responsables de la sécurité des systèmes d'information (RSSI), en mettant en lumière leurs interactions et leurs enjeux spécifiques dans le contexte bancaire.

Les sections suivantes (3.2 et 3.3) ont détaillé la méthodologie employée pour la collecte et l'analyse des données. Nous avons utilisé une approche qualitative basée sur des entretiens biographiques pour recueillir des récits détaillés des acteurs impliqués. La partie 3.4 a spécifiquement décrit le processus de codage des données selon la méthodologie de Dubar et Demazière, soulignant l'importance de cette approche pour structurer et interpréter les données qualitatives. Le codage a permis d'identifier des thèmes récurrents, des motifs et des relations causales, offrant une compréhension approfondie des identités professionnelles et des problématiques de cybersécurité dans les contextes étudiés. La partie 3.6 a constitué une étape clé dans notre recherche en permettant une analyse inter-cas comparative entre le secteur bancaire français et libanais. En examinant les pratiques et les dynamiques de cybersécurité à travers ces deux contextes distincts, nous avons pu identifier des modèles récurrents, des divergences et des tendances émergentes. Cette comparaison a enrichi notre compréhension des défis et des opportunités spécifiques à chaque environnement, tout en renforçant la validité externe de nos conclusions.

L'analyse des données collectées et codées, couplée à l'approche comparative inter-cas, nous a permis de dégager plusieurs conclusions importantes :

- Identités Professionnelles et Juridictionnelles : les identités professionnelles des auditeurs internes et des RSSI, ainsi que les problèmes juridictionnels liés à leurs rôles, varient significativement entre les deux contextes étudiés. Les différences de réglementation et de culture organisationnelle influencent ces dynamiques.
- Pratiques de Cybersécurité : les pratiques de cybersécurité diffèrent en fonction des contextes socio-économiques et culturels. Les banques françaises et libanaises

adoptent des approches distinctes en réponse à leurs environnements spécifiques.

- Recommandations Contextualisées : les recommandations formulées à partir de cette analyse sont adaptées aux réalités particulières de chaque contexte, offrant des solutions pertinentes pour améliorer la cybersécurité bancaire à la fois en France et au Liban.

Ce chapitre a fourni une analyse détaillée et comparative du rôle de l'audit interne dans la cybersécurité bancaire. En intégrant des approches théoriques et méthodologiques robustes, nous avons pu éclairer les enjeux complexes liés aux identités professionnelles, aux juridictions et aux pratiques de cybersécurité dans différents contextes. Les résultats obtenus enrichissent notre compréhension des dynamiques internes au sein des établissements bancaires et offrent des perspectives précieuses pour améliorer les pratiques de cybersécurité dans un environnement globalisé et diversifié.

CHAPITRE 4.

RESULTATS DE LA RECHERCHE (1) : CONTEXTE ORGANISATIONNEL ET CONSTRUCTION IDENTITAIRE

Sommaire du chapitre 4. Les résultats de recherche

4. Résultats de recherche

Ce chapitre a pour objet de restituer les résultats de recherche. Il se divise en deux sections. La première détaille les éléments contextuels : l'organisation de la BPVF sur le terrain bancaire français et des banques libanaises sur le terrain bancaire libanais. Nous prenons soin de rappeler l'historique, l'organisation et la politique de gestion des risques dans chaque établissement. La deuxième section appréhende l'organisation de la cybersécurité sous l'angle des identités professionnelles. Précisément il restitue comment se construisent les identités au regard de la question de la cybersécurité. Les schèmes spécifiques des entretiens réalisés à la BPVF et dans les banques libanaises sont présentés en complément. Cette démarche de restitution offre l'occasion de faire dialoguer la construction identitaire relative à un risque (ou un ensemble de risques) et la manière dont un établissement s'organise pour gérer ce risque (ou cet ensemble de risques).

4.1 Contexte d'organisation par établissement

En complément de l'historique, de l'organisation et de la politique de gestion des risques au sein des banques, nous approfondissons le cas de la BPVF au regard du risque cyber en nous fondant sur le rapport d'audit publié en 2018. Nous nous attardons sur le contexte des banques libanaises qui est spécifique par rapport aux banques françaises et mondiales. Nous complétons ces restitutions par un l'examen de la nouvelle organisation mise en place par le groupe BPCE pour gérer les risques de cybersécurité en conformité aux recommandations du rapport d'audit publié en 2022.

4.1.1 De la minimisation des enjeux à une focalisation dans les discours et les actes

Les banques populaires, créées sur un modèle mutualiste, ont fusionné au lendemain de la Première Guerre mondiale pour devenir, entre autres, des banques d'entrepreneurs. Le Groupe BPCE (Banque Populaire - Caisse d'Épargne) est créé en 2009 et progresse jusqu'à devenir actuellement le deuxième groupe bancaire français dans le pays. Il détient Natixis, la Banque Palatine et le Crédit Foncier (BPVF, 2023).

La BPVF est une grande banque de détail chargée, entre autres, de préserver et protéger l'épargne populaire au niveau national français. L'intérêt de l'étude de la BPVF réside dans le fait qu'elle soit un modèle de confiance pour les Français, une banque à taille humaine qui porte des valeurs coopératives et qui est peu exposée à l'international. Elle possède un modèle économique traditionnel qui a bénéficié d'une croissance plus forte que d'autres banques qui

opèrent selon des modèles modernes. Dans ce sens, les banques libanaises sont aussi bâties sur des modèles économiques traditionnels et constituent de ce fait des réplications multiples qui donnent à saisir la variété et la diversité du secteur bancaire libanais.

Le Groupe BPCE, deuxième groupe bancaire en France, couvre l'ensemble des métiers de la banque et de l'assurance à travers ses réseaux coopératifs et indépendants, comprenant 14 Banques Populaires et 15 Caisses d'Épargne, appartenant à 9 millions de sociétaires. En tant qu'autorité centrale et établissement de crédit agréé, BPCE est structuré en société anonyme à directoire et conseil de surveillance, détenue à 50 % par les Banques Populaires, avec la Banque Populaire Val de France (BPVF) détenant 4,31 %. En tant que société holding, BPCE gère les participations dans ses filiales et centralise les excédents de ressources des Banques Populaires, tout en exécutant des opérations financières cruciales pour le développement et le refinancement du groupe. Il est important de souligner que la Banque Populaire Val de France (BPVF) dépend de BPCE pour la gestion des risques, n'étant pas autonome dans ce domaine et respectant les réglementations et procédures établies par le groupe. En ce qui concerne la politique de groupe sur la gestion de la cybersécurité, la BPVF dispose de sa propre organisation interne, de son propre conseil d'administration et de sa propre stratégie commerciale. Le degré d'indépendance de la BVPF par rapport au groupe BPCE varie également en fonction de la nature des décisions prises. Cela permet de s'assurer que ces décisions s'inscrivent dans la stratégie globale du groupe et préservent l'intérêt commun. Dans le contexte de la cybersécurité, la BVPF doit se conformer aux politiques et aux orientations générales de sécurité définies par le groupe BPCE. De fait, la cybersécurité, restée un temps l'affaire des filiales, est devenue un enjeu de groupe.

4.1.1.1 Un risque parmi d'autres : dépendance de la gestion des risques aux ressources entre 2018 et 2019

La BPVF suit les préconisations et les procédures du groupe BPCE en termes de gestion de risques et de profilage de poste au niveau organisationnel : le niveau des risques constitué de la direction des risques, de la conformité et du contrôle permanent du Groupe BPCE en charge du contrôle permanent et Le niveau de l'audit interne constitué de l'audit interne, l'inspection générale du groupe, qui est en charge des inspections régulières. Les fonctions locales de contrôle permanent et périodique s'insèrent dans le cadre de filières de contrôle intégrées, par un lien fonctionnel fort aux directions centrales de contrôle de BPCE correspondantes (BPVF, 2019)

4.1.1.1.1 Première ligne de défense : un contrôle permanent hiérarchique

Le contrôle permanent dit hiérarchique (1^{ier} niveau), premier maillon du contrôle interne, est

exercé par les directions opérationnelles ou fonctionnelles sous l'autorité de leur hiérarchie. Ces services sont responsables des risques associés aux opérations, notamment en mettant en place des autocontrôles formalisés, traçables et déclarables, en vérifiant la conformité des opérations, et en finalisant les procédures de traitement avec des descriptions détaillées des responsabilités et des contrôles. Ils mettent également en œuvre les recommandations des fonctions de contrôle de second niveau et alertent ces dernières en cas de besoin (BPVF, 2019).

Les discours du RSSI Didier. G de la BPVF confirment que les opérateurs informatiques agissent en premier niveau de contrôle pour assurer la cybersécurité à la BPVF.

4.1.1.1.2 Deuxième ligne de défense : un contrôle permanent par des entités dédiées

Les contrôles de second niveau, indépendants des activités opérationnelles, se concentrent sur la documentation et la mise en œuvre du plan de contrôle annuel, la mise à jour des référentiels de contrôle en fonction des risques et des exigences réglementaires, et les inspections permanentes du socle commun du Groupe. Ils produisent et analysent les résultats, assurent un Reporting en lien avec les contrôles de premier niveau, effectuent une revue continue de la mise en œuvre des recommandations, et suivent les plans d'actions correctives définis par le Groupe BPCE (BPVF, 2019).

En termes de sécurité de l'information, ce que nous retenons du discours du RSSI de la BPVF, le responsable de sécurité de l'information RSSI agit en second niveau pour faire face aux cyberattaques dans la BPVF.

4.1.1.1.3 Troisième ligne de défense : l'audit interne implique le contrôle périodique et permanent

L'audit interne de la Banque Populaire Val de France assure des contrôles réguliers sur l'ensemble des activités, incluant le contrôle permanent, pour garantir la qualité, l'efficacité, la cohérence et le bon fonctionnement de la gestion des risques. Il évalue la situation financière, les niveaux de risques pris, et assure la sécurité des données informatiques, en rendant compte directement au Directeur général et au conseil d'administration. Indépendant des directions opérationnelles et du contrôle permanent, l'audit interne intervient également en troisième niveau pour la sécurité de l'information (BPVF, 2019).

Une mission d'audit interne menée en 2019 sur le département informatique a notamment recommandé l'embauche d'un deuxième RSSI au sein de la direction informatique.

Nous présentons un tableau ci-dessous qui regroupe des discours extraits lors de nos entretiens entre 2018 et 2019 avec le Chef de mission d'audit interne, du directeur des risques conformité

et contrôle permanent, du RSSI et du directeur de l'audit interne de la BPVF. L'audit interne est positionné en 3ième niveau au sein de la BPVF en assurance permanente.

Tableau 8 : l'audit interne agit en 3ième ligne de défense

Répondant	Idée-clé	Verbatim
Chef de mission d'audit interne	L'audit interne agit en 3ième ligne de défense.	*« Non moi je ne suis pas tout à fait d'accord. Nous on est en 3ième niveau. Nous on vient vérifier que c'est bien fait mais nous on intervient en 3ième niveau donc pour moi ce n'est pas à nous de maintenir tout seuls la cybersécurité c'est avec la direction des risques, c'est avec les autres services »*
Directeur des risques conformité et contrôle permanent	L'audit interne n'a pas un pouvoir de sanction. Il exerce un contrôle permanent en 3ième ligne de défense.	*« L'audit interne c'est du niveau 3, En France, vous avez le contrôle permanent de niveau 3, le contrôle permanent de niveau 2 c'est moi, et le contrôle de niveau 3 c'est l'audit. Le niveau 3 il fait des missions ponctuelles, des missions qui peuvent être sur la cyber criminalité. Mais un rôle d'audit ni un rôle de contrôle ni un rôle de gérer l'opérationnel. »* *« Les rôles sont clairement définis, et le niveau 3 n'a pas de pouvoir de sanction non plus. »*
Responsable de la sécurité des systèmes de l'information (RSSI)	En France, l'audit agit en troisième niveau en réalisant des missions ponctuelles, périodiques.	*« L'audit, de mon point de vue, c'est la règlementation des contrôles qui, en France et en Europe, intervient en troisième niveau, et effectue des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. Donc, l'audit effectue des missions en troisième niveau qui peuvent être beaucoup plus longues et plus approfondies… »* *« En France, comme je vous l'ai dit, il y a trois niveaux :* *Il y a les métiers qui réalisent des contrôles de premier niveau. Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits. Et puis, il y a l'audit en troisième niveau, comme on disait tout à l'heure, qui effectue des missions ponctuelles, périodiques. »*
Directeur de l'audit interne	L'audit interne n'a pas de rôle opérationnel à mener.	*« L'informatique est un contrôle de premier niveau. L'audit n'a pas de rôle opérationnel à mener. »* *« L'audit interne doit apporter à la gouvernance de la banque l'assurance d'un pilotage effectif et pérenne de la cybersécurité »*

4.1.1.1.4 Le dispositif de gestion des risques et de certification de la conformité

La fonction gestion des Risques et Conformité assure, entre autres, un contrôle permanent des risques et de la conformité. Elle veille à l'efficacité du système de gestion des risques en assurant une évaluation et une prévention des risques, une élaboration d'une politique des risques intégrée aux politiques de gestion des activités opérationnelles, et une surveillance continue des

risques. Au sein de l'organe central de BPCE, la direction des risques, de la conformité et des contrôles permanents du Groupe BPCE est chargée de cohérence, homogénéité, efficacité et exhaustivité de la mesure, du suivi et du contrôle des risques.

Elle est en charge de la gestion consolidée des risques du Groupe BPCE. Donc, la mission de la direction des risques, de la conformité et des contrôles permanents du Groupe BPCE s'exerce de manière indépendante des directions opérationnelles (BPVF, 2019).

4.1.1.1.5 Le rôle de la fonction des risques de la BPVF

Le directeur des risques, conformité et contrôle de la Banque Populaire Val de France rapporte les risques à la direction générale et supervise la politique des risques, en alignant les pratiques avec celles du Groupe BPCE (BPVF, 2019).

Le tableau ci-dessous regroupe le discours extrait lors de nos entretiens entre 2018 et 2019 sur la BPVF du directeur des risques conformité et contrôle permanent. Il confirme que le budget détermine la qualité de la gestion des risques au sein de la BPVF. Il se trouve face à des difficultés en termes de détections des cyberattaques. Il insiste particulièrement sur le poids de la contrainte financière face au coût des opérations de cybersécurité.

Tableau 9 : la gestion des risques demeure une affaire des moyens financiers

Répondant	Idée-clé	Verbatim
Directeur des risques conformité et contrôle permanent	Prévention très faible en cybersécurité à cause du manque de culture et connaissances en sécurité informatique spécialisé.	*« Mon objectif est de rapporter les risques à la direction générale, de prévenir les risques. »* *« C'est un constat sur la partie technique. Et donc, pour faire ce qu'on devait faire, les tests d'intrusion, au niveau de prévention cyber, de faire un scan des données qui étaient sur le serveur, donc un certain nombre de missions, d'actions de mesure d'effectuer en interne. »*
	Même si elle est organisée en interne, la gestion quotidienne de la cybersécurité est coûteuse..	*« Parce que technique, il faut avoir de l'argent pour faire des requêtes, il faut avoir de l'argent pour mettre les machines en travail, il faut avoir de l'argent pour faire des tests d'intrusion et de communication. »*
	Manque de personnels compétents dans le domaine de la cybersécurité exige le recours à un cabinet externe spécialisé pour assister et aider sur certains missions.	*« Oui, on l'a déjà fait l'année passée.et par contre l'année prochaine, on va la refaire. »* *« On n'a pas les gens compétents, et quand on ne les a pas, on fait appel à un cabinet. On n'avait pas la compétence pour faire ce que l'audit nous demande de faire. Donc, on a fait appel à un cabinet pour nous alerter sur le fait des tests d'intrusion, qui sont sur la partie technique, sur la cybersécurité »*

4.1.1.1.7 Les principaux risques de l'année 2018-2019

Le profit de risque global de la BPVF correspond à celui d'une banque de réseau. Les risques sont concentrés essentiellement sur l'activité de crédit, afin de soutenir et de financer l'économie.

La répartition des risques pondérés de la BPVF au 31 décembre 2018 est la suivante :

- Le risque de crédit représente 89,85 % des risques pondérés ;
- Les risques opérationnels représentent 10,15 % des risques pondérés.

Compte tenu de l'activité de la Banque Populaire Val de France (absence de salle des marchés, portefeuille financier limité), le risque de marché est absent des risques pondérés (BPVF, 2019).

Nous présentons ci-dessous le graphe de répartition des risques pondérés de la BPVF extrait du rapport d'audit en 2018 :

Figure 14 : la répartition des risques au sein de la BPVF en 2018

Source : le rapport annuel 2018 de la BPVF (Banque Populaire Val de France, 2019).

De toute évidence les risques liés à la cybersécurité n'étaient pas prioritaires pour la BPVF lors de notre première phase de collecte de données et la réalisation des entretiens. Ces risques étaient intégrés dans les risques opérationnels qui ne représentaient selon le rapport d'audit en 2018 à peine 10% des risques totaux de la BVPF.

Le tableau ci-dessous restitue le consensus du directeur des risques conformité et contrôle permanent, du RSSI et du superviseur de l'audit interne quant au fait que les risques liés à la cybersécurité ne sont – à cette période – pas prioritaires pour la BPVF. Cette gestion des risques dépend de moyens financiers et humains. Pour illustrer l'évolution radicale des points de vue depuis, nous présenterons en troisième partie le rapport d'audit en 2023 qui fait des risques liés à la cybersécurité une priorité et les identifie comme risque majeurs auxquels le groupe BPCE et en particulier à la BPVF font face.

Tableau 10 : la cybersécurité n'est pas qualifié comme risque majeur au sein de la BPVF

Répondant	Idée-clé	Verbatim
Superviseur d'audit interne	L'audit interne ne considère pas le risque de cybersécurité comme un risque important mais le qualifie comme un risque bancaire parmi d'autres.	*« En termes de cyber sécurité, je vais vous dire que ce n'est pas le sujet à l'audit actuel. A l'audit actuellement, ce n'est pas le sujet principal la cyber sécurité. C'est un sujet niveau banque. A l'audit, c'est un sujet parmi tant d'autres. Notre rôle au quotidien est la protection de la clientèle. En termes de régulateur, ce n'est pas la cyber sécurité. »*
Directeur des risques conformité et contrôle permanent	Le directeur des risques déclare que beaucoup d'autres risques sont plus important que le risque cyber à la BPVF.	*« Ce n'est pas seulement le sujet car il y a d'autres risques plus important que le cyber. Il y a plein de risque. ». »*
Responsable de la Sécurité des Systèmes d'Information (RSSI)	La cybersécurité est un risque opérationnel parmi d'autres à la BPVF.	*« Une cartographie c'est destiner à identifier les risques opérationnels, à les évaluer, à sélectionner les plus importants et à mener des plans d'actions de réduction des risques. Sachant que la cyber sécurité est un risque opérationnel parmi d'autres risques opérationnelles.»*

4.1.1.1.8 La macro cartographie des risques

La BPVF dispose d'une cartographie des risques macro conforme à la réglementation dédiée au contrôle interne qui précise la nécessité de disposer d'une cartographie des risques identifiant et évaluant les risques liés aux facteurs internes et externes ainsi que les Orientations sur la gouvernance interne. La BPVF s'aligne avec cette obligation en se conformant à la macro-cartographie établie par le Groupe BPCE. L'objectif principale de cette macro cartographie est de sécuriser le fonctionnement des établissements, de consolider leur rentabilité financière et l'évolution dans le temps. La BPVF comme chaque établissement du Groupe BPCE doit identifier et évaluer ses risques son profil de risque et ses risques prioritaires. Cette approche fondée sur les risques à travers la notation du système de gestion des risques risque permet la mise en place et le suivi de plans d'action ciblés (BPVF, 2019).

4.1.1.1.9 Le suivi des risques liés à la sécurité des systèmes d'information

En dépit de la priorité limitée accordée à la cybersécurité au sein du groupe BPCE, une politique de sécurité de l'information a été instaurée pour protéger les systèmes d'information et définir les obligations à suivre pour tous les établissements de BPCE en France ainsi que pour toute autre entité ayant accès à ses systèmes. En 2018, des améliorations substantielles ont été apportées au pilotage de la gouvernance et des risques en matière de sécurité de l'information, incluant une nouvelle gestion des politiques de sécurité des systèmes d'information, des plans

d'actions spécifiques et une classification des actifs informatiques. Le groupe a également pris des mesures significatives dans le domaine de la cybersécurité, telles que le renforcement des contrôles d'accès aux applications depuis 2015, la sensibilisation continue des employés à la cybersécurité, l'amélioration de la détection des flux et des événements suspects via un Security Operation Center (SOC) Groupe fonctionnant 24/7, et l'intégration du *Computer Emergency Response Team (CERT*) Groupe BPCE dans la communauté *InterCERT-FR* dirigée par l'Agence Nationale de la Sécurité des Systèmes d'Information. De plus, un projet de renforcement supplémentaire au sein de la communauté européenne était en cours de planification pour début 2019.

4.1.1.1.10 La synthèse des risques pour la période de 2018-2019

Selon le rapport d'audit de 2018 de la BPVF, nous pouvons retirer deux hypothèses :

- Le risque cyber est qualifié comme un risque opérationnel parmi d'autres.
- La gestion du risque cyber est dépendante de ressources financières (risques) et de ressources humaines (audit interne).

Nos entretiens avec les différents acteurs au sein de la BPVF valident ces hypothèses.

4.1.1.2 Une approche financière et individualisée du risque cyber en 2019-2020

Le groupe BPCE (Banque Populaire Caisses d'Épargne) a établi un rapport sur les risques le 31 décembre 2021. Ce rapport intitulé « Pilier III » (conformément à la réglementation de Bâle) a pour objectif d'instaurer une discipline de marché par un ensemble d'obligations déclaratives soit qualitatives soit quantitatives en permettant une amélioration de la transparence financière dans l'évaluation des expositions aux risques, les procédures d'évaluation des risques et l'adéquation des fonds propres. Le pilier I s'est intéressé aux prescriptions minimales de fonds propres alors que le pilier II enrichit le processus de surveillance prudentielle. Ce rapport détaille les chiffres clés, la typologie des risques et le contexte réglementaire, les facteurs de risques, l'organisation générale du dispositif de contrôle interne du Groupe BPCE et la gestion du capital et à l'adéquation des fonds propres.

Les différents facteurs et types de risques tels qu'indiqués dans le rapport sont : les risques de crédit, les risques de contrepartie, les opérations de titrisation, les risque de marché, les risque de liquidité, de taux et de change, les risques juridiques, le risque climatique, les risques opérationnels (risques cyber), les risques de non-conformité et sécurité, et les risques assurances, gestion d'actifs, conglomérat financier. (BPCE, 2021)

4.1.1.2.1 La Crise COVID-19 et un nouveau regard sur les risques

En raison de l'évolution de l'environnement, le Groupe BPCE porte une attention particulière à l'anticipation et à la maîtrise des risques émergents. Ainsi, une analyse prospective est réalisée semestriellement pour identifier les risques pouvant affecter le Groupe et est présentée au Comité des risques et de la conformité puis au Comité des risques du Conseil d'administration.

Après une forte contraction de l'économie mondiale liée à la pandémie de Covid-19 en 2020, la révision à la hausse des prévisions de croissance pour juin 2021, notamment pour la France, prouve que la sortie de crise est plus forte que prévu. Cette crise a profondément modifié l'environnement dans lequel évolue le Groupe BPCE. De fait, cela exacerbe considérablement l'impact des différents types de risques qui affectent les activités du groupe.

Compte tenu de ces crises, le groupe BPCE donne la priorité à une vigilance constante et évolutive face aux cyber risques dans un contexte de digitalisation de l'économie et des services financiers. Le groupe BPCE reste attentif envers la sophistication des attaques et les éventuelles vulnérabilités des systèmes IT des banques du groupe. (BPCE, 2021)

C'est seulement en 2021 que la cybersécurité devient un risque opérationnel prioritaire face à tous les autres risques et le groupe BPCE évolue en lançant plusieurs actions pour renforcer la cybersécurité au sein du groupe.

4.1.1.2.2 Une culture renouvelée au bénéfice d'une focalisation sur la cybersécurité

Une étude réalisée par OpinionWay sur la confiance et les banques montre que lorsqu'un évènement négatif comme une cyberattaque entache la confiance des clients de manière durable, il en résulte un recul de l'économie et spécialement dans le secteur bancaire. Cela incite les établissements à prendre en compte les enjeux de cybersécurité et à prendre des mesures pour accroître la confiance dans les dispositifs qui sont mis en place. La crise engendrée par WannaCry n'est plus un problème de cybersécurité ni un problème économique mais aussi un problème de confiance. Sans une cybersécurité fiable et reconnue, la BPVF amenuise son capital de marque. L'étude suggère que l'opinion se fonde plutôt sur la confiance dans la marque que dans la technologie elle-même. Une cyberattaque peut également avoir aussi comme conséquences des coûts élevés en termes de récupération et de vérification des informations corrompues. Au groupe BPCE, l'idée infuse de l'impact financier de la cybersécurité et du coût lié à la gestion des attaques, au risque de réputation et l'attribution qu'il peut engendrer. (BPCE, 2021)

Les entretiens menés entre 2018 et 2019 auprès du RSSI et du directeur de l'audit interne atteste d'un renversement de discours : la cybersécurité au sein de la BPVF « demeure » primordiale

pour restaurer et assurer la confiance des clients d'une part, et pour préserver la valeur de la banque d'une autre part. La cybersécurité y apparaît comme un élément majeur de préservation de la confiance des clients.

Tableau 11 : la cybersécurité restaure la confiance des clients en préservant le capital de la banque

Répondant	Idée-clé	Verbatim
Directeur d'audit interne de l'i-BP	Le directeur d'audit interne de l'i-BP reconnaît que la cybersécurité renforce la confiance des clients en préservant leur données bien protégés.	*« Pour une raison déjà que notre métier bâtit sur la confiance de nos clients, donc, si, Euuuuuuuuuhhh, c'est effectivement nous n'assurons pas la sécurité des données, nous perdrons cette confiance. »*
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Le RSSI prévoit réduire le risque de cybersécurité pour protéger les données bancaires.	*« …risque d'attaques, risque de fuites de données, risque d'arrêt d'activité, risque de cyber malveillant, risque cyber fraude. Je pense au risque, mais je pense aussi à autre mesure pour réduire ce risque pour protéger nos données bancaires. »*

4.1.1.2.3 La synthèse des risques pour la période de 2019-2020

Suite à l'examen du rapport d'audit de 2019-2020 de la BPVF, trois hypothèses émergent quant à l'évolution de la perception du risque :

- Le risque cyber est désormais identifié comme un risque opérationnel prioritaire par rapport aux autres risques ;
- La gestion du risque cyber doit être consolidée par une stratégie de cybersécurité efficace ;
- La cybersécurité est cruciale pour instaurer la confiance des clients et promouvoir la rentabilité financière en préservant le capital de la BPVF.

4.1.2 Une nouvelle organisation de la gestion du risque cyber : un risque majeur, une gestion sous traitée

L'analyse du contexte organisationnel des banques libanaises est cruciale pour offrir une perspective alternative sur la gestion des risques cyber. Notre étude examine des éléments clés tels que la structure organisationnelle, la taille et la complexité des institutions, la réglementation et la conformité, la culture de sécurité, les partenariats, la sensibilisation et la formation, ainsi que la gestion des risques. En analysant ces différents aspects, nous pouvons mieux comprendre les facteurs influençant la cybersécurité dans ce secteur. Cette approche permet également de considérer les spécificités de chaque banque dans notre investigation sur le rôle de l'audit interne dans la cybersécurité bancaire. Notre analyse est complétée par les

données du secteur bancaire français, en particulier celles de la BPVF, qui apportent une richesse et une profondeur supplémentaires. Le contexte bancaire libanais révèle une limitation : bien que la cybersécurité soit reconnue comme un risque tangible, elle n'est souvent pas priorisée en raison du contexte exceptionnel.

4.1.2.1 La liquidité libanaise façonnée par les crises et guerres

Le secteur bancaire libanais a été constamment influencé par les guerres et crises tout au long de l'histoire du Liban, notamment la guerre civile entre 1975 et 1990, qui a gravement affecté l'économie et le secteur bancaire (Chaigne-Oudin et Khoury, 2010).

La stabilisation de la livre libanaise, ancrée au dollar américain depuis 1997, a été une politique centrale pour la Banque centrale libanaise, visant à restaurer la stabilité après une dévaluation significative post-guerre civile (Dibeh, 2002). L'accord de Taëf en 1990 a marqué le début de la restructuration du secteur bancaire, avec des incitations à la consolidation bancaire et au renforcement prudentiel dans les années 1990. Le système bancaire libanais, encadré par des lois spécifiques et un environnement juridique favorable, joue un rôle crucial dans l'économie nationale. Malgré une croissance du PIB, la dette globale a augmenté, majoritairement financée par les banques locales.

Nous soulignons l'impact de la guerre civile sur le secteur bancaire libanais, qui a entrepris une reconstruction et une réforme en libéralisant le secteur financier et en encourageant les investissements étrangers. Les politiques du gouverneur de la BDL, M. Riad Salameh, ont permis de créer une soupape de sécurité grâce à la gestion efficace des réserves de change, maintenant ainsi un niveau élevé de liquidités et de capitaux. Par conséquent, les banques libanaises sont en mesure de s'adapter aux exigences de Bâle II et III et de réorganiser leurs systèmes internes, démontrant ainsi la solidité du secteur bancaire libanais (Khoury, 2011).

Le secteur bancaire libanais a été profondément affecté par une série de crises, y compris la guerre de 2006 avec Israël et la crise politique et économique de 2019, qui ont considérablement perturbé l'environnement bancaire. À son apogée entre 2019 et 2021, le secteur bancaire représentait trois fois le PIB du Liban, avec des dépôts atteignant plus de 150 milliards de dollars (Al-Attar, 2020). La crise financière de 2019 a provoqué une crise de liquidité, marquée par des restrictions sur les retraits en espèces et les transferts à l'étranger, ainsi qu'une dépréciation significative de la monnaie locale, sapant la confiance dans les banques libanaises. Malgré sa robustesse, le secteur bancaire a été affaibli par de lourdes dettes, bien qu'il reste un pilier crucial de l'économie libanaise (Gilguy, 2010).

Nous nous intéressons au niveau organisationnel dans les banques libanaises pour analyser comment est appréhender la cybersécurité.

4.1.2.2 Le secteur bancaire libanais : un relique d'un modèle libéral

Les fondements du libéralisme économique ont été incorporés dans le système législatif après l'indépendance. Le secret bancaire a été garanti par la loi à partir de 1956 et la libre circulation des capitaux a été instaurée en 1948. Le pays a profité de sa situation géographique pour devenir une plateforme financière majeure et un refuge pour les capitaux fuyant la nationalisation du socialisme arabe (Égypte, Syrie et Irak) dans les années 1950 et 1960 (Perosino, 2019).

Le Liban, a été désigné souvent comme la « Suisse du Moyen-Orient » pour son système bancaire libéral. La décision de suivre une législation libérale visant à promouvoir l'attractivité de l'épargne étrangère par le biais du secret bancaire, rend l'économie libanaise en prospérité. La stratégie a porté ses fruits car les investisseurs fuient les pays voisins et déposait leurs capitaux dans les banques libanaises. Le secret bancaire demeure une obligation légale, pour les banques, afin de conserver la confidentialité des informations sur leurs clients. Une levée de cette obligation peut être demandée par la justice dans le cadre d'une enquête pénale. L'opacité du système bancaire varie d'un pays à l'autre, en fonction de sa législation. Le Liban adopte cette législation comme stratégie économique pour attirer les investisseurs bancaires locaux qui souhaitent rester anonymes (Meier, 2022).

Le secret bancaire au Liban, historiquement un levier de croissance économique, s'est transformé en un défi dans le contexte actuel de crise, malgré les efforts de réforme pour se conformer aux normes internationales. Cette pratique discrétionnaire, défendue par l'oligarchie politico-financière, persiste malgré ses implications sur la transparence et les revenus fiscaux. Nos discussions avec les principales banques libanaises mettent en lumière des approches variées en matière de cybersécurité, influencées par la politique bancaire libérale et la diversité organisationnelle au sein de chaque institution.

4.1.2.3 L'impact détaillé de la crise financière de 2019-2021 sur le secteur bancaire libanais

Depuis près de quatre ans, le Liban traverse la crise économique et financière la plus dévastatrice de son histoire moderne, exacerbée par l'épidémie de COVID-19 et l'explosion au port de Beyrouth en 2020. Cette crise a provoqué une contraction économique sévère, avec une diminution drastique du PIB nominal de 52 milliards de dollars américains en 2019 à 23,1 milliards de dollars américains en 2021. Le secteur bancaire libanais, confronté à des contrôles stricts des capitaux et à une crise de confiance, a vu ses activités de prêt et d'attraction de dépôts

gravement affectées. La dépréciation de la monnaie et l'inflation à trois chiffres ont fortement diminué le pouvoir d'achat, impactant particulièrement les petits déposants et les PME. Le taux de chômage a grimpé à 29,6 % en 2022, exacerbant les conditions sociales déjà désastreuses, avec une estimation que plus de la moitié de la population se trouve sous le seuil de pauvreté. (Khalil, 2022).

L'explosion au port de Beyrouth a amplifié les déficiences structurelles persistantes du Liban, incluant des infrastructures défaillantes, un réseau électrique dysfonctionnel, des pénuries d'eau, une gestion insatisfaisante des déchets et des finances publiques déséquilibrées. Une analyse des impacts financiers de la crise de 2019-2021 sur les banques libanaises montre une détérioration marquée des ratios de liquidité depuis 2016, révélant une crise bancaire en gestation depuis plusieurs années. Parallèlement, une diminution de l'implication financière des politiciens dans la recapitalisation des banques après 2017, malgré leur maintien d'une forte influence administrative, souligne leur implication potentielle dans la crise financière du secteur bancaire libanais (El-Chaarani, 2022).

4.1.2.4 La synthèse organisationnelle du terrain bancaire libanais

Suite à nos entretiens sur les huit banques libanaises et quelques observations du secteur bancaire libanais de nature libéral, nous soulignons que la vision et la gestion de la cybersécurité diffère d’une banque à une autre suite à différents facteurs.

Tableau 12 : les idées clés sur le terrain bancaire libanais

Idée-clé	Observations
Autonomie	Les banques libanaises sont autonomes. Dans environnement bancaire libéral, chaque banque est autonome et dispose de sa propre gouvernance et de sa propre stratégie organisationnelle. Nous avons observé une variété de modèles de gestion et d'approches en matière de cybersécurité où chaque banque possède des priorités différentes à la cybersécurité en fonction de ses objectifs commerciaux, de ses ressources disponibles et de son évaluation des risques.
Taille et complexité	Les banques libanaises varient considérablement en termes de taille, de structure et de complexité organisationnelle. Nous avons remarqué la présence des départements dédiés à la cybersécurité avec des équipes d'experts dans les grandes banques. Par exemple, dans la banque AUDI, le département dédié à la cybersécurité est le « Specific Department Information Security and Business Continuity. » D'autres banques plus petites délèguent la responsabilité de la cybersécurité à d'autres départements comme le département informatique. Nous soulignons que cette diversité de taille et de complexité entraîne des différences dans la gestion de la cybersécurité.
Environnement réglementaire	Bien que le secteur bancaire libanais soit libéral, il est également soumis à des réglementations et des directives émises par la Banque du Liban (BDL). Ces exigences réglementaires en matière de cybersécurité sont interprétées et mises en œuvre différemment par chaque banque. Nous avons observé que la banque AUDI adopte des mesures de cybersécurité plus strictes que d'autres en fonction de son interprétation des réglementations et de son engagement envers la protection de ses données et de ses systèmes.
Sensibilité aux risques et attaques	Les banques envisagent les risques et des menaces liées à la cybersécurité de manière différente. La société générale de la banque au Liban SGBL a connu des incidents de sécurité antérieurs et plus conscientes des risques, ce qui les inciter à adopter des mesures de sécurité plus avancées. Il s'agit WannaCry[6] en 2017. D'autres banques moins exposées et moins sensibilisées aux problématiques de cybersécurité ont recours à des pratiques moins avancées.
Culture organisationnelle et leadership	La culture organisationnelle et le leadership influencent la gestion de la cybersécurité. Nous avons observé des dirigeants accorder une grande importance à la cybersécurité et promouvoir une culture de la sécurité à tous les niveaux de l'organisation, tandis que d'autres sont moins négligents à ce domaine.

La gestion de la cybersécurité dans les banques libanaises varie en fonction de l'autonomie institutionnelle, de la diversité organisationnelle, de la taille, de la complexité des

[6] WannaCry a été l'une des pires cyberattaques de tous les temps, avec plus de 200 000 victimes dans le monde et des milliards de dollars de dommages. Introduit pour la première fois le 12 mai 2017, WannaCry est un logiciel malveillant de type crypto Worm ransomware qui cible les ordinateurs exécutant les systèmes d'exploitation Microsoft Windows. Il crypte les données stockées sur votre ordinateur et demande une rançon de 300 à 600 dollars en bitcoins. Lorsque WannaCry est installé sur un ordinateur, il crée également une porte dérobée sur le système infecté.

établissements, du cadre réglementaire, de la perception des risques et menaces, ainsi que de la culture organisationnelle et du leadership. Ces variables conduisent à une diversité d'approches et de pratiques en matière de cybersécurité au sein du secteur bancaire libanais. Malgré le risque réel que représente la cybersécurité pour ces institutions, elle n'est souvent pas considérée comme une priorité absolue dans un environnement global dégradé. L'intégration des données du secteur bancaire français, notamment celles de la BPVF, enrichit notre analyse en offrant une perspective enrichie et approfondie sur le sujet.

Nous constatons que la gestion du risque de cybersécurité est intégrée dans une structure organisationnelle non participative, ce qui peut renforcer des identités distinctes et parfois conflictuelles.

4.1.2.5 La cybersécurité nécessite des ressources internes et externes

La direction générale de la BPVF est responsable de l'évaluation complète et fiable des risques de cybersécurité, rapportant régulièrement au conseil d'administration pour l'approbation du cadre de gestion des risques cyber. Le comité des risques assure la qualité des informations présentées au conseil, tandis que le comité d'audit supervise leur développement et leur surveillance. La direction alloue les ressources nécessaires à la sécurité informatique, en mobilisant à la fois des équipes internes spécialisées et des prestataires externes pour les audits du département informatique.

4.1.2.6 Du principe… : l'usage de ces ressources doit être équilibré

À la BCE, l'approche principale consiste à équilibrer judicieusement les ressources internes et externes pour maintenir le contrôle de la politique de cybersécurité tout en bénéficiant des compétences spécialisées difficiles à acquérir en interne. À partir des observations à la BPVF, il apparaît que les ressources internes sont souvent plus coûteuses mais offrent un niveau de contrôle et de confiance accru. En revanche, les ressources externes sont généralement moins onéreuses mais exigent une confiance et une coordination plus poussées. La direction générale de la BPVF a réussi à harmoniser sa politique de gestion des risques de cybersécurité avec une allocation appropriée des ressources, assurant ainsi une protection efficace de ses systèmes d'information contre les menaces cybernétiques. Bien que certaines tâches de cybersécurité soient externalisées, cela ne décharge pas la responsabilité de sécurité de la BPVF qui demeure responsable de la protection de ses systèmes d'information. La priorité est de garantir que les ressources allouées correspondent aux objectifs de la politique de cybersécurité et que la sécurité soit intégrée dans toutes les décisions commerciales. La collaboration avec des prestataires externes ne remplace pas les compétences internes mais complète la stratégie

globale de gestion des risques de cybersécurité.

4.1.2.7 …à la réalité : la cybersécurité est sous-traitée

La BPVF a opté pour externaliser une partie significative de sa gestion des risques de cybersécurité en raison des compétences spécialisées que ces prestataires externes possèdent et que la banque ne détient pas en interne, tout en cherchant à maîtriser ses coûts dans ce domaine. Cette décision a été prise après une évaluation minutieuse des risques et des avantages associés à l'externalisation, notamment les préoccupations telles que la perte de contrôle sur les informations et les processus, la dépendance excessive envers les prestataires externes, et une potentielle augmentation de la vulnérabilité à des cyberattaques ciblées, toutes régulées par la BCE et l'ANSSI via des normes strictes et des régulations nationales françaises. Pour garantir la sécurité et la conformité, la BPVF utilise des critères rigoureux pour sélectionner ses prestataires externes, tels que des contrats détaillés, des exigences strictes en matière de sécurité et de conformité, une surveillance continue de la performance et des plans de sortie clairs. Il est crucial que la BPVF continue d'investir dans le renforcement de ses capacités internes en cybersécurité afin de superviser efficacement ses relations avec les prestataires externes et de maintenir la sécurité globale de ses opérations bancaires.

4.1.2.8 La cybersécurité est un domaine en constante évolution

La cybersécurité est un domaine en constante évolution et les compétences nécessaires pour garantir la sécurité des systèmes d'information sont hautement spécialisées et demandent une mise à jour continue des connaissances. Les campagnes de sensibilisation à la cybersécurité réalisées par la BPVF sont à ce sujet notables. La directrice de l'audit a décidé d'avoir recours à un prestataire extérieur pour effectuer des tests d'intrusion en raison du manque de compétences en interne pour ce type d'audit. Nous avons observé que les audits internes bancaires sont très différents des audits de sécurité informatique et que les équipes internes d'auditeurs bancaires ne possédaient pas les compétences nécessaires pour effectuer des tests d'intrusion de manière efficace. A la demande supplémentaire des auditeurs internes, le recours à ce prestataire externe a été réalisé et pour garantir que les tests sont effectués avec précision et professionnalisme.

4.1.2.9 Un budget d'audit interne pour renforcer la cybersécurité

Au niveau de la direction de l'audit interne, un budget annuel peut être utilisé pour faire appel à des prestataires externes sur des spécificités ou expertises techniques qui ne sont pas disponibles en interne. Ces profils des collaborateurs présents dans les équipe d'audit n'ont pas des compétences techniques informatiques dans la sécurité. En revanche, nous avons noté le

choix de la BPVF de na pas constituer un budget en interne pour former les auditeurs en place ou recruter des auditeurs internes spécialisés en sécurité informatique.

4.1.2.10 Faire intervenir des prestataires spécialisés en sécurité informatique pour effectuer des tests d'intrusion

La cybersécurité se transforme constamment avec des menaces et des vulnérabilités qui évoluent rapidement. Nous avons observé le manque de compétences en interne en cybersécurité. En découle, la nécessité de faire appel à des cabinets extérieurs pour combler les lacunes comme les tests d'intrusion, les audits de sécurité, les analyses de vulnérabilités... La BPVF a fait intervenir des prestataires externes spécialisées en sécurité informatique pour effectuer des tests d'intrusion parce qu'elle ne possède pas l'expertise et les ressources nécessaires pour effectuer de tels tests en interne. Nous retenons une pénurie de compétences spécialisées et un manque de ressources budgétaires pour investir dans la formation et les outils nécessaires.

Les tests d'intrusion sont perçus par le RSSI de la BPVF comme une cause potentielle de dommages collatéraux et de perturbation du fonctionnement normal des systèmes. Il justifie le recours à des prestataires externes pour ce type de mission, car ils disposent de l'expertise technique nécessaire pour mener ces tests en toute sécurité.

4.1.3 Une gestion du risque cyber au sein de la BPVF : un modèle français

Le rapport d'audit en 2022 fait état de l'émergence d'une nouvelle organisation au sein du groupe BPCE en matière de SSI. Le groupe BPCE institue des projets d'amélioration de la résilience opérationnelle parmi lesquels une feuille de route résilience cyber est prise en charge par un groupe de travail dédié.

La BPVF commence à adopter de nouvelles politiques de cybersécurité à l'échelle de la gestion organisationnelle de la sécurité des systèmes d'informations.

4.1.3.1 L'architecture de la sécurité des systèmes d'informations (SSI)

La Direction Sécurité Groupe (DS-G) est devenue responsable de la sécurité des systèmes informatiques (SSI) et de la lutte contre la cybercriminalité en définissant, mettant en œuvre et évoluant les politiques SSI groupe. Elle réalise aussi un contrôle permanent et consolidé de la SSI ainsi qu'une veille technique et réglementaire. En 2022, le groupe BPCE a mis en place une nouvelle filière SSI qui regroupe le responsable de la sécurité des systèmes d'information groupe (RSSI-G), laquelle anime cette filière et les responsables SSI de l'ensemble des entreprises, parmi lesquels se trouve le RSSI de la BPVF. Le RSSI de la BPVF était jusque-là

rattaché à la DSI (Le RSSI réunit la cellule de crise en cas d'attaque et sert d'interface avec les opérateurs informatiques de l'i-BP). Une nouvelle organisation est mise en place, qui regroupe tous les RSSI des établissements liés, filiales directes et des GIE informatiques fonctionnellement au RSSI-G (BPCE, 2021).

Nous évoquons ici le sujet de la culture de cybersécurité, de la mise en place d'un réseau de défense pour faire face aux cyberattaques qui se fonde sur le partage d'informations relatives aux menaces en cybersécurité. Les banques sans exception sont attaquées et sont incapables d'anticiper la menace. Il s'agit d'instaurer une culture de défense collective, et de créer un réseau de défense.

La création de ce réseau nécessite une mise en conformité aux standards du réseau bancaire, une large couverture en matière de cyber-assurance et un effort de responsabilisation de la banque, de l'employé au management : un cercle vertueux est créé (Trouchaud, 2018).

Cette collaboration conjointe à la capitalisation du savoir et de prospective autour des incidents de cybersécurité, de façon quasi mécanique, doit accroitre le niveau de sécurité global. Dans ce contexte renouvelé, le RSSI occupe désormais une place centrale, *a minima* pour diffuser l'information.

4.1.3.2 Les missions du RSSI-Groupe

Un RSSI-G est placé pour lier tous les RSSI des différents établissements. Il anime et coordonne les réunions entre les RSSI à travers ce lien fonctionnel en impliquant que :

- Toute nomination de responsable SSI soit notifiée au RSSI-G ;
- La politique sécurité des systèmes d'information groupe soit adoptée au sein des entreprises selon des modalités d'application soumises à la validation du responsable SSI groupe.

Les rapports concernant le niveau de conformité à la politique du groupe SSI, l'examen continu de SSI, le niveau de risque SSI, les incidents majeurs SSI et les mesures prises sont envoyés au RSSI Groupe (BPCE, 2021).

Le positionnement du RSSI devient central dans le groupe BPCE. Il doit agir comme le chef d'orchestre en matière de cybersécurité. Il se positionne comme un consultant interne qui aide les dirigeants à arbitrer les données en cybersécurité.

4.1.3.3 La cartographie de la sécurité des systèmes de l'information

Le discours du RSSI sur la cartographie des risques opérationnels fait nettement apparaître des risques liés à la cybersécurité. Pour l'audit interne en revanche, ce risque n'est pas prioritaire.

Le superviseur d'audit explique : *« en termes de cybersécurité, je vais vous dire que ce n'est pas le sujet à l'audit actuel. A l'audit actuellement, ce n'est pas le sujet principal la cyber sécurité. C'est un sujet niveau banque. A l'audit, c'est un sujet parmi tant d'autres. Notre rôle au quotidien est la protection de la clientèle. En termes de régulateur, ce n'est pas la cyber sécurité… »*

La BPCE a mis en place un nouveau projet d'élaboration d'une cartographie SSI exhaustive des systèmes d'information du groupe et des systèmes d'information privés des établissements à travers deux chantiers majeurs :

- Une campagne annuelle d'évaluation de la maturité du Groupe sur les cinq piliers référentiel NIST *(Detect, Identify, Protect, Respond, Recover)* afin d'atteindre les objectifs chiffrés, de piloter les actions et d'en mesurer l'efficacité ;
- Un programme groupe de gestion des identités et des droits (IAM) qui a pour objectif d'établir des référentiels groupe pour les personnes, les applications et les entreprises, et d'intégrer toutes les applications du Groupe dans l'IAM avec un provisionnement automatique et une vue globale des habilitations (BPCE, 2021).

4.1.3.4 Les nouveaux dispositifs mis en place pour lutter contre la cybercriminalité

Avec la transformation numérique, l'ouverture des systèmes d'information du Groupe sur l'extérieur (cloud, Big data, etc.), une évolution des usages des collaborateurs et des clients conduit également à une plus grande utilisation d'Internet et des technologies connectées (tablettes, smartphones, applications fonctionnant sur tablettes et mobiles…). De ce fait, les actifs du groupe sont de plus en plus exposés aux cybermenaces. Ces attaques visent une cible bien plus large que les seuls systèmes d'information. Leur objectif est de tirer parti des vulnérabilités et des faiblesses potentielles des clients, des employés, des processus métier, des systèmes d'information et des systèmes de sécurité des campus et des centres de données.

C'est pour ces raisons que le groupe BPCE a mis en place des dispositifs pour réduire les risques liés à la cybersécurité à travers la mise en place d'un nouveau *Security Operations Center (SOC)* group unifié opérationnel intégrant un niveau 1, fonctionnant en 24x7. Des mesures additionnelles ont été prises pour renforcer les dispositifs de lutte contre la cybercriminalité :

- Travailler sur la sécurité des sites web hébergés en externe ;
- Améliorer la capacité des tests de sécurité pour les sites Web et les applications ;
- Mettre en place d'un programme de Divulgation Responsable des vulnérabilités par

le CERT[7] Groupe BPCE (BPCE, 2021).

4.1.3.5 Les nouvelles campagnes de sensibilisation des collaborateurs à la cybersécurité

En 2021, au sein de la BPCE SA, les efforts en matière de sensibilisation à la sécurité des systèmes d'information (SSI) ont été intensifiés, avec la poursuite des campagnes annuelles contre le phishing et la participation active au « Mois européen de la cybersécurité ». Les activités incluent des vérifications régulières des permissions et des droits sur les ressources du système d'information, la surveillance étendue des contenus web publiés, ainsi que le renforcement des plans de traitement des vulnérabilités et de la prévention des fuites de données par courriel ou via des services en ligne. De plus, de nouvelles initiatives de sensibilisation et de formation, telles que des tests de phishing et des séances d'accueil pour les nouveaux collaborateurs, ont été lancées pour renforcer la sécurité face aux menaces croissantes liées au travail à distance (BPCE, 2021).

4.1.3.6 Sortir de la gouvernance verticale

Pendant notre analyse approfondie de la BPVF, nous avons remarqué que la direction générale assigne au RSSI un rôle essentiellement technique, fondé sur ses compétences spécialisées en systèmes informatiques. En ce qui concerne la gestion de la cybersécurité, le RSSI reconnaît son manque d'expertise et délègue cette fonction aux opérateurs informatiques de l'i-BP (voir tableau 13).

[7] Autorité de certification du groupe

Tableau 13 : le RSSI est mal positionné et limité en compétences en sécurité informatique

Répondant	Idée-clé	Verbatim
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Le RSSI avoue qu'il n'est pas expert dans le domaine de la cybersécurité.	*« Dans le domaine de la cybersécurité, les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire, comme la « BPVF », nous ne sommes pas des experts en sécurité informatique. Les experts en sécurité informatique sont chez les opérateurs informatiques et ne sont pas dans les établissements comme une banque populaire.»*
	Le RSSI limite son rôle en cybersécurité à réunir la cellule de crise et faire le lien avec les opérateurs informatiques.	*« Personnellement, en tant que responsable de la sécurité des systèmes d'information en cas de crise et moi qui réunirait la cellule de crise avec tous les métiers dont je vous ai parlé tout à l'heure. Et c'est moi qui fais l'interface entre ces métiers et les opérateurs informatiques. »*
	Le RSSI confie une partie de ses tâches pour assurer la cybersécurité aux opérateurs informatiques.	*« C'est ce que je vous ai expliqué plutôt le travail des opérateurs informatiques. On confit notre informatique à un opérateur et c'est eux qui sont en charge de mettre en place des contres mesures pour éviter le risque de cyberattaque. »*
	Le RSSI préconise que les décisions stratégiques en cybersécurité sont prises par la direction générale.	*«Les décisions menées sur les systèmes d'information sont faite par la direction générale.»*
Responsable informatique	Les responsables informatiques sont sensibilisés par le RSSI s'il y a des attaques.	*« S'il y a des incidents ou des attaques qu'on était perçu par la centrale informatique. Il va nous sensibiliser et donc nous on va faire la communication auprès des collaborateurs. »*
	Le RSSI se concentre sur le rôle de sensibilisation pour fournir les informations nécessaires et faire le relai auprès des utilisateurs.	*« Le problème c'est moi que le seul rôle que je peux avoir, car tout ce qui est outils informatiques et réseaux c'est piloter par la centrale informatique. J'ai aucun moyen. Mais la détection à notre niveau, elle est toujours après. On ne peut rien anticiper, on ne peut rien mesurer. Donc pour moi, à mon niveau, ça va être la sensibilisation, la communication ou bien la gestion de la crise quand il y a une attaque et du coup donc j'ai vraiment besoin du RSSI et de la sécurité groupe parce que c'est eux qui vont nous alimenter en informations pour pouvoir faire le relai auprès des utilisateurs. »*

La BPVF applique une structure de gouvernance verticale où le RSSI se concentre principalement sur la sensibilisation des collaborateurs et la coordination de la cellule de crise en cas d'incident cybernétique, agissant comme un intermédiaire entre les opérateurs informatiques et la direction générale pour les décisions stratégiques. Ce modèle révèle une perception limitée du rôle du RSSI en matière de cybersécurité par les responsables

informatiques. Parallèlement, les décisions stratégiques concernant la cybersécurité sont souvent prises par des gestionnaires qui ne possèdent pas nécessairement une expertise approfondie dans ce domaine, soulignant ainsi la nécessité d'adopter un modèle de gouvernance participative intégrant tous les acteurs clés, y compris les experts en sécurité informatique, les auditeurs internes et les utilisateurs finaux.

Dans cette optique, la BPVF, intégrée dans le groupe BPCE, commence à mettre en œuvre une approche plus holistique de la sécurité de l'information à travers toute l'organisation, en renforçant une culture de la sécurité encourageant l'engagement de tous les niveaux. Un comité de sécurité de l'information a été instauré, réunissant régulièrement des représentants de diverses parties prenantes pour évaluer les risques et élaborer des stratégies préventives, supervisé par le RSSI-Groupe. Ce dernier doit désormais relever directement de la direction générale plutôt que de la direction informatique, et ses responsabilités doivent inclure des compétences de gestion stratégique visant à protéger efficacement les données sensibles de l'institution bancaire.

Conclusion intermédiaire

Cette partie 4.1 propose une analyse approfondie du cadre organisationnel de la BPVF au sein du secteur bancaire français et des banques libanaises dans leur contexte spécifique, mettant en lumière les politiques de gestion des risques avec un accent particulier sur la cybersécurité. Nous avons examiné en détail la structuration de la BPVF au sein du groupe BPCE, soulignant son degré variable d'autonomie et sa conformité aux directives du groupe en matière de sécurité informatique. La gouvernance, le contrôle interne et la gestion des risques sont organisés selon le modèle des trois lignes de défense, avec une participation accrue du RSSI et de l'audit interne dans la réponse aux menaces cyber.

Cependant, la cybersécurité n'a pas été une priorité majeure pour la BPVF à l'époque de notre étude, représentant une fraction des risques totaux, ce qui a retardé la mise en œuvre de mesures correctives adaptées aux défis actuels. La pandémie de COVID-19 a marqué un tournant, avec une prise de conscience croissante des risques cyber, incitant le groupe BPCE à renforcer ses dispositifs de sécurité. Une nouvelle structure organisationnelle a émergé, mettant l'accent sur la création d'un réseau de défense collaboratif et la centralisation des responsabilités du RSSI pour une meilleure coordination.

Concernant les banques libanaises, nous avons mis en lumière l'impact des conflits et des crises sur leur approche de la cybersécurité, influencée par des stratégies diversifiées liées à

l'autonomie institutionnelle, à la diversité organisationnelle et à la perception des risques. La cybersécurité représente un risque tangible mais n'est pas considérée comme une priorité dans le contexte difficile du Liban.

En synthèse, cette section a mis en évidence l'évolution des perspectives internes sur le risque cyber et les structures organisationnelles adoptées, se déclinant en trois phases :

- Initialement, le risque cyber était considéré comme un risque parmi d'autres, géré de manière marginale par le RSSI et l'audit : une juridiction anecdotique partagée RSSI et audit;
- Le risque cyber a été centralisé et intégré comme une responsabilité commune et centrale : une juridiction commune et centrale ;
- Ultérieurement, il a été externalisé vers des entités spécialisées, marquant ainsi une évolution vers une gestion externalisée du risque cyber : une juridiction externalisée.

4.2 Les identités professionnelles au regard du risque cyber

Dans cette section, nous appréhendons la cybersécurité sous la perspective des identités professionnelles. Nous présentons les schèmes spécifiques des entretiens réalisés à la BPVF qui valident les points du rapport d'audit publié en 2019 en aboutissant en particulier aux résultats de recherche issues du schème spécifique du RSSI. Nous introduisons le schème commun qui résume la situation à la BPVF en soulignant les résultats de recherche liées à l'identité professionnelle des acteurs au sein de la BPVF en matière de cybersécurité. Nous concluons cette section par le schème commun aux entretiens réalisés dans les banques libanaises en finalisant par les résultats de recherche associés au secteur bancaire libanais.

4.2.1 Les schèmes spécifiques des entretiens réalisés à la BPVF confirment les points du rapport d'audit de 2019

En nous conformant à la méthode de codage de Dubar et Demazière (1997) nous faisons ressortir les points saillants des identités professionnelles des acteurs concernés et nous mesurons les conséquences au regard de la gestion du risque cyber.

4.2.1.1 La synthèse chronologique de codage en fonction des identités professionnelles

Le codage a été réalisé selon la méthodologie de Dubar et Demazière pour identifier les identités professionnelles des acteurs concernés. Tout d'abord, nous avons procéder à la phase de collecte des données en menant des entretiens biographiques avec les différents acteurs au sein de la BPVF dans le domaine de la cybersécurité en se focalisant sur les professions d'audit interne et de RSSI. Au cours de ces entretiens, nous avons recueilli des informations pertinentes sur leur identité professionnelle telles que les expériences professionnelles, les compétences, les responsabilités, les valeurs, les attitudes...

Après retranscription, nous avons procédé à une analyse thématique des données transcrites détaillé dans le chapitre de la méthodologie. Une fois les thèmes et les catégories identifiés, nous avons attribué des codes ou des étiquettes spécifiques à chaque occurrence des thèmes dans les entretiens. Nous avons organisé ces codes par un schème spécifique à chaque entretien qui permet de visualiser les différentes catégories et les occurrences des acteurs dans les entretiens. En analysant les codes et les schèmes émergents, nous pouvons interpréter les données pour comprendre plus en profondeur l'identité professionnelle des auditeurs internes et des RSSI dans le domaine de la cybersécurité à la BPVF. Nous avons identifié les caractéristiques clés, les similitudes et les différences entre les auditeurs et les RSSI afin de tirer des conclusions sur les dynamiques professionnelles.

Cette méthodologie de codage nous permet d'obtenir une compréhension approfondie de l'identité professionnelle des auditeurs internes et des RSSI au sein de la BPVF en rapport avec la cybersécurité.

4.2.1.2 Le schème spécifique à chaque entretien

Les récits spécifiques des acteurs interrogés (directeur d'audit interne, responsable de la sécurité de l'information, responsable informatique, directeur de l'audit interne i-BP, le directeur des risques conformité et contrôle permanent, le superviseur de l'audit interne, le chef de mission d'audit interne et la directrice générale, expriment des difficultés importantes et récurrentes aux niveau de la compréhension de la cybersécurité au sein de la BPVF. Nous avons remarqué que chaque acteur développe sa propre vision quand il s'agit de gérer la cybersécurité.

Dans chacun des huit entretiens analysés, nous avons repéré une disjonction principale qui opère la partition des séquences racontant le parcours des actants intervenants dans le récit et les arguments délimitant le point de vue du sujet. Cette trame commune au-delà des spécificités des histoires individuelles, ne manque pas d'évoquer la même problématique : le manque de compétences informatiques spécialisées dans le domaine de la cybersécurité.

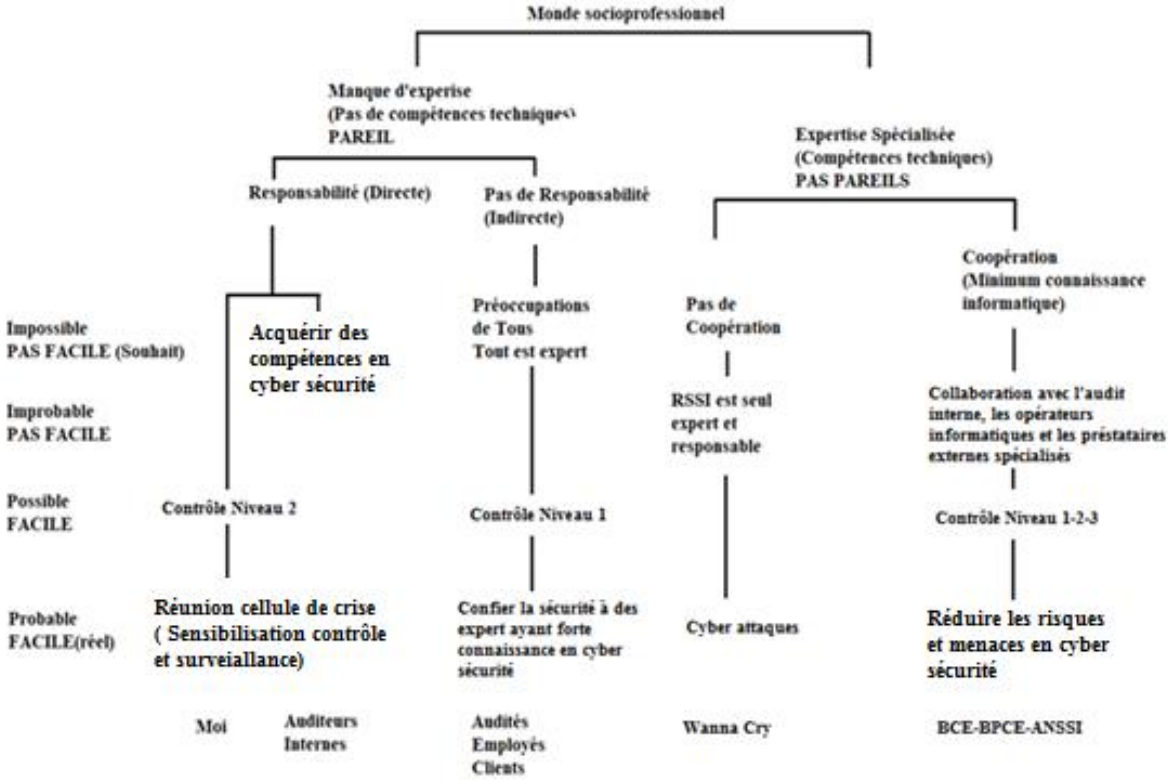


Figure 15 : Le schème spécifique du RSSI

Source : Élaboration personnelle

Nous présentons ci-dessus comme illustration le schème spécifique du responsable de sécurité des systèmes de l'information. Le reste des schèmes sera présenté en annexes.

4.2.1.3 La synthèse du schème identitaire spécifique du RSSI en lien avec son la cybersécurité

Dans le cadre spécifique du RSSI, une analyse révèle deux catégories distinctes dans son environnement socioprofessionnel. D'une part, il identifie une catégorie similaire à la sienne, regroupant des individus sans compétences techniques ni expertise en cybersécurité. Au sein de cette catégorie, le RSSI assume des responsabilités telles que la sensibilisation, la surveillance et la coordination de la cellule de crise, qu'il considère comme relativement simples. Il justifie cette approche en soulignant que sa fonction se positionne principalement au deuxième niveau de défense, rendant ardue l'acquisition de compétences techniques approfondies en cybersécurité. D'autre part, le RSSI distingue une catégorie différente composée d'acteurs possédant une expertise avérée en cybersécurité. En raison de ses propres limites techniques, il ne s'identifie pas pleinement à cette catégorie. Il affirme que la responsabilité de la sécurité en cybersécurité est une préoccupation partagée par tous les acteurs de la BPVF, y compris les clients et les employés, et estime crucial de confier cette sécurité à des experts possédant des compétences solides dans ce domaine. Il exprime le désir de collaborer étroitement avec l'audit interne, les opérateurs informatiques et les prestataires externes spécialisés afin de garantir la sécurité des systèmes d'information, en proposant la mise en place de niveaux de sécurité clairement définis (niveaux 1, 2 et 3) pour réduire efficacement les risques et les menaces.

L'identité professionnelle du RSSI dans ce contexte spécifique se manifeste à travers les concepts d'identité autonome et d'identité attribuée, ainsi que par la distinction entre les pairs et les non-pairs. L'identité autonome fait référence à la perception que le RSSI a de lui-même, de son rôle et de ses compétences dans le domaine de la cybersécurité. Il se voit comme un acteur ayant à la fois des responsabilités directes et indirectes dans ce domaine, tout en reconnaissant les limites de ses compétences techniques. L'identité attribuée, quant à elle, renvoie à la manière dont le RSSI est perçu par les autres acteurs de la BPVF. Il fait une distinction entre ceux qui partagent ses limitations techniques (tels que les auditeurs, les employés et les dirigeants) et ceux qui possèdent des compétences spécialisées en cybersécurité (comme l'Agence nationale de la sécurité des systèmes d'information et les opérateurs informatiques). Cette distinction repose sur les compétences techniques et l'expertise en cybersécurité. Le RSSI se sent exclu de la catégorie des non-pairs en raison de ses propres déficiences dans ce domaine.

En conclusion, l'identité professionnelle du RSSI par rapport à la cybersécurité est caractérisée par sa reconnaissance de sa position intermédiaire dans la hiérarchie de la sécurité informatique, située entre les non-spécialistes et les experts en cybersécurité au sein de la BPVF. Il joue un rôle de facilitateur en orchestrant la collaboration entre divers acteurs clés et en promouvant l'établissement de niveaux de sécurité bien définis pour renforcer la protection contre les risques et les menaces en matière de cybersécurité.

4.2.2 Le schème commun aux huit entretiens réalisés dans la BPVF

Pour présenter le schème commun, nous nous sommes fondés sur les huit schèmes spécifiques réalisés sur les significations du manque de compétences en cybersécurité.

Les récits des différents acteurs montrent comment se construit, à travers le recours à des cabinets externes spécialisés, la déresponsabilisation sur l'assurance de la cybersécurité, la peur de ce risque majeur… Aussi, aux impasses et à la faiblesse des compétences techniques, ils opposent des normes formelles et des procédures explicites (certifications, diplôme spécialisé, examen…) qui présentent ce manque de profils en interne. Ils se fondent donc sur des prestataires externes spécialisés pour les aider à abandonner la « casquette » *non technique* voire *incompétent* pour gérer la cybersécurité.

4.2.2.1 Un schème commun en lien avec l'identité professionnelle

Nous analysons le schème commun qui est un résumé qui regroupe les points saillants des identités professionnelles des acteurs clés au sein de la BPVF. Nous l'avons construit en analysant les schèmes spécifiques à travers les entretiens menés avec le RSSI, le responsable informatique, le directeur d'audit interne, le directeur d'audit interne de l'i-BP, le chef de mission d'audit interne, le superviseur d'audit interne, le directeur des risques conformité et contrôle permanent et le directeur général.

4.2.2.2 Synthèse du schème commun regroupant les huit entretiens

Le schème commun de la BPVF met en évidence plusieurs aspects clés de l'identité professionnelle des acteurs rencontrés.

Elle souligne l'existence de deux mondes socioprofessionnels au sein de la BPVF, distingués par la présence ou l'absence d'expertise technique en interne. Le premier groupe, qualifié de PAREIL, est caractérisé par un manque d'expertise technique interne, ce qui conduit à l'externalisation de certaines responsabilités liées à la cybersécurité. Dans ce groupe, la responsabilité directe du RSSI est limitée à la sensibilisation et à la réunion de la cellule de crise. Pour renforcer le RSSI qui présente un manque de compétence en cybersécurité, l'audit

interne a recommandé d'embaucher un deuxième RSSI à temps plein pour couvrir tous les aspects de la banque. Cependant, des contraintes de coût et de budget orientent la stratégie de la BPVF à externaliser l'assurance de la cybersécurité au lieu de former les gens en interne.

Le deuxième groupe, qualifié de PAS PAREILS, est associé à une expertise technique présente en externe. Il met en évidence le recours à des experts externes pour assurer la cybersécurité, mais également aussi pour éviter les tensions et les conflits entre l'audit interne et le RSSI dans la gestion de la cybersécurité. La collaboration et la coopération entre les professions restent un objectif à atteindre, avec des initiatives telles que le recours à un cabinet externe spécialisé pour les missions d'audit sur le département informatique.

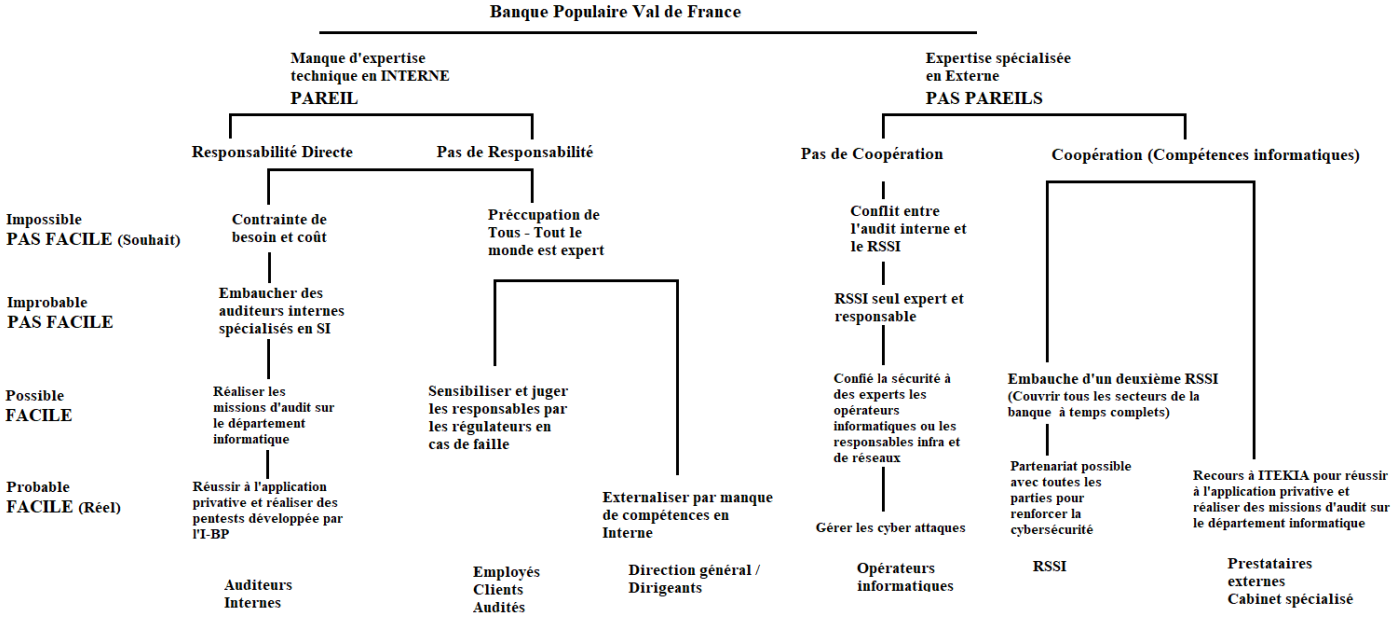


Figure 16 : le schème commun regroupant les huit entretiens de la BPVF

Source : élaboration personnelle

Cette synthèse permet de saisir que la construction identitaire des acteurs concernant le champ de la cybersécurité conforte le recours à des ressources externes. La construction de cette identité partiellement commune « d'incompétents en cybersécurité » facilite la collaboration et la coopération entre les différentes fonctions, notamment l'audit interne et le RSSI.

4.2.2.3 Le schème commun associé aux identités professionnelles des auditeurs internes et RSSI

Nous pouvons observer des aspects spécifiques liés à l'identité professionnelle de l'auditeur interne et du RSSI au sein de la BPVF. Le RSSI, se présentant comme un généraliste et un

facilitateur, opère finalement dans un domaine proche de celui de l'audit interne. L'auditeur interne, bien que faisant partie du groupe des PAREILS sans expertise technique, joue un rôle distinct et crucial en étant impliqué dans la gestion de la cybersécurité en tant que 3ième ligne de défense. Il fournit des recommandations suite aux missions d'audit interne réalisées sur le département informatique. Des tensions peuvent émerger entre l'audit interne et le RSSI lors des missions d'audit, suggérant un désaccord potentiel quant aux responsabilités et à l'approche de la cybersécurité au sein de la BPVF. L'auditeur interne, chargé de juger les responsables en cas de faille de sécurité, souligne son rôle de contrôle et de surveillance, distinct de celui du RSSI.

Quant au RSSI, son rôle est crucial pour la cybersécurité de la BPVF. Il navigue dans un monde socioprofessionnel divisé en deux catégories : le groupe PAREIL sans expertise technique, et le groupe PAS PAREIL composé d'experts externes en cybersécurité. Le RSSI ne se sent pas inclus dans la seconde catégorie en raison de ses propres limitations techniques. Néanmoins, la structure lui assigne la responsabilité directe de la cybersécurité. En réponse, le RSSI limite son rôle à la coordination de la cellule de crise en cas d'attaques et à la sensibilisation.

Dans le contexte de l'identité professionnelle, nous soulignons certains éléments liés à la position du RSSI au sein de la BPVF. Selon le schème commun, le RSSI est décrit comme faisant partie du département informatique, étant rattaché à la DSI. Le rattachement hiérarchique des acteurs influence la construction identitaire des acteurs. Cela peut indiquer une position organisationnelle qui influence son identité professionnelle. Le fait que le RSSI soit attaché à la DSI peut créer une dynamique particulière où ses responsabilités et son rôle dans la cybersécurité sont affectés par cette relation hiérarchique. Par exemple, le RSSI se retrouve parfois en conflit avec l'audit interne lors des missions d'audit sur le département informatique. Cette dynamique reflète des différences d'opinions et d'approches entre l'audit interne et le RSSI en matière de cybersécurité. L'auditeur interne construit son identité à partir d'un corpus normatif, basé sur les normes et nouvelles réglementations en cybersécurité, tandis que le RSSI le fait à partir de son expérience professionnelle au sein du service.

L'auditeur interne a une responsabilité directe et indirecte à l'égard de la cybersécurité. La responsabilité directe dans la surveillance des pratiques au sein de l'organisation. En cela il se conçoit comme contribuant à la protection des informations et des systèmes contre les cybermenaces. Sa responsabilité indirecte tient à son positionnement comme acteur-pivot. La cybersécurité est une préoccupation pour tous, y compris des clients et des employés. L'auditeur est donc tout désigné pour collaborer avec le régulateur dans l'élaboration des normes.

Le RSSI assumer également une responsabilité double. Sa responsabilité directe relève de l'assurance de la cybersécurité au sein de la BPVF. Il a la responsabilité de réunir une cellule de crise en cas d'incident de sécurité et de sensibiliser l'organisation aux enjeux de cybersécurité. Sa responsabilité indirecte est liée au recrutement des experts externes en cybersécurité.

Nous concluons que cette analyse des identités professionnelles sous l'angle organisationnel met en évidence les dynamiques et les tensions potentielles qui peuvent exister au sein de la BPVF en matière de cybersécurité. Il est essentiel d'établir une collaboration solide entre les auditeurs internes, les RSSI et d'autres parties prenantes pour garantir une approche intégrée et efficace de la gestion de la cybersécurité dans l'organisation.

4.2.2.4 Les résultats de recherche issues du schème commun dans la BPVF

La synthèse du schème commun met en évidence les caractéristiques et les dynamiques clés liées à l'identité professionnelle des acteurs au sein de la BPVF en matière de cybersécurité. Les identités professionnelles structurent les pratiques en même temps qu'elles sont structurées par ces dernières. L'auditeur interne se positionne comme un généraliste-pivot, tandis que le RSSI, bien que partiellement expert en cybersécurité, agit davantage comme un animateur, ce qui le conduit à adopter un rôle de généraliste. Nous aboutissons à un professionnel spécialisé dans les processus (généraliste de processus) et un spécialiste des méthodes (généraliste des méthodes). Cette situation soulève une question critique : n'y a-t-il pas un généraliste de trop dans la structure organisationnelle ?

Cette observation met en lumière les tensions potentielles et les chevauchements de rôles au sein de la BPVF. L'auditeur interne, en s'appuyant sur un corpus normatif et des réglementations en cybersécurité, exerce un contrôle et fournit des recommandations basées sur les normes. De son côté, le RSSI, bien qu'initialement focalisé sur des tâches techniques, évolue vers une position plus générale, centrée sur la coordination et la sensibilisation.

Ces dynamiques peuvent avoir des répercussions significatives sur l'efficacité de la cybersécurité au sein de la BPVF. Il devient crucial de réévaluer les rôles et les responsabilités pour éviter les redondances et garantir une approche cohérente et efficace en matière de sécurité. Cette réflexion pourrait également mener à des décisions stratégiques telles que le recrutement de spécialistes supplémentaires ou la redéfinition des missions pour clarifier les attributions et optimiser la collaboration entre les différents acteurs.

4.2.2.5 Les principaux points clés émergeant du schème commun de la BPVF

Nous avons assigné à chacun des huit entretiens réalisés au sein de la BPVF un schème

spécifique. Nous avons ensuite fusionné ces schèmes pour obtenir un schème commun, offrant une vision globale de la cybersécurité au sein de l'organisation.

Les principales clés et résultats identitaires émergents des schèmes spécifiques et du schème commun sont les suivants :

- Limitation du rôle du RSSI : le RSSI est principalement confiné à des responsabilités de sensibilisation, de gestion des cellules de crise, et de liaison avec les opérateurs informatiques. Cette limitation façonne son identité professionnelle en le positionnant davantage comme un coordinateur généraliste plutôt qu'un expert technique.
- Renforcement recommandé par l'audit interne : le rapport d'audit interne de 2018 recommande l'embauche d'un second RSSI pour renforcer la cybersécurité et assurer une couverture complète des secteurs à temps plein. Cette recommandation reflète une reconnaissance institutionnelle du besoin de renforcer l'identité professionnelle du RSSI en ajoutant une dimension plus technique et spécialisée à son rôle.
- Impact des contraintes budgétaires sur l'identité professionnelle : les contraintes budgétaires limitent l'internalisation de la cybersécurité, influençant l'identité professionnelle des auditeurs internes spécialisés en sécurité informatique et des informaticiens experts en cybersécurité. Ces professionnels se voient souvent contraints de se percevoir comme des acteurs ayant des compétences techniques sous-utilisées en raison de restrictions budgétaires.
- Influence du manque de compétences techniques : le manque de compétences techniques parmi les auditeurs internes et les responsables de la sécurité des systèmes d'information conduit souvent à l'externalisation de la cybersécurité. Cette situation façonne leur identité professionnelle en les positionnant davantage comme gestionnaires de risques et facilitateurs de processus, plutôt que comme praticiens techniques de la cybersécurité.

4.2.3 Le schème commun aux entretiens réalisés dans les banques libanaises

Pour présenter le schème commun, nous nous sommes fondés sur les trente-deux schèmes spécifiques réalisés à travers les entretiens sur les huit banques libanaises à l'ordre de quatre entretien par banque. Nous rappelons le recours à la méthode de codage de Dubar et Demazière (1997) qui fait ressortir les points saillants des identités professionnelles des auditeurs internes et des RSSI à travers leurs récits qui expliquent comment se construit ces schèmes spécifiques.

Nous soulignons l'exceptionnalité du terrain bancaire libanais qui est conflictuel et en crise économique et monétaire ainsi que l'interactions avec les acteurs durant les entretiens réalisés.

4.2.3.1 L'adaptation de la méthodologie de Dubar et Demazière en réponse à la crise du secteur bancaire libanais : une approche pour l'application du schème spécifique

Le terrain bancaire libanais libéral, dans le contexte actuel, est un terrain conflictuel en crise monétaire et économique. La gestion de la cybersécurité diffère d'une banque à une autre pour diverses raisons comme l'autonomie des banques, la diversité organisationnelle, la taille et de la complexité, l'environnement réglementaire, la perception des risques et des menaces, ainsi que de la culture organisationnelle et du leadership. Durant nos entretiens, nous avons remarqué cette diversification au niveau organisationnelle. La situation de crise économique, financière et monétaire qui a touché le secteur bancaire libanais a nécessité une adaptation de la méthodologie de Dubar et Demazière en ce qui concerne l'application du schème spécifique.

Nous résumons ces trente-deux entretiens en un schème spécifique sans pouvoir ressortir les points saillants des identités professionnelles des acteurs concernés. Nous n'avons pas pu repérer ces identités professionnelles pour plusieurs raisons.

4.2.3.2 L'absence de repérage des identités professionnelles des auditeurs internes et des RSSI

Dans un contexte de crise financière, les participants préoccupés par leur réputation et leur statut professionnel ont préféré réciter des réponses pré-apprises pour éviter de compromettre leur image ou leur position au sein du secteur bancaire en crise. Certains participants étaient soucieux de représenter leur banque de manière cohérente et professionnelle, ce qui les a amenés à adopter un discours standardisé plutôt que de mettre en avant leur identité professionnelle individuelle. Concernant la cybersécurité, les discussions se sont concentrées sur les concepts, les meilleures pratiques et les défis généraux plutôt que sur les rôles professionnels spécifiques. Nous citons d'autres raisons supplémentaires qui pourraient expliquer cette absence de repérage des identités professionnelles dans les entretiens comme le manque de formalisation des rôles et des compétences des auditeurs internes et RSSI qui ne sont pas clairement définis. Nous avons remarqué également que les auditeurs internes ont des responsabilités multiples et polyvalentes, ils se concentrent davantage sur des tâches générales plutôt que sur des rôles professionnels spécifiques. Il est important de comprendre ces facteurs contextuels et organisationnels spécifiques pour expliquer pourquoi l'identité professionnelle est absente dans le secteur bancaire libanais. Dans un tel contexte, la construction d'une identité

professionnelle liée à un sujet aussi particulier que la cybersécurité est entravée.

4.2.3.3 La synthèse du schème commun regroupant les trente-deux entretiens

Nous adaptons ici la synthèse du schème commun des banques libanaises au modèle du schème spécifique de la BPVF en identifiant ces similarités. Nous notons l'existence de deux mondes socioprofessionnels distincts au sein des banques libanaises, différenciés par la présence ou l'absence d'expertise technique interne. Le premier groupe, qualifié de « PAREIL », est caractérisé par un manque d'expertise technique parmi les auditeurs internes, ce qui conduit à la simplification ou à l'externalisation de certaines responsabilités en matière de cybersécurité. Le second groupe, qualifié de « PAS PAREILS », dispose d'une expertise technique présente en externe. Il est également observé que la cybersécurité ne revêt pas une importance primordiale dans le secteur bancaire libanais.

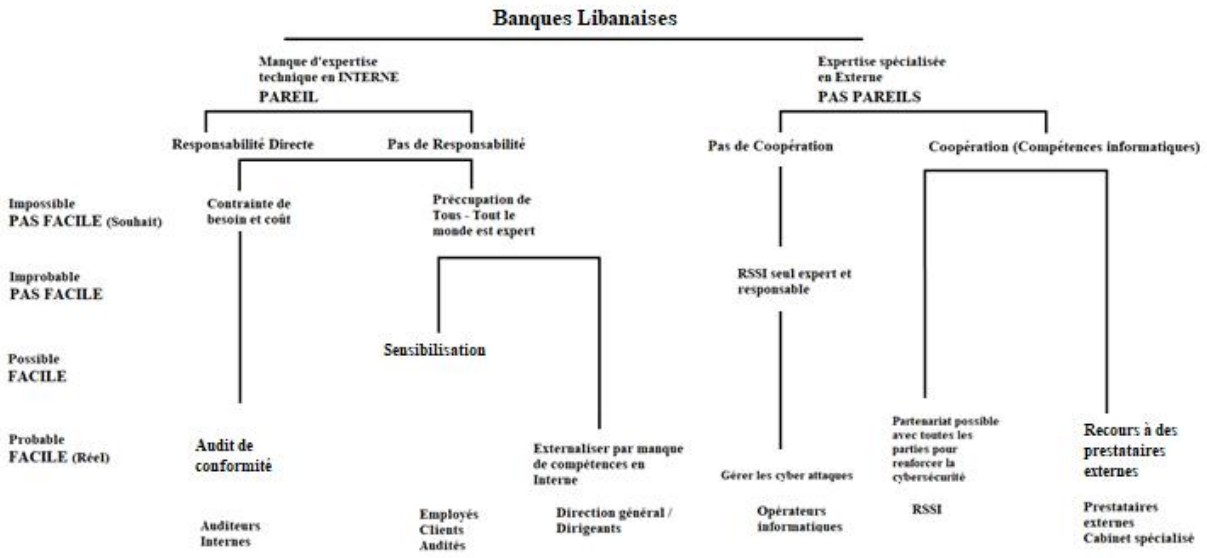


Figure 17 : le schème commun regroupant les trente-deux entretiens sur le secteur bancaire libanais

Source : élaboration personnelle

4.2.3.4 Les points clés émergeant du schème commun des banques libanaises

L'analyse du schème commun aux banques libanaises révèle les points suivants :

- Les départements informatiques et les RSSI sont chargés de garantir la cybersécurité dans les banques libanaises, étant les seuls responsables de la mise en place des mesures de sécurité et de la protection des systèmes informatiques contre les cyberattaques.
- L'audit interne agit en tant que troisième ligne de défense, visant à s'assurer que les RSSI remplissent correctement leurs responsabilités en matière de cybersécurité.
- Les auditeurs internes reconnaissent leur manque de connaissances en cybersécurité,

ce qui peut limiter leur capacité à évaluer efficacement les mesures de sécurité mises en place et à identifier les risques potentiels.

- La cybersécurité ne semble pas être une priorité majeure dans le secteur bancaire libanais, probablement en raison de la crise économique et financière qui a conduit à une focalisation accrue sur d'autres enjeux financiers.

La construction identitaire en rapport à la cybersécurité montre une différence fondamentale avec le cas français de la BPVF : l'enjeu accordé à la cybersécurité étant faible, l'audit interne s'en détourne presque, laissant la gestion de ce risque entièrement au domaine du RSSI.

Conclusion intermédiaire

Cette partie 4.2 de notre thèse nous a permis de plonger dans l'univers complexe de la cybersécurité au sein de la BPVF, en explorant les identités professionnelles des acteurs clés tels que les auditeurs internes et les RSSI. À travers une approche méthodique basée sur les schèmes spécifiques issus d'entretiens approfondis, nous avons mis en lumière des facettes cruciales de la manière dont ces professionnels perçoivent et interagissent avec la cybersécurité au sein de leur organisation.

Une des conclusions majeures de cette analyse réside dans la différenciation des acteurs en cybersécurité, entre ceux qui possèdent des compétences techniques spécifiques (PAS PAREILS) et ceux qui en manquent (PAREIL). Cette distinction souligne l'importance vitale des compétences techniques en cybersécurité et suggère que le manque de ces compétences peut entraîner des défis importants. Le rôle central du RSSI dans cet écosystème complexe a été mis en évidence. Il se situe dans une position intermédiaire, avec des responsabilités directes et indirectes en matière de cybersécurité. Sa perception de lui-même et de son rôle, ainsi que la manière dont il est perçu par les autres acteurs, définissent son identité professionnelle. Le RSSI aspire à collaborer étroitement avec d'autres professionnels pour garantir la sécurité de l'organisation, en reconnaissant ses propres limites en termes de compétences techniques.

Dans le contexte de l'organisation, nous avons constaté que l'identité professionnelle des acteurs est profondément influencée par la structure et la culture de la BPVF. La division entre ceux qui ont des compétences techniques internes et ceux qui externalisent cette expertise a des répercussions sur la manière dont la cybersécurité est gérée. Les contraintes budgétaires et la crise économique ont également un impact sur les décisions organisationnelles en matière de cybersécurité.

Synthèse du chapitre 4 : analyse des résultats et réflexions sur les identités professionnelles en cybersécurité

Le chapitre 4 de notre thèse met en lumière les résultats de nos recherches sur la cybersécurité au sein de la BPVF, en se focalisant sur les identités professionnelles des acteurs clés, notamment les auditeurs internes et les RSSI. Ce chapitre est structuré en deux parties : la première (4.1) se concentre sur la revue de la littérature et les méthodes utilisées, tandis que la seconde (4.2) présente les résultats des entretiens et de notre analyse.

Nos investigations ont révélé plusieurs points essentiels. Premièrement, nous avons souligné l'importance cruciale des compétences techniques en cybersécurité dans le contexte de la BPVF. La distinction entre les acteurs « PAREIL » et « PAS PAREIL » met en lumière les défis auxquels sont confrontés les professionnels manquant de ces compétences, ce qui souligne la nécessité de développer et de renforcer les compétences techniques au sein de l'organisation.

L'analyse des identités professionnelles des auditeurs internes et des RSSI a permis de mettre en évidence les tensions potentielles dans la gestion de la cybersécurité. Les auditeurs internes, en tant que troisième ligne de défense, jouent un rôle de contrôle et de surveillance, mais peuvent se heurter à des divergences d'opinion avec les RSSI concernant les responsabilités et les approches. Les RSSI, malgré leurs compétences techniques limitées, occupent une position centrale en cybersécurité et démontrent un fort désir de collaboration avec d'autres parties prenantes, illustrant ainsi l'importance d'une approche collective pour garantir la sécurité organisationnelle.

Notre analyse organisationnelle a également mis en lumière l'influence significative de la structure et de la culture de la BPVF sur les identités professionnelles des acteurs. Les contraintes budgétaires et la crise économique ont conduit à des choix organisationnels, comme l'externalisation de certaines responsabilités liées à la cybersécurité.

CHAPITRE 5.

Résultats de la recherche (2) : L'IDENTITÉ AFFECTE LA GESTION DU RISQUE CYBER

Sommaire du chapitre 5. L'identité affecte la gestion du risque cyber

5. L'identité affecte la gestion du risque cyber

Ce chapitre se répartit en quatre parties. La présentation des résultats de recherche s'établit selon trois approches : une approche positive de l'identité (traits saillants), une approche relative inspirée du travail de Dubar et une approche juridictionnelle (Abbott).

La première partie consiste à analyser les identités et les relations entre les professions en charge de la cybersécurité dans la BPVF en France et les banques libanaises. La deuxième partie consiste à examiner plus en détail les identités des auditeurs internes et des RSSI. La troisième partie explore l'impact des identités professionnelles à l'égard des professions d'audit interne et RSSI au niveau juridictionnel dans la gestion de la cybersécurité. La dernière partie présente la synthèse des résultats de recherche sur le terrain bancaire français et libanais ainsi que la base des points communs.

Tableau 14 : la présentation des résultats selon trois approches

<table>
<tr><th>Description</th><th>Partie A</th><th>Partie B</th><th>Partie C</th></tr>
<tr><td rowspan="2">Section 1 & Section 2</td><td>Traits saillants des identités professionnelles</td><td>Le regard réflexif des acteurs quant à leur capacité de répondre à des attaques.</td><td rowspan="3">Synthèse des résultats de terrain</td></tr>
<tr><td>Approche relative</td><td>Le regard externe (pour Autrui) sur cette capacité de répondre aux attaques.</td></tr>
<tr><td>Section 3</td><td>Approche juridictionnelle</td><td>Le positionnement des professions dans les rôles à jouer face à une attaque.</td></tr>
</table>

5.1 Les identités et les relations entre les professions : approche positive ou fonctionnelle

Nous appréhendons les identités et les relations entre les fonctions au sein de la BPVF selon trois approches. La première consiste à analyser d'une manière générale les identités des fonctions des banques populaires et caisses d'épargne en France en charge de la cybersécurité. La deuxième approche consiste à examiner plus en détail les identités des auditeurs internes et des RSSI. La troisième approche vient compléter la deuxième en soulignant l'impact des nouvelles exigences du groupe BPCE à l'égard des professions d'audit interne et RSSI.

5.1.1 Les fonctions et les relations traditionnelles au sein de la BPVF

Pour rappel, la BPVF structure son organisation de lutte contre le risque cyber à travers :

- La direction de la Sécurité des Systèmes d'Information, en charge de veiller à la sécurité des systèmes informatiques de la banque en étroite collaboration avec le service informatique pour s'assurer que les systèmes de la banque sont à jour, sécurisés et résistants aux attaques ;
- La direction de la Gestion des Risques Informatiques, en charge de l'identification et de la gestion des risques de sécurité informatique en coopération avec le service de la sécurité des systèmes d'information pour s'assurer que les risques sont identifiés et gérés de manière proactive ;
- Le service Gestion des Identités et des Accès, responsable de la gestion des identités et des droits d'accès aux systèmes informatiques de la banque ;
- Le service de gestion des incidents de sécurité, en charge de gérer les incidents de sécurité informatique tels que les attaques de virus ou de phishing ;
- La direction de la conformité, en charge du contrôle du respect des normes de sécurité et de la conformité réglementaire du point de vue de la sécurité informatique.

En collaborant, ces différentes fonctions sont censées être en mesure d'assurer à la BPVF un système d'information sécurisé et résistant aux attaques qui garantit la sécurité des données et la protection des clients de la banque (BPVF, 2023).

L'audit interne n'intervient pas directement dans la gestion de la cybersécurité. Les auditeurs internes agissent en troisième niveau de défense et sont responsables de l'évaluation de l'efficacité des processus, des contrôles et des procédures de la banque. Ils effectuent des audits

réguliers pour s'assurer que les processus sont bien conformes aux règles et normes établies, y compris en matière de sécurité informatique.

5.1.2 La gestion de la cybersécurité à la BPVF : un enchaînement de processus géré par des professions multiples et complémentaires

Nous avons mené huit entretiens relatifs aux postes de directrice générale, directeur d'audit, directeur d'audit de l'informatique Banque Populaire I-BP, superviseur d'audit interne, chef de mission d'audit interne, responsable informatique, responsable de la sécurité des systèmes d'information et directeur des risques et de conformité. Pour l'audit interne, nous avons échangé avec le directeur d'audit de la BPVF, le directeur d'audit d'i-BP, et avec un chef de mission d'audit interne et un superviseur d'audit interne rattaché au chef de mission. Notre sélection du chef de mission et du superviseur n'était pas aléatoire, mais porté sur deux personnes (Monsieur T.L et Mme A.S) qui ont mené un audit de cybersécurité en 2018 sur le département informatique. En totalité, nous avons réalisé les entretiens conformément au guide d'entretien fournis en annexe. Monsieur D. G est le responsable de la sécurité des systèmes d'information (RSSI) de la BPVF en charge la sécurité des systèmes d'information et la protection des données et des informations contre les cyberattaques. Il est le seul à mettre en œuvre et définir la politique de sécurité des systèmes d'information tout en surveillant de manière constante la sécurité informatique de la banque. Un comité de sécurité informatique est responsable de la supervision des activités de sécurité informatique de la BPVF. Il s'assure que les risques de sécurité ont été correctement identifiés et gérés. Il se compose du DSI comme président et des membres de la direction, du RSSI, de l'équipe de sécurité informatique et de l'auditeur interne. Il convient de souligner l'importance du rôle transversal que peux jouer l'audit interne pour renforcer la cybersécurité dans la BPVF.

Ci-dessous un graphique synthétise la démarche d'assurance contre le risque cyber sous un angle hiérarchique.

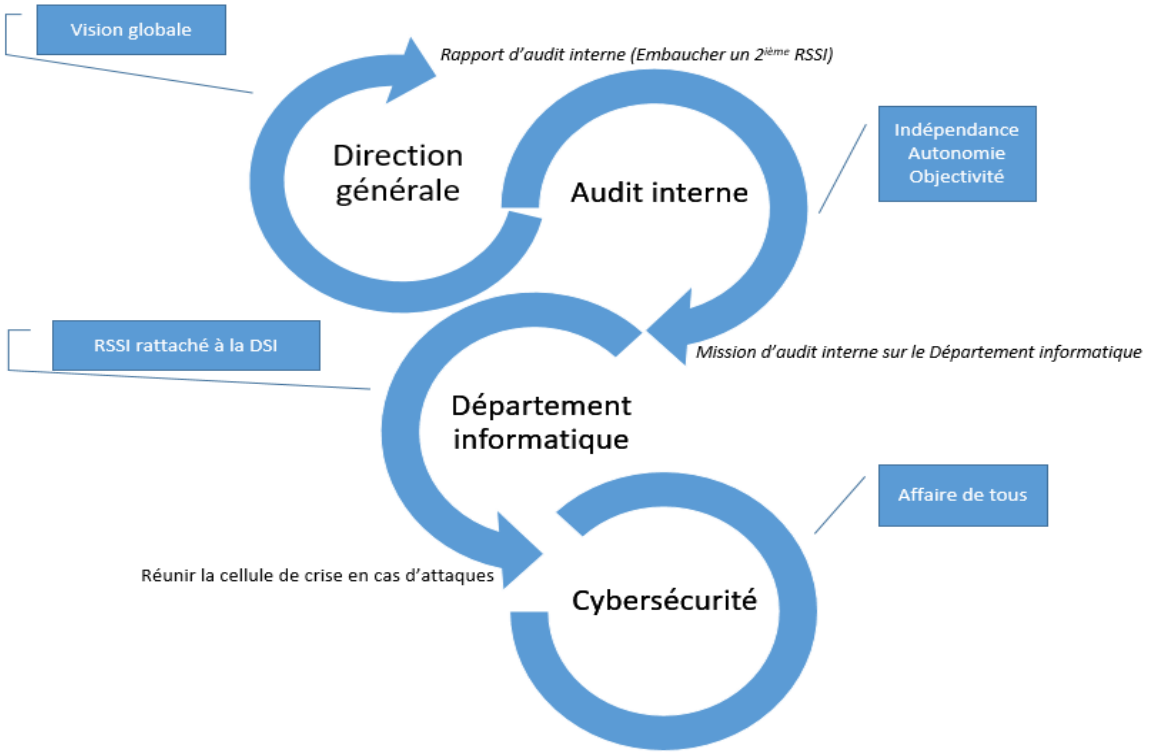


Figure 18 : la démarche hiérarchique de l'assurance de la cybersécurité au sein de la BPVF

Source : élaboration personnelle

Durant les missions d'audit, nous avons remarqué que les auditeurs internes et le RSSI échangent pour évaluer les risques de sécurité informatique, mettre en place des mesures de sécurité et des plans d'urgence en cas d'incident. Dans des cas où les auditeurs internes n'avaient pas de compétences techniques spécialisés, ils se sont fondés sur les rapports du RSSI pour évaluer la sécurité informatique de la banque. Au niveau organisationnel, les auditeurs internes ont proposé l'embauche d'un second RSSI et des procédures complémentaires pour renforcer les processus de sécurité. L'audit réalisé en 2018 n'était pas un audit technique spécialisé en cybersécurité mais portait plus largement sur le domaine informatique. Par manque de compétence technique en cybersécurité, la BPVF envisage de faire appel à des prestataires externes spécialisés, comme le cabinet ITEKIA pour effectuer un audit cybersécurité sur le département informatique. Les auditeurs internes ont par ailleurs recommandé des améliorations en matière de sécurité informatique. Ils ont suivi la mise en œuvre de ces recommandations en coordination avec le RSSI, Monsieur D.G, qui évoque toujours la nécessité d'investir dans la sécurité informatique. Les auditeurs internes et le RSSI participent aussi à un Comité de sécurité informatique pour échanger leur expertise et contribuer à la définition des politiques de sécurité informatique de la banque.

En cas de crise, le RSSI réunit la cellule de crise avec tous les métiers. Il assure l'interface entre

ces métiers et les opérateurs informatiques. Selon une procédure bien définie, il suit les instructions des opérateurs informatiques sur la façon d'agir sur une incidence spécifique en cas de protocole de gestion de crise. Il existe aussi un protocole de gestion de crise au niveau des opérateurs informatiques qui lorsqu'ils sont avertis d'une cyber-attaque importante. Ces opérateurs réunissent les RSSI des établissements rattachés à ces attaques. En cas de crise, c'est le rôle du RSSI de réunir sa propre cellule de crise à l'échelle de l'établissement. Plus précisément, le RSSI se décrit comme gérant l'organisation de la crise au sein de la BPVF en plusieurs étapes :

- Identifier la crise. Il est informé et commence à coordonner la réponse à la crise en fonction des protocoles établis à l'avance dès lors qu'un incident de cybersécurité est identifié.
- Analyser la situation. Il évalue l'ampleur de l'incident et identifie les systèmes et les données qui pourraient être affectés. Il coordonne avec d'autres membres de la cellule de crise pour identifier les sources de l'attaque, les failles de sécurité qui ont été exploitées et les mesures à prendre pour limiter les dégâts.
- Mettre en place des mesures d'urgence. Il met en place les mesures d'urgence nécessaires pour limiter l'impact de l'incident en coordination avec les membres de la cellule de crise. Il peut désactiver certains systèmes, mettre en place un pare-feu ou limiter l'accès aux données.
- Coordonner la réponse à la crise. Il échange avec les membres de la cellule de crise pour coordonner la réponse à la crise. Dans des cas complexes, le RSSI peut avoir recours à des services agréés de sécurité informatique spécialisé, des autorités réglementaires ou des organismes d'application de la loi.
- Communiquer avec la direction. Il informe la direction générale de l'incident et de la réponse à la crise en fournissant des rapports réguliers sur l'état de la situation et en proposant des recommandations et des mesures pour éviter de futurs incidents.
- Évaluation de la réponse à la crise. Le RSSI et les membres de la cellule de crise évaluent la réponse à la crise et identifient les actions à prendre pour améliorer les procédures de sécurité informatique de la banque après la fin de la crise.

Il convient à présent de comprendre comment les identités positives, dont l'opérateur principal est la compétence, sont à l'origine de l'enchainement de ces processus.

5.1.3 Vers une complémentarité née de la divergence des identités des auditeurs internes et des RSSI

Les rôles des auditeurs internes et des RSSI sont perçus, fonctionnellement parlant, comme différents et complémentaires. L'auditeur interne a pour mission d'évaluer les procédures et les processus de la BPVF afin de s'assurer qu'ils sont conformes aux normes et réglementations en vigueur. A l'échelle de la cybersécurité, il est censé également identifier les vulnérabilités de sécurité et les risques associés aux processus et aux systèmes informatique de la banque. Tandis que les RSSI sont plus orientés vers les aspects techniques de la cybersécurité. Ils ont plus une expertise technique fondée sur leurs compétences informatiques. Ils mettent en place des mesures de sécurité appropriées pour protéger les systèmes d'information de la banque contre les cybermenaces tout en évaluant les risques et en mettant en place des solutions de sécurité appropriées pour les atténuer. Le RSSI coopère avec les opérateurs informatiques (équipes techniques) pour s'assurer que les systèmes sont configurés de manière appropriée et que les mises à jour de sécurité sont appliquées de manière régulière. Les auditeurs internes peuvent parfois être perçus comme des policiers, car ils sont chargés d'assurer la conformité aux réglementations et aux normes de sécurité dans un domaine technique. Cependant, leur rôle est également de fournir des recommandations pour améliorer les procédures et les processus de la banque, ce qui peut contribuer à renforcer la sécurité informatique.

Les entretiens réalisés au sein de la BPVF font ressortir les identités des auditeurs internes et des responsables informatiques. Nous présentons dans le tableau ci-dessous les traits saillants de la constitution de l'identité des auditeurs internes et des RSSI que nous avons pu repérer durant nos entretiens.

Tableau 15 : le détail des identités professionnelles des auditeurs internes et des RSSI

Traits saillants de l'identité	Auditeurs Internes	Responsable de la sécurité des systèmes de l'information RSSI
Compétence	Généraliste non technique	Technique et expérience spécialisée
	Création de la valeur ajoutée	Passif – Pas proactif
Regard Extérieur	Traités comme des policiers, gendarmes	Traités comme des Geeks (techniques)
	Compétence managériale	Pas de compétence managériale
	Indépendance	Attachement à la DSI
	Absence de la cellule de crise	Cellule de crise sans action
	Ponctuel, Règlementaire	Indispensable
	Objectivité, contentieux	Subjectivité
Habilitation	Habilitation Signature Rapport d'audit	Pas d'Habilitation Pas de signature
Profil de Poste	Poste diplômé (Certificat en audit interne…)	Poste technique (Certification en sécurité, codage, systèmes…)

5.1.3.1 La compétence comme opérateur central des identités positives

L'auditeur interne doit avoir une solide expertise technique dans le domaine de l'audit, y compris la compréhension des normes d'audit, des pratiques de contrôle interne et des méthodologies d'audit. Sa capacité à analyser et à évaluer les processus et les risques est essentielle pour qu'il mène à bien son travail. Le RSSI doit avoir une solide expertise technique dans le domaine de la sécurité des systèmes d'information. Il doit comprendre les technologies, le codage, les architectures et les protocoles de sécurité, ainsi que les meilleures pratiques en matière de sécurité informatique.

5.1.3.1.1 Généraliste non technique versus technique et expertise spécialisée

Les compétences constituent un élément structurant en cela que les auditeurs internes apparaissent comme des généralistes et les RSSI comme dotés d'une expertise technique. Le tableau suivant en atteste. Les auditeurs internes façonnent leur identité professionnelle autour d'un sentiment de limites et de lacunes. La sous-traitance de ces missions au cabinet externe spécialisé *ITEKIA* les conforte dans ce sentiment, même si le fait d'être donneur d'ordre apporte un élément de compensation (ils deviennent compétents par délégation).

Tableau 16: l'absence des expertises spécialisés en sécurité informatique chez les auditeurs internes

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Compétence		Généraliste non technique	Technique et expertise spécialisée
Profession		**Extraits des Verbatim**	
Chef de mission d'audit interne	Le chef de mission avoue qu'ils font appel à des auditeurs spécialisés en sécurité informatique pour faire des audits sur le département informatique. Ils ne possèdent pas les compétences techniques nécessaires en interne pour le faire.	*« En interne chez nous on n'a pas d'auditeur spécialisé en sécurité du système d'information on n'a pas d'auditeur qui sont spécialisé en informatique et pour voir si le système d'informatique est bien verrouillé il faut une certaine compétence d'informatique on a pas en interne donc on a fait appeler à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. »* *« Comme on est des auditeurs généralistes on a dû faire appel à des cabinets externes donc nous avons travaillé avec des cabinets externes qui ont auditée le système d'information de nos banques. Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT en fait on est des auditeurs généralistes de banque mais pas des auditeurs spécialisés des systèmes information il y a des cabinets. »*	*« Faire des tests d'intrusion pour voir s'ils ont été bien verrouillé parce que nous on n'a pas pu faire en interne, ce sont des compétences techniques spécialisées en sécurité informatique »*
Superviseur d'audit interne	Le superviseur de l'audit avoue qu'il est généraliste et incompétent sur la sécurité informatique. Il avoue que le RSSI doit gérer la cybersécurité parce qu'il est doté de compétences techniques spécialisés.	*« Nous, nous sommes des gens qui sont généralistes et la plupart des temps, on est curieux, on a des méthodes pour apprendre des sujets qu'on ne connaît pas »* *« Je disais tout à l'heure que les auditeurs sont généralistes et on n'a pas de compétence, je vous rappelle qu'il est généraliste »*	*« La nouvelle personne va arriver chez Didier G. pour collaborer avec lui. Car ce qui manquait Didier G. en expertise technique, la clairement c'est pour renforcer ce sujet-là. »* *« Après, en termes d'expertises, on n'a pas l'expertise, on les a laissés à leurs métiers et on a fait en sorte que les gens se comprennent. »*
RSSI	Le RSSI qualifie l'auditeur interne comme non expert dans le domaine de la cybersécurité et généraliste avec de connaissances générales.	*« C'est comme la sécurité est un métier d'expert, les auditeurs internes dans une banque sont généralistes dans les effets bancaires. »* *« Ce sont des gens avec de général connaissances des processus à faire, ce ne sont pas des spécialistes, une bonne connaissance des métiers*	*« C'est comme la sécurité est un métier d'expert... »* *« Je pense que le traitement opérationnel de la sécurité des systèmes d'information doit être au plus près des métiers. Il faut que ce soit très opérationnel par des gens qui ont des expertises et une connaissance de la*

	Le RSSI affirme que la cybersécurité doit être confiée à des profils techniques spécialisés.	*bancaires, et ils ont des attitudes à bien communiquer, ils ont des attitudes à bien analyser, à bien identifier les risques »*	*sécurité des systèmes d'information. »*
Responsable informatique	Le responsable informatique valide que le RSSI et le département informatique sont dotés de compétences informatiques spécialisés.		*« Il faut avoir justement quelques notions des travaux des utilisateurs en langage commun. Donc ça je pense que c'est important. C'est l'une des principales qualités qui sont requises pour le poste de responsable informatique. Et puis être à l'aise aussi des outils parce que ça bouge tout le temps avec l'innovation »* *« RSSI avec de bonnes connaissances en informatique au niveau des banques, je pense que c'est primordial. »* *« Je suis entouré de personnes compétentes »*

5.1.3.1.2 Recul et valeur ajoutée versus leadership en stress

L'audit interne est défini par l'IFACI[8] comme suit : *« l'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance, et en faisant des propositions pour renforcer leur efficacité »* (IFACI, 2017).

Les auditeurs internes ont intégré la valeur ajoutée des missions et la prise de recul comme marqueurs de leur identité.

Selon une étude de Vanson Bourne portant sur 800 RSSI aux États-Unis et au Royaume-Uni, 88 % ont signalé des niveaux de stress modérés à élevés. Ces effets affectent leur vie professionnelle et personnelle (Filippone, 2020). La majorité des cadres RSSI interviewés (90%) par Nominet présentent des niveaux élevés de stress, un tiers signalent des problèmes de santé physique causés par le stress, la moitié signalent des problèmes de santé mentale (Cimpanu, 2020).

Le RSSI, au-delà de son discours, exprime physiquement la nervosité et le stress durant notre entretien. Il se ronge les ongles, émet une transpiration excessive, adopte une voix mal

[8] L'Institut Français de l'Audit et du Contrôle Internes (IFACI) regroupe plus de 5 300 professionnels de l'audit et du contrôle internes et, plus largement, de toutes les fonctions contribuant à la maîtrise des risques. L'IFACI est affilié à The IIA, réseau mondial représentant plus de 185 000 professionnel (https://www.ifaci.com)

assurée… Au niveau de la cybersécurité, il reconnait avoir du mal à communiquer efficacement avec les parties prenantes et à mobiliser les ressources nécessaires pour mettre en œuvre des mesures de sécurité. Il se justifie en expliquant qu'il est souvent seul et sans équipe face aux défis à relever en cybersécurité. Cela peut engendrer un sentiment de frustration et d'inefficacité professionnelle. Le RSSI trouve des difficultés lors de la mise en œuvre des politiques de sécurité, la gestion des risques et la sensibilisation à la sécurité au sein de la BPVF. Sa perception par rapport aux différents acteurs est affectée.

Son identité professionnelle est façonnée par le stress, le manque de compétence en cybersécurité et la crainte de la critique. Il se sent dévalorisé et peu confiant dans son rôle parce qu'il ne parvient pas à exercer un leadership efficace. Il va remettre en question sa compétence et son aptitude à occuper le poste de RSSI, ce qui peut avoir un impact négatif sur sa confiance en lui et sa satisfaction professionnelle.

Ces faiblesses ont été identifié dans le rapport d'audit interne qui recommande l'embauche d'un deuxième RSSI pour accompagner D.G dans son travail afin de couvrir certains champs de compétences qu'il ne possède pas. Le nouveau RSSI disposera de connaissances techniques spécialisés en cybersécurité.

Tableau 17: l'absence des compétences de leadership chez les RSSI

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Compétence		Valeur ajoutée	Passif et non proactif
Profession		**Extraits des Verbatim**	
Chef de mission d'audit interne	Le rapport d'audit interne a qualifié le RSSI proactif dans son travail, et n'a pas les compétences nécessaires pour anticiper les menaces en cybersécurité.	*« Moi c'est plutôt actuellement le fait de présenter nos travons à des directions et de les faire réfléchir sur des améliorations sur le contrôle interne donc c'est pouvoir proposer des rapports avec des recommandations avec* ***la valeur ajoutée*** *pour la banque, c'est ce qui me valorise en gros. »*	*« ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'il ont relevé c'est que justement le RSSI n'est pas suffisamment pro actif, ça serait près des services que tout est bien fait quand tu avais un développement d'implication privative parce que quand tu développes une implication privative il fait prendre en compte la sécurité de système d'information et ça le cabinet externe a trouvé que justement on ne prenais pas suffisamment compte la sécurité du système d'information pour développer des application privatives.»*

Directeur d'audit interne	Le rapport d'audit interne recommande de recruter un deuxième RSSI pour couvrir tous les aspects de la sécurité de la BPVF.	*« Il y a des audités qui ont compris qu'on est là pour valeur ajoutée. »*	*« Il y a vais quelques points de faiblesse mais justement ce rapport d'audit a permis de commencer à améliorer des choses en terme de dispositif du contrôle de recrutement de RSSI, c'est en cours d'amélioration »*

5.1.3.2 La crédibilité comme marqueur de l'identité positive : diplôme versus profilage de poste

Les auditeurs internes se fondent sur leur diplôme et sur les certificats en audit interne (CISO, CIA…) tandis que les RSSI se fondent sur le profilage de leur poste, dont l'aspect technique est attesté par des certifications en sécurité (codage, systèmes informatiques…)

Les titulaires de postes en audit interne que nous avons interviewés ont investi du temps et des efforts dans leur éducation et leur formation ce qui leur a permis d'être qualifiés comme experts dans leur domaine et ce qui peut renforcer leur confiance en eux-mêmes et à perception positive de leur rôle professionnel. En revanche, le RSSI a avoué qu'il ne possède pas des connaissances suffisantes en sécurité informatique. Il est pourtant considéré comme le garant de la sécurité informatique au sein de la BPVF. L'absence d'expertise spécialisée en sécurité peut remettre en question sa crédibilité auprès de ses collègues, de la direction et des employés. Le tableau ci-dessous rend compte de ce défi de crédibilité.

Tableau 18 : le manque d'expertise spécialisée en sécurité informatique chez le RSSI

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Compétence		Diplômé certificat en Audit	Certification en sécurité
Profession		**Extraits des Verbatim**	
Chef de mission d'audit interne	Diplôme DECF en comptabilité et audit externes dans les cabinets d'expertise comptables	*« J'ai fait une école de commerce à paris dans un institut supérieur du commerce. Ensuite, j'ai fait un DECF un diplôme de comptabilité. J'ai commencé à faire ma carrière dans l'audit comptable dans cabinet d'expertise comptable en audit externe et en suite j'ai rejoint la Banque populaire de Bourgain France compte en audit interne. »* *« J'ai fait une école de commerce de comptabilité sur l'entre an audit externe, c'est dans les cabinets d'expertise comptable donc j'ai fait l'audit et je vais voir les entreprises,*	

		mais j'été externe du l'entreprise et du coup j'ai voulez faire de l'audit interne un audit à l'intérieur de l'entreprise, mais c'été la suite logique de l'audit externe »	
Superviseur d'audit interne		*« une formation comptable, je suis expertise comptable en fait. Avant d'être expertise comptable, j'ai réalisé un Bac+4 en comptabilité.»*	
RSSI	Le RSSI ne possède pas un contexte en sécurité informatique. (Pas de diplômes ou certification en sécurité informatique)		*« Le Certificat d'aptitude professionnelle à la profession des banques et un brevet professionnel de banque de trois ans et j'ai fait la première année de l'Institut technique bancaire ITB.* *Mon parcours, ça a été un parcours à la profession bancaire pendant une trentaine d'année. Donc, j'étais responsable du traitement des chèques au moyen de paiement. Ensuite, j'étais responsable de la monnaie c'est-à-dire tout ce qui tourne autour des cartes bancaires. Ensuite, j'étais responsable de l'ensemble des moyens de paiement, les chèques, les virements, les traitements, les cartes bancaires, les moyens de paiement internationaux. Et on m'a fait opposition compte tenu de mes connaissances de production bancaire. On m'a fait la proposition de m'occuper de risques opérationnels. C'est une suite un peu logique. »*
Directeur de l'audit interne de l'i-BP	Certifications d'audit interne international	*« J'ai fait une étude en 3ième cycle en gestion complété ça et puis depuis Euhhhh j'ai fait pas mal de formation continu dans le cadre de mission. En particulier, je suis certifié donc sésame et Sillac, sont deux certifications d'audit interne international. »*	
Directeur de l'audit interne	Expérience en Audit interne dans un des 4 cabinets d'audit	*J'ai 42 ans, j'ai un master en France Européenne management, à l'université « STAFFORDSHIRE ». J'ai commencé comme auditeur financier à PricewaterhouseCoopers. Puis, en 2003, comme auditeur interne dans la caisse d'épargne du Pas-de-Calais.*	
Responsable	Master MIAGE qui		*« J'ai achevé un master Méthodes Informatiques*

informatique	permet d'acquérir une bonne compréhension des systèmes d'information.		*Appliquées à la Gestion des Entreprises (MIAGE) à l'université d'Orsay à Paris. Le but de ce master était de me permettre à réaliser des projets dans les organisations et d'acquérir une bonne compréhension des systèmes d'information. Il m'a donné aussi des connaissances informatiques en analyse, conception et développement ainsi qu'une première approche des structures organisationnelles et des outils du management. »*

5.1.3.3 L'identité pour autrui : émergence de paradoxes structurants

Les traits saillants des auditeurs internes et des RSSI sous le regard d'autrui (*Identités pour Autrui*) relèvent de paradoxes structurants : indépendance versus rattachement à la DSI, objectivité versus indépendance, obligation règlementaire versus action indispensable sur le fond, policiers/gendarmes versus geeks, manque de compétences en systèmes informatique versus expert en sécurité informatique.

5.1.3.3.1 L'indépendance des auditeurs internes constitue une source de confiance pour les interlocuteurs alors que le RSSI est tributaire de son rattachement à la DSI

L'indépendance des auditeurs internes leur permet d'accomplir leur tâche de manière objective et impartiale, c'est du moins l'élément d'identité qu'ils dégagent. L'indépendance est essentielle pour assurer qu'ils peuvent fournir des recommandations et des conseils objectifs pour améliorer la posture de sécurité de la BPVF. Cette indépendance renforce leur crédibilité et l'image d'intégrité professionnelle. Elle leur permet de mener des audits et des enquêtes de manière autonome sans crainte de pressions qui pourraient compromettre l'objectivité de leurs conclusions.

Des guides et recommandations de l'ANSSI constituent des bases méthodologiques pour la BPVF et la BPCE en renforçant leur parc informatique et leur cybersécurité. Ce guide invite à une démarche proactive en matière de cybersécurité en s'assurant que des audits internes indépendants soient réalisés régulièrement. Pour les régulateurs comme l'ANSSI, cette indépendance est qualifiée comme un élément clé pour s'assurer que la BPVF respecte les règlementations et les normes en matière de sécurité des données. Étant une autorité de contrôle compétente en France, l'ANSSI propose des bonnes pratiques de sécurité à suivre comme la sensibilisation régulière du personnel, la revue régulière des droits d'accès, la réalisation

régulière de cartographies de son SI, la mise en place de mécanismes de détection et de surveillance, la journalisation et l'analyse des journaux et la mise à jour automatique des cas de détection de menaces liées aux nouvelles vulnérabilités.

Pour le RSSI, l'indépendance de l'auditeur est perçue comme un gage de professionnalisme et d'objectivité.

Tableau 18 : l'indépendance des auditeurs internes au sein de la BPVF

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Regard Externe		Indépendant	Attachement hiérarchique à la DSI
Profession		**Extraits des Verbatim**	
Directeur d'audit interne de l'i-BP	L'audit interne est indépendant et rattaché direct au DG.	*« Indépendance, honnêteté. Il y a tout un code déontologique qui existe… »* *« Déjà nous sommes rattachés au directeur générale. Nous avons aussi un accès au conseil d'administration pour le cas échéant »*	
Directeur des risques conformité et contrôle permanent	Les auditeurs internes sont indépendants à travers un lien fonctionnel avec l'inspection générale du groupe.	*« Ils sont rattachés directement au directeur générale, et forcement ils sont indépendants. Ils ont rôle, un lien hiérarchique avec le directeur général, et il a un lien fonctionnel avec l'inspection générale du groupe BPCE ».*	
Directeur d'audit interne	Les auditeurs internes doivent conserver leur indépendance de jugement en accédant directement au DG s'ils trouvent des anomalies.	*« Il faut aussi que l'audit soit indépendant, dans son appréciation, qu'on ne puisse pas lui imposer le plan d'audit. Le plan d'audit, c'est la banque qui le fait, mais il faut que l'audit puisse dire : « il y a tel problème dans telle entité, il faut faire une mission ». Enfin, l'audit doit être totalement indépendant dans les conclusions, quitte à ce que la banque prenne la responsabilité de ne pas suivre les recommandations. Il doit conserver son indépendance de jugement et pouvoir accéder directement au directeur général s'il a quelque chose à dire. Et au président du comité d'audit. »* *« L'audit doit être totalement indépendant dans les conclusions, quitte à ce que la*	

		banque prenne la responsabilité de ne pas suivre les recommandations. Il doit conserver son indépendance de jugement et pouvoir accéder directement au directeur général s'il a quelque chose à dire. » *« Ce n'est pas le rôle de l'audit. L'audit n'a pas une vocation à être actif. C'est-à-dire nous nous sommes une fonction de contrôle et c'est légal parce que si on était à la fois responsable de la mise en œuvre des auditeurs, on aura une confusion des genres et on s'est jugé partie. »*	
Chef de mission d'audit interne	L'auditeur est professionnel et indépendant. Il vérifie si les normes sont bien appliquées au sein de l'organisation.	*« Il doit avoir un principe d'indépendance c'est-à-dire nous on est là pour vérifier donc on doit être indépendant des personnes comme audit parce qu'on doit surveiller si les normes sont bien appliqués donc il ne faut pas de collision entre guillemet il faut qu'on soient disponible, professionnelle, à l'écoute il faut qu'on vaille pas trop parce qu'on vient déranger les gens dans le travail donc il faut prendre en compte les impératives des autres employées donc il y a tout un aspe de professionnalisme mais à la fois d'empathie et d'indépendance c'est tout ça pour moi l'auditeur. »*	
Responsable informatique	L'auditeur est indépendant dans ses jugements alors que le RSSI est rattaché à la centrale informatique.	*« En étant détaché, en étant pas jugé partie, c'est comme ça que l'auditeur peut garder sa crédibilité et donner des recommandations pour l'amélioration continu. »*	*« On communiquait s'il y a des incidents ou des attaques par le RSSI qui a été informé par la centrale informatique »*

Les prestataires externes valorisent l'indépendance des auditeurs internes dans leur mission en cybersécurité. Cette indépendance façonne leur identité professionnelle en renforçant leur confiance et leur crédibilité. L'indépendance demeure une exigence cruciale qui permet d'instaurer la confiance des actionnaires et des partenaires stratégiques dans la protection des états financiers ce qui constituent des supports incontournables pour l'évaluation de la performance de la BPVF et pour la prise de décisions futures spécialement en matière de cybersécurité.

Rattaché à la DSI, les RSSI sont perçus pour autrui comme des experts en sécurité informatique et des acteurs-clés pour garantir la protection des systèmes et des données de la BPVF. Leur rôle stratégique transversal est essentiel pour assurer la confiance et la sécurité dans un

environnement numérique en constante évolution. Néanmoins, nous avons repéré quelques points négatifs associés au rattachement du RSSI à la Direction des Systèmes d'Information :

- Conflits d'intérêts. La DSI est responsable de la mise en place et de la gestion des systèmes d'information, tandis que le rôle du RSSI est de garantir la sécurité et la protection de ces systèmes. Les objectifs de performance technologique de la DSI entrent en conflit avec les exigences de sécurité du RSSI, ce qui peut compromettre son indépendance et sa capacité à prendre des décisions impartiales.
- Hiérarchie et autorité. Le RSSI est perçu comme un membre de l'équipe informatique plutôt que comme un responsable de la sécurité indépendant. Cela limite son autorité et sa capacité à influencer les décisions stratégiques relatives à la sécurité de l'information au sein de l'entreprise.
- Perception externe. Ce rattachement du RSSI à la DSI est perçu de manière négative par les parties prenantes externes, telles que les clients et les régulateurs. Certains considèrent que cela compromet l'indépendance du RSSI et remet en question sa capacité à évaluer objectivement la sécurité de l'organisation.
- Limitation de la vision globale. Le RSSI peut être plus étroitement aligné sur les aspects techniques de la sécurité informatique, ce qui limite sa vision globale de la sécurité de la BPVF. Il est moins impliqué dans les discussions stratégiques et les décisions organisationnelles liées à la gestion des risques, à la conformité réglementaire et aux aspects humains de la sécurité ce qui entraîne des lacunes dans la mise en œuvre de mesures de sécurité globales et une concentration excessive sur les aspects techniques.

Ce rattachement rend essentielle la collaboration interprofessionnelle. Une communication et une collaboration efficaces entre le RSSI, la direction et les autres départements aident à surmonter les conflits d'intérêts et à renforcer l'indépendance du RSSI.

5.1.3.3.2 L’objectivité renforce l’identité professionnelle des auditeurs internes dans le sens d’une expertise fiable et impartiale, alors que le RSSI appuie son expertise sur une expérience singulière.

Les auditeurs internes renforcent leur crédibilité et leur professionnalisme en adoptant une approche objective. A l’inverse, les RSSI ont développé une expérience singulière de la sécurité informatique, et leur jugement en devient hautement subjectif. Le RSSI qui a réussi à résoudre des problèmes de sécurité complexes ou à faire face à des incidents va se sentir et sera perçu

plus compétent et valorisé dans son rôle. Son identité professionnelle en tant que leader en cybersécurité est alors renforcée.

Les conséquences organisationnelles de ce positionnement identitaire se mesurent au quotidien. Le RSSI de la BPVF, D.G. reste fermé à adopter de nouvelles méthodes ou à remettre en questions ses propres convictions au niveau de la gestion de la cybersécurité. Son attitude limite sa capacité à s'adapter aux évolutions rapides de la cybersécurité. Cela rejaillit sur son identité professionnelle, perçue comme moins ouverte à l'innovation et à la collaboration.

La tension entre l'objectivité méthodologique de l'auditeur et la subjectivité expérientielle du RSSI peut créer un conflit interprofessionnel., et à trois niveaux :

- L'auditeur interne cherche à évaluer et à améliorer les processus de sécurité tandis que le RSSI résiste au changement et préfère des méthodes plus traditionnelles ;
- Le RSSI est réticent à partager des informations et cela peut entraver le processus d'audit ;
- Les exigences de conformité de l'auditeur télescopent potentiellement l'approche du RSSI qui se veut pragmatique.

Le RSSI doit trouver un équilibre entre sa subjectivité fondée sur son expérience passée et son objectivité professionnelle. Il doit développer une identité professionnelle fondée sur l'apprentissage continu et l'adaptabilité ce qui va lui permettre de relever avec succès les défis de la cybersécurité dans un environnement en constante évolution.

Tableau 20 : une prise de décisions basée sur l'objectivité des auditeurs internes et la subjectivité du RSSI

Traits saillants de l'identité	Description	Auditeurs Internes	RSSI
Regard Externe		Objectivité	Subjectivité lié à l'expérience technique
Profession		**Extraits des Verbatim**	
Superviseur d'audit interne	Les auditeurs internes fournissent des recommandations à travers le rapport d'audit suivant un regard objectif.	*« Objectivité parce que nous sommes attachés au DG. Nous sommes indépendants vis-à-vis de tous les autres services du groupe. Nous avons tout pouvoir entre guillemets, nous avons accès à tous les éléments, les informations. On ne peut pas nous faire de rétention d'informations, et d'autre façon, notre premier client est notre directeur général. »*	*La cybersécurité est un domaine nouveau à la banque.* *Nous avons remarqué que les RSSI, les responsables informatiques et les opérateurs informatiques se basent sur leurs expériences professionnelles plutôt que sur leurs connaissances techniques pour prendre des décisions au niveau de la cybersécurité.* *Chacun a sa propre vision de la cybersécurité. Nous qualifions le RSSI subjectif et ses décisions liés à l'expérience technique.*
Directeur d'audit interne de l'i-BP	Les auditeurs internes se basent sur des preuves pour présenter leur rapport à la DG.	*« Nous sommes très objectives, d'ailleurs tout ce que nous disons nous le basons sur des preuves, et ensuite, sauf dans des cas très exceptionnel ou de malveillance, nous n'attaquons jamais les personnes mais les situations »*	

5.1.4.3.3 Les identités professionnelles mises à mal par la pénurie de ressources : l'expertise réglementaire pour les auditeurs internes, les moyens matériels et humains pour le RSSI

L'audit interne règlementaire est en charge de vérifier et de s'assurer que la BPVF se conforme aux réglementations et aux normes applicables en matière de cybersécurité. En matière de cybersécurité, les auditeurs internes doivent posséder une connaissance approfondie des réglementations et des normes pertinentes à travers une formation spécialisée si nécessaire et un suivi constant des évolutions règlementaires. Leurs identités professionnelles sont liées fortement à leur expertise d'interprétation et d'application des exigences règlementaires spécifiques. Ils sont aussi en charge de vérifier que la BPVF respecte les exigences légales et réglementaires en matière de sécurité des systèmes d'information en réalisant des audits de conformité et en évaluant les politiques et les procédures. Leurs identités professionnelles est étroitement liée à leurs responsabilités de garantir la conformité aux réglementations. Nous avons observé que les auditeurs internes au sein de la BPVF ne possèdent pas ces compétences spécialisées et donc ont recours à des cabinets externes spécialisées.

Le RSSI, D.G s'est déclaré indispensable au niveau de la BPVF pour gérer la cybersécurité. La

nature critique de son rôle entraîne une pression et une responsabilité accrues. La protection contre les cybermenaces est une tâche complexe et en constante évolution, ce qui peut mettre à rude épreuve son identité professionnelle en nécessitant une gestion du stress et de la résilience. En cas d'incident de sécurité ou de faille, sa réputation va être mise en jeu. Même s'il a mis en place des mesures de sécurité adéquates, une attaque réussie est perçue comme un échec professionnel. Son identité professionnelle est affectée en termes de confiance et de perception externe.

Les contraintes budgétaires en cybersécurité limitent les capacités d'action du RSSI et provoquent de la frustration. Le RSSI se retrouve en difficulté d'acquérir les ressources nécessaires telles que des outils de sécurité avancés ou des logiciels en détection des menaces. Les formations de sensibilisation en cybersécurité sont aussi restreintes à cause du manque de budget. Les ressources allouées à la cybersécurité sont limitées, ce qui a entraîné des défis pour le RSSI. Ces contraintes budgétaires et organisationnelles peuvent restreindre la mise en œuvre de mesures de sécurité adéquates, ce qui peut être frustrant pour lui en termes de sentiment d'efficacité et de capacité à relever les défis de manière optimale.

Tableau 19 : l'audit interne est une obligation règlementaire au niveau de la BPVF

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Regard Externe		Règlementaire	Indispensable
Profession		**Extraits des Verbatim**	
Superviseur d'audit interne	L'audit interne est une obligation règlementaire au niveau de l'organisation.	« Pour moi de toute façon, au sens large, l'audit interne est réglementaire. Donc, toutes les banques ont forcément un audit interne.»	
Directeur des risques conformité et contrôle permanent		« C'est une obligation règlementaire. Nous sommes obligés d'avoir une fonction d'audit interne dans toutes les banques. »	
Directeur d'audit interne de l'i-BP	Selon les normes et la législation en France, l'audit interne est un audit légal à travers un code de déontologie.	« Selon les normes et la législation en France, l'audit interne est un audit légal. Quand se faire auditer n'est pas un choix pour les audités. C'est une obligation légale. »	« Je pense que notre banque a mis en place une fonction de RSSI pour gérer les problématiques de sécurité informatique. En conséquence, dans le cas d'absence d'un RSSI, les

		« Il y a tout un code de déontologie qui a été défini par la profession et qui existe au niveau international et qui est en France produit par l'IFACI, » « La règlementation française oblige les banques à avoir un audit interne. »	rôles des différents acteurs peuvent être sensiblement partagés, du fait notamment de l'absence d'une seconde ligne voir troisième ligne de maîtrise formalisée. »
RSSI	La politique de sécurité des systèmes d'information oblige la BPVF à désigner un RSSI assigné à elle.		« Parmi la politique de sécurité des systèmes d'information, chaque établissement doit désigner un responsable de la sécurité des systèmes d'information, un « RSSI ». Et pour la banque populaire « Val de France », c'est moi qui ai été désigné. »
Responsable informatique	Le responsable informatique préconise la nécessité d'avoir un RSSI doté de compétences techniques au sein de la BPVF.		« RSSI avec de bonnes connaissances en informatique au niveau des banques, je pense que c'est primordial. » « Après, il faut qu'il y ait des rôles en banque justement les RSSI, c'est très important, qui sont en banque et qui ont des rôles bien spécifiés pour pouvoir centraliser et prendre connaissances des problématiques qu'on pouvait rencontrer. Donc, s'il y un RSSI au niveau des banques, je pense que c'est primordial. »

5.1.4.3.3 Les auditeurs internes sont perçus comme des gendarmes et le RSSI comme un geek aux compétences limitées à la technique et difficilement contrôlable

Les auditeurs internes sont fréquemment qualifiés de policiers ou de gendarmes. Cette perception assoit une autorité et une forme de crainte à leur endroit. Néanmoins, l'assimilation à des policiers ou des gendarmes engendre également un conflit de rôles pour les auditeurs internes en cybersécurité. Leur rôle principal est de mener des évaluations objectives et de fournir des recommandations pour améliorer la sécurité des systèmes d'information, plutôt que de s'assurer de l'application de la loi. Ce conflit de rôles peut affecter leur identité

professionnelle et leur capacité à maintenir une approche (si possible) neutre et objective lors des audits. Cela entrave la collaboration et la communication entre les groupes professionnels.

Le développement de compétences interpersonnelles solides devient une nécessité pour construire des relations de confiance avec les parties prenantes et maintenir une identité professionnelle assise sur la collaboration et l'échange d'informations.

Le RSSI est perçu comme un « geek technique » difficilement contrôlable malgré son manque de compétences sur des sujets techniques. D.G., lucide à cet égard, peut se percevoir comme un imposteur. Cette perception engendre un sentiment d'insécurité et d'inadéquation professionnelle, remettant en question sa légitimité dans son rôle de responsable de la sécurité de l'information. Ce manque de confiance en soi entrave sa capacité à influencer les décisions stratégiques et à obtenir le soutien nécessaire pour mettre en œuvre des mesures de sécurité appropriées. Son usage du vocabulaire technique est une arme à double-tranchant : d'un côté il se couvre d'une incursion trop en avant de non techniciens dans ses sujets en donnant une impression de maîtrise, de l'autre il peut éveiller les soupçons, comme s'il voulait « noyer le poisson ».

Et pourtant le RSSI souhaite être reconnu pour autre chose que ses compétences techniques, il ressent le besoin de se former et de développer d'autres compétences liées à la gestion de la sécurité de l'information. Cela peut inclure des compétences en gestion des risques, en gouvernance, en communication stratégique, en leadership, etc. Le RSSI devra investir du temps et des efforts supplémentaires pour acquérir ces compétences et façonner une identité professionnelle plus riche.

Tableau 22 : les auditeurs internes font face à des réticences lors de leurs missions d'audit

Traits saillants de l'identité	**Description**	**Auditeurs Internes**	**RSSI**
Regard Externe		Policiers, gendarmes	Geeks (techniques)
Profession (poste)		**Extraits des Verbatim**	**Extraits des Verbatim**
Chef de mission d'audit interne	Les auditeurs internes sont traités comme des gendarmes et des contrôleurs dans la BPVF.	*« L'audit est un rôle de gendarme mais on n'est pas là que pour ça. C'est-à-dire quand on fait partie de l'entreprise puis quand on veut faire avancer une entreprise en proposant des actes d'amélioration mais pas que des gendarmes mais ça dépend des audités. »*	*« Le RSSI est un véritable GEEK quand il s'agit de choisir les derniers gadgets technologiques pour optimiser notre environnement de travail. Il connaît tous les nouveaux appareils et logiciels avant même leur sortie sur le marché ! »*
Directeur de l'audit interne de l'i-BP	Les auditeurs internes font face à des braquages lors de leurs missions d'audit sur les différents départements au sein de la BPVF.	*« On peut avoir des braquages, de même que quand on redonne nos messages, des messages qui ne sont pas de très haut niveau, qui peuvent surmonter à la commission bancaire. Donc il faut être très comment très… savoir extrêmement mesurer nos propos. »* *« Le phénomène de rejet de l'auditeur interne est un phénomène que j'allais dire, qui est un peu naturel à la base, puisque quelque part, on n'a pas tendance à aimer quand quelqu'un évalue votre travail surtout lorsqu'on sait que potentiellement l'audit amènera des recommandations qui diront que les choses ne vont pas. Donc, il y a à la fois donc ce rejet parce que les gens naturellement n'aiment pas trop même voir ce qui font par contre il y a cette compréhension du fait qu'aujourd'hui effectivement l'audit est devenu nécessaire. »*	
RSSI	Dans le département informatique, certains employés craignent les auditeurs internes…	*« Alors ils ne sont pas forcément peur ou intimidés, mais en règle générale, les collaborateurs ont crainte d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre. »* *« Comme vous dites sur les nouveaux collaborateurs qui viennent de prendre un poste dans un domaine qui ne connaissent pas, ils n'aiment pas avoir l'audit sur le dos. »*	*« En tant que RSSI, j'ai un côté GEEK qui me pousse à explorer constamment de nouvelles technologies et à les intégrer dans nos processus pour améliorer notre efficacité opérationnelle. C'est passionnant de voir comment l'innovation peut transformer notre façon de travailler au quotidien. »*

Dans la plupart des organisations, les systèmes d'information et les fonctions d'audit interne sont impliqués dans la sécurité de l'information. La fonction de sécurité informatique a la responsabilité principale de concevoir, de mettre en œuvre et de maintenir un programme de sécurité de l'information rentable. L'audit interne fournit un examen et une analyse indépendants des initiatives de sécurité de l'information de l'organisation. Idéalement, les commentaires fournis par l'audit interne peuvent être utilisés pour améliorer l'efficacité globale de la sécurité des informations de l'organisation. Ces deux fonctions devraient travailler en synergie pour maximiser l'efficacité du programme de sécurité des systèmes d'information d'une organisation (Steinbart et Al, 2012).

Une mauvaise communication entre l'audit interne et la sécurité de l'information peut avoir un impact négatif sur la relation entre ces fonctions. En effet, il existe des preuves considérables que des problèmes de communication qui reflètent des différences de contexte et de connaissances sous-tendent de nombreux désaccords qui se produisent souvent entre les directeurs d'audit et les directeurs informatiques (CFO, 2008).

Les auditeurs internes sont appelés à être diplomates et flexibles dans leur discours pour éviter des braquages et des conflits avec d'autres fonctions lors des missions d'audit interne sur les départements au sein de la BPVF.

5.1.3.4 Mise en perspective des résultats

La synthèse des identités professionnelles des auditeurs internes et des RSSI met en évidence plusieurs facteurs importants comme la compétence, l'absence de crédibilité du RSSI et les regards externes. En termes de perspective, il est essentiel de comprendre ces éléments pour parvenir à une synthèse cohérente.

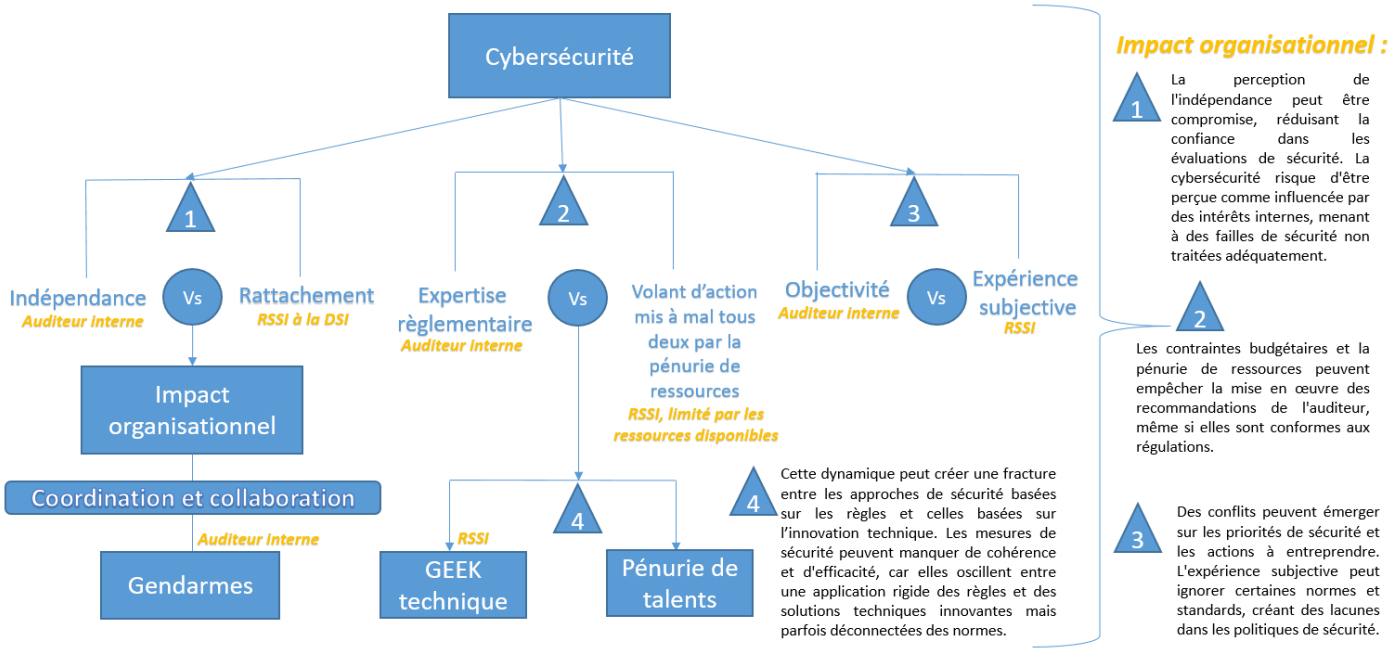


Figure 19 : les tensions organisationnelles entre les auditeurs internes et le RSSI et leurs impact sur la cybersécurité

Source : élaboration personnelle

Nous reviendrons en fin de chapitre sur l'impact organisationnel de ces tensions pour une compréhension approfondie de leur influence sur la résilience de l'organisation face aux cybermenaces. Du point de vue de la compétence, les auditeurs internes ont pour rôle d'évaluer et d'améliorer les processus de sécurité informatique de la BPVF. Ils sous traitent à des cabinets externes spécialisés pour un manque de compétences. Ces cabinets externes possédant des expertises en matière de gouvernance, de conformité et d'efficacité des contrôles de sécurité développeront une légitimité professionnelle dans ce domaine spécifique. En outre, l'absence de crédibilité du RSSI crée un conflit. Il ne parvient pas à adopter de nouvelles méthodes, à être ouvert à l'innovation et à la collaboration ce qui remet en question sa crédibilité professionnelle. Il en résulte des tensions avec les auditeurs qui cherchent à évaluer et à améliorer les pratiques de sécurité. (Directeur de l'audit interne de l'i-BP : *« on peut avoir des braquages, de même que quand on redonne nos messages, des messages qui ne sont pas de très haut niveau, qui peuvent surmonter à la commission bancaire. Donc il faut être très comment très… savoir extrêmement mesurer nos propos. »*)

L'importance des regards externes réside dans le fait qu'ils fournissent une perspective objective et impartiale sur les identités professionnelles des auditeurs internes et des RSSI.

Les points de vue externes, tels que les rapports d'audit indépendant et les évaluations objectives renforcent la crédibilité de l'auditeur interne et influence la perception de la

compétence du RSSI.

5.1.4 Les banques libanaises à la recherche d'une identité professionnelle

Dans le contexte actuel, la cybersécurité n'est pas une priorité pour les banques libanaises, en grande partie en raison de ressources limitées, de priorités concurrentes et d'un manque de sensibilisation aux risques de sécurité informatique. Cependant, le facteur prédominant demeure la crise économique et financière affectant le secteur bancaire libanais.

Cette négligence reflète également l'absence de structures professionnelles clairement définies pour les auditeurs internes et les RSSI dans le domaine de la cybersécurité. Sans intégration de la cybersécurité comme un élément structurant de leurs identités professionnelles, il est difficile de répondre efficacement aux attaques et menaces cyber croissantes. Promouvoir une culture de la cybersécurité au sein de ces rôles clés pourrait non seulement renforcer la résilience des banques contre les cybermenaces, mais aussi solidifier leur rôle stratégique dans la protection des actifs et des données critiques des institutions financières.

Conclusion intermédiaire

Cette partie 5.1 nous a permis de nous pencher sur les identités et les liens entre les banques libanaises en charge de la cybersécurité et la BPVF en France.

Pour mener notre analyse, trois approches différentes ont été utilisées : une approche générale des identités professionnelles, un focus sur les identités des auditeurs internes et des RSSI et une discussion sur les effets des nouvelles exigences du groupe BPCE sur ces métiers. Nous en avons tiré des conclusions sur l'impact de ces identités sur les réponses organisationnelles au problématiques de cybersécurité. Nos recherches montrent que le BPVF met davantage l'accent sur la cybersécurité, les auditeurs internes jouant un rôle essentiel dans l'évaluation des procédures de sécurité. Même si leurs connaissances techniques en cybersécurité peuvent être limitées, les auditeurs internes sont considérés comme les gardiens de la conformité et de l'efficacité des contrôles de sécurité. Les RSSI, en revanche, sont considérés comme des experts techniques en matière de sécurité informatique, mais ils peuvent avoir des difficultés à résoudre des problèmes de leadership et de communication.

L'identité professionnelle des auditeurs internes est largement façonnée par leur indépendance, leur objectivité et leurs connaissances en matière de réglementation.

Cette première partie du chapitre 5 nous a permis de mieux comprendre les rôles des auditeurs

internes et des RSSI dans le cadre du BPVF dans les banques françaises et libanaises en soulignant les difficultés et les possibilités auxquelles ces acteurs sont confrontés ainsi que l'importance de la connaissance, de l'enseignement et de la coopération pour renforcer leur identité professionnelle dans le secteur de la cybersécurité.

5.2 Analyse des identités des auditeurs internes et des responsables informatiques selon une approche relative

Nous complétons ici notre analyse par une approche relative des identités professionnelles pour faire un focus sur les processus sociaux. Nous nous focalisons sur la transaction identitaire avec soi et avec autrui et examinons ses effets sur la perception de l'identité des auditeurs internes et des RSSI.

L'identité n'est pas statique, mais plutôt un processus dynamique et en évolution constante. Nous soulignons que l'identité pour soi et pour autrui est un concept complexe qui nécessite une analyse approfondie des interactions entre les auditeurs internes et les RSSI.

5.2.1 Une analyse des doubles transactions des auditeurs internes et des RSSI

Les récits biographiques réalisés sont riches de processus identitaires à travers les classements et les appartenances, les compétences et les affiliations, les préférences et les évaluations, qui impliquent des négociations informelles avec aussi avec « soi-même ».

Pour mémoire, la double transaction est articulée comme l'identité revendiquée pour soi-même à travers l'expérience biographique, et l'identité que reconnait autrui sur la base des critères et normes de gestion et de fonctionnement.

Il s'est agi d'analyser la forme symbolique des auditeurs internes et de RSSI, c'est-à-dire le langage à travers lequel ils s'expliquent, racontent et argumentent (Dubar et Demazière, 1997).

Le tableau ci-dessous résument le schéma de la double transaction identitaire de Dubar (2015) :

Tableau 23 : l'identité pour soi et pour autrui

Identité pour soi (Subjective) ▼	Identité pour Autrui ►	**Transaction Objective**	
		Par lui-même	Par Autrui
Transaction subjective	Continuité	*Représentation de soi par soi « Moi »*	*Représentation d'un sujet par autrui*
	Rupture	*Définition ou images de soi données à autrui « je »*	*Image d'un sujet données par autrui*

5.2.2 Les auditeurs internes : identité pour soi et pour autrui

L'identité pour soi se réfère à la perception individuelle que chacun a de soi-même, c'est-à-dire comment on se voit et se définit. Les professionnels de l'audit interne se décrivent comme ponctuels, règlementaires, objectifs, indépendants, diplômés et certifiés en audit interne, en apportant de la valeur ajoutée et en étant sérieux et autonomes. Cette identité pour soi est fondée sur la perception de leurs compétences, de leurs qualités et de leur rôle dans l'organisation.

L'identité pour autrui fait référence à la façon dont les autres perçoivent et décrivent une personne ou un groupe. Les auditeurs internes sont perçus comme des policiers ou des gendarmes, des contrôleurs. Cela suggère que leur rôle est souvent associé à celui d'une autorité qui vérifie et contrôle le respect des règles et des procédures au sein de la BPVF. Cette perception peut être influencée par les interactions que les auditeurs internes ont avec d'autres membres de l'organisation, qui peuvent les voir comme des personnes qui cherchent des erreurs ou des non-conformités.

Cette divergence peut être le résultat de la nature même du rôle de l'auditeur interne, qui implique souvent de signaler des problèmes ou des non-conformités, ce qui est souvent perçu comme une intrusion ou une menace par certains membres de la BPVF.

En ce qui concerne spécifiquement la cybersécurité, les auditeurs internes gagnent en légitimité au fur et à mesure que le risque cyber est considéré comme central. Plutôt qu’une limite, ils perçoivent leur caractère généraliste comme les autorisant à traiter de la cybersécurité entre autres sujets. C’est la méthodologie d’audit qui constitue leur spécialité. Ils se considèrent donc aptes à évaluer les risques liés à la cybersécurité, à identifier les lacunes dans les politiques et les procédures de sécurité, et à recommander des mesures d'amélioration pour renforcer la posture de sécurité de la BPVF. L’identité pour autrui des professionnels de l’audit est cependant, assimilée à l’image de gendarme. Cela peut être dû à plusieurs facteurs qui créent de l’ambiguïté. D’un côté, face à des risques très marqués, le rôle d’agent de contrôle strict est légitime. De l’autre, ils demeurent intrusifs.

Tableau 24 : l'identité pour soi et pour Autrui des auditeurs internes

Identité pour soi (Subjective) ▼	Identité pour Autrui ►	**Transaction Objective**	
		Reconnaissance	Non Reconnaissance
Transaction subjective	Continuité	Promotion (Interne) Identité au sein de la BPVF *Ponctuel – Règlementaire – Objectif – Indépendant - Diplômé, certifié en Audit interne*	Blocage (Interne) identité de métier *Policiers – Gendarmes – Contrôleurs intrusifs*
	Rupture	Conversion (Externe) Identité au réseau *Valeur ajoutée – Généraliste non technique (vue d'ensemble)*	Exclusion (Externe) *Sérieux – autonome - sécurité*

Les analyses qui suivent sont tirées d'une interprétation des récits biographiques dont les verbatim ont été présentés dans la section précédente.

5.2.3 Le RSSI : identité pour soi et pour autrui

Le RSSI est un acteur central de la cybersécurité au sein de la BPVF. Il comprend les enjeux et les défis liés à la sécurité des systèmes d'information. En ce qui concerne son identité pour soi du RSSI, il se perçoit généralement comme un expert en cybersécurité, ayant une connaissance approfondie des risques et des meilleures pratiques en matière de sécurité. Il est responsable de la définition et de la mise en œuvre des politiques de sécurité, de la gestion des incidents de sécurité et de la sensibilisation des employés à la cybersécurité. Le RSSI considère son rôle comme indispensable à la protection des actifs numériques de l'organisation et à la prévention des attaques informatiques.

En ce qui concerne l'identité pour autrui du RSSI, il est généralement perçu comme un expert technique hautement qualifié et essentiel à la BPVF. En raison de son expertise et de ses connaissances spécialisées, il est souvent qualifié comme une autorité en matière de cybersécurité au sein de l'organisation. Les autres membres de l'organisation peuvent le percevoir comme un leader en matière de sécurité, responsable de la mise en place de mesures de protection efficaces et de la gestion des incidents de sécurité.

Pour favoriser une identité pour autrui positive, il le RSSI peut chercher à développer des relations de confiance avec les autres membres de l'organisation. Cela peut être réalisé grâce à

une communication claire et transparente sur les enjeux de cybersécurité, en fournissant des conseils et des solutions adaptées, ainsi qu'en démontrant la valeur ajoutée de la sécurité des systèmes d'information pour l'ensemble de l'organisation. L'identité pour soi du RSSI dans le domaine de la cybersécurité se base sur son expertise spécialisée et son contexte informatique, tandis que son identité pour autrui est souvent perçue comme un expert indispensable à la BPVF, chargé de protéger les actifs numériques de l'organisation.

Tableau 20 : l'identité pour soi et pour autrui des RSSI

Identité pour soi (Subjective) ▼	Identité pour Autrui ►	**Transaction Objective**	
		Reconnaissance	Non Reconnaissance
Transaction subjective	Continuité	Promotion (Interne) Identité au sein de la BPVF *Compétences techniques – Expertise spécialisé – Subjectif — contexte informatique*	Blocage (Interne) identité de métier *Geeks – Résolution des problèmes – Vision stratégiques*
	Rupture	Conversion (Externe) Identité au réseau *Passif – Pas proactif*	Exclusion (Externe) *Indispensable à la BPVF*

Une analyse supplémentaire des discours des actants sera d'étudier l'énonciation et la subjectivité dans le langage des auditeurs internes et des RSSI. Ces analyses sont subjectives, complexes et très larges en sociologie. Nous nous limitons à l'analyse réalisé qui est suffisante à notre problématique et à nos résultats de recherche.

Conclusion intermédiaire

Nous avons exploré en profondeur dans cette partie 5.2 les identités professionnelles des auditeurs internes et des RSSI au sein du BPVF en mettant l'accent sur l'identité pour soi et l'identité pour autrui. Nous avons mis en lumière la complexité de ces identités et la manière dont elles peuvent évoluer en fonction des perceptions et des interactions des personnes au sein de l'organisation.

Cette analyse ajoute à la précédente une conception de l'identité comme processus dynamique et en constante évolution plutôt que statique. La perception que les auditeurs internes ont de leur identité en tant que professionnels de l'audit interne, en mettant l'accent sur leurs capacités, leur objectivité et leur contribution à la valeur ajoutée de l'audit interne, a un impact sur la façon

dont ils se perçoivent dans l'organisation. Pour d'autres, qui les perçoivent souvent comme des disciplinaires stricts et policiers, cette identité peut cependant être différente. De la même manière, l'identité des RSSI repose sur leur connaissance de la cybersécurité et leur rôle crucial dans la protection des actifs numériques, tandis que leur identité aux yeux des autres les désignent souvent comme des leaders et des experts techniques dans le domaine de la sécurité informatique.

Nous soulignons dans cette partie la gestion des identités professionnelles des auditeurs internes et des RSSI notamment dans le contexte de la cybersécurité. Il est essentiel que ces professionnels établissent des liens de confiance au sein de l'entreprise afin de promouvoir une identité positive pour les autres. Pour y parvenir, il est nécessaire de communiquer clairement, de proposer les bons conseils et de montrer comment leur expertise ajoute de la valeur. Par ailleurs, il est crucial de reconnaître que la nature de leur position peut parfois donner lieu à des perceptions défavorables, mais qu'ils peuvent modifier ces perceptions en précisant comment ils contribuent à la gouvernance et à la gestion des risques.

L'identité professionnelle des auditeurs internes et des RSSI est en fin de compte liée à leurs connaissances, à leur compréhension de leur rôle et à leurs interactions avec les autres membres de l'organisation. En plus de favoriser une compréhension mutuelle de leur rôle crucial dans la protection des actifs organisationnels et la gestion des risques, une gestion efficace de ces identités peut contribuer à développer la confiance.

5.3 Impact organisationnel des identités professionnelles au regard de la gestion des risques

Nous avons vu dans le 5.1 comment les identités positives pouvaient, en soi, avoir un impact sur l'organisation de la lutte contre le risque cyber. Mais l'opérateur qui permet de passer des identités professionnelles à l'organisation nous semble plus fondamentalement la juridiction. De fait, les juridictions circonscrivent les champs des problématiques organisationnelles qui relèvent d'une profession ou d'une autre. Elles révèlent les possibles conflits de légitimité à traiter d'un sujet, de même que les zones de l'organisation qui peuvent demeurer lacunaires, c'est-à-dire prises en charge par aucune profession en place.

5.3.1 Résultats de recherche : les juridictions cyber à la BPVF

Nous avons observé que la cybersécurité demeure une nécessité technique mais aussi organisationnelle. Le RSSI n'appréhende pas l'importance que peut jouer l'audit interne dans la gestion de la cybersécurité dans la banque sous prétexte que cette fonction n'a pas de compétences technique spécialisé. De surcroît, le RSSI est incapable d'assumer la responsabilité de la gestion de la cybersécurité. Il affirme dans certains cas que ce n'est pas sa responsabilité et qu'il n'a pas les compétences dans ce domaine. Jouissant d'un espace discrétionnaire, il prend des décisions sans rendre compte à personne. Nous présentons les résultats de recherche sous l'angle juridictionnel suite à nos analyses sur le terrain bancaire français que nous renforçons par des verbatim.

5.3.1.1 La profession de RSSI revendique une juridiction

Les RSSI jouent sur leur expertise pour justifier que telle ou telle mission ne les concerne pas. Dans ce que l'on observe, les RSSI définissent les contours de leur juridiction de manière discrétionnaire (parce qu'ils sont les seuls à comprendre le sujet). Normalement, le fait de réclamer une juridiction implique pour celui qui la réclame, qu'il rende des comptes sur l'usage qu'il fait de cette juridiction.

Tableau 26: la profession revendique une juridiction

Observations perçues		Extraits des Verbatim
Profession		**RSSI**
RSSI	*La profession revendique une juridiction. (Opportuniste)*	*« Les qualités de RSSI, nous ne sommes pas des experts en sécurité informatique… la sécurité des systèmes d'informations est piloter au niveau du groupe BPCE en spécifique par des opérateurs informatiques… on a une petite structure qui fait seulement des développements internes. » « C'est moi en tant que RSSI…Chaque établissement doit désigner un responsable de la sécurité des systèmes d'information, un RSSI. Et pour BPVF, c'est moi qui ai été désigné. »*
Responsable informatique		*« Nous en tant que service informatique est très piloté par le groupe et puis par les préconisations du RSSI dans le groupe. Donc moi je n'ai aucun lien avec toute la partie de sécurité du groupe. C'est le RSSI qu'il là. C'est lui qui est responsable de maintenir la cybersécurité en première partie… »*
Directeur d'audit		*« Les responsables de l'audit interne ont la responsabilité supplémentaire d'assurer la conformité globale de l'audit interne avec les Normes et d'en rendre compte mais pas l'interaction en premier niveau sur la cybersécurité. »*

Les RSSI doivent répondre aux exigences réglementaires en matière de cybersécurité et sont responsables de la mise en place de mesures de sécurité adéquates pour protéger les actifs informatiques de l'organisation. Ils sont soumis à des audits internes et externes pour évaluer l'efficacité de leurs efforts de sécurité. Les auditeurs internes jouent un rôle complémentaire en évaluant de manière indépendante l'efficacité des politiques et des procédures de sécurité mises en place par les RSSI en contribuant à assurer la conformité réglementaire. La combinaison de l'expertise technique des RSSI et de la supervision objective de l'audit interne renforce la cybersécurité dans le secteur bancaire.

5.3.1.2 Du conflit à l'éclatement des juridictions : instauration de *no man's lands*

Nous avons remarqué que les conflits entre les auditeurs internes et les RSSI portent sur les attributions des uns et des autres. Ces conflits portent à qui revient le fait de gérer et de recommander sur les questions de cybersécurité. Nos analyses nous ont amenée à un *no man's land* en gestion de cybersécurité à un moment donné, à une déresponsabilisation des parties.

Tableau 27: l'éclatement de la juridiction vers une juridiction plus élargit

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Superviseur d'audit	*L'éclatement de la juridiction : une juridiction plus élargit.*	*« C'est l'affaire de tous, il faut que ce soit une préoccupation de tous. Il faut changer la mentalité, il faut éviter les comportements à risque. Pour moi, c'est une préoccupation de tous, parce qu'on peut tous se faire attaquer... »*
Directeur des risques conformité et contrôle permanent		*« Le RSSI. C'est le responsable de sécurité et système informatique qui est responsable de maintenir la cybersécurité dans notre banque…Oui, c'est seulement son rôle la sécurité de l'information. »*
Responsable informatique		*« C'est le RSSI seul justement…et tous les services également en fait »*
Directeur d'audit interne		*« C'est la responsabilité du service informatique de maintenir la cybersécurité » « c'est Didier qui est responsable en premier d'assurer la cybersécurité »*

La question centrale réside dans la définition précise des juridictions et des compétences respectives des auditeurs internes et des RSSI. Les auditeurs internes sont chargés de l'évaluation objective des politiques, procédures et contrôles de sécurité en place. Ils veillent à ce que les pratiques de cybersécurité soient conformes aux réglementations et aux normes en vigueur, identifiant les lacunes et proposant des recommandations pour les corriger. En revanche, le RSSI est responsable de la gestion quotidienne de la sécurité des systèmes d'information. Son expertise technique lui permet de définir les politiques de sécurité, de mettre en œuvre des mesures de protection et de coordonner la réponse aux incidents de cybersécurité. Le manque de répartition claire des rôles et des responsabilités entre ces deux groupes professionnels entraîne des chevauchements ou des vides en matière de responsabilités, générant des tensions et des situations conflictuelles. Par exemple, l'auditeur interne peut constater que les mesures de sécurité mises en place par le RSSI ne répondent pas aux exigences réglementaires ou aux meilleures pratiques de la cybersécurité, les jugeant insuffisantes et inappropriées. De leur côté, les RSSI peuvent percevoir les auditeurs internes comme manquant de compétences techniques, estimant qu'ils ne comprennent pas suffisamment les enjeux opérationnels de la cybersécurité. Ces perceptions divergentes peuvent conduire à des conflits

sur la légitimité des prises de décisions en matière de cybersécurité. Une situation conflictuelle émerge lorsque les auditeurs internes préconisent l'adoption de nouvelles solutions de sécurité conformes aux dernières normes réglementaires. Cependant, le RSSI, évaluant la faisabilité technique et les implications opérationnelles, considère ces recommandations comme irréalisables ou non prioritaires, créant ainsi un blocage décisionnel.

De plus, cette dynamique conflictuelle peut également conduire à des situations lacunaires. Par exemple, si les auditeurs internes et les RSSI ne parviennent pas à s'accorder sur la mise en place de mesures spécifiques de cybersécurité, certaines responsabilités essentielles peuvent être négligées. Prenons le cas de la surveillance continue des systèmes pour détecter des anomalies. Si le RSSI considère cette tâche comme essentielle mais que les auditeurs internes estiment que les ressources allouées ne sont pas suffisantes pour une surveillance efficace, cette divergence peut mener à une surveillance inadéquate, exposant la banque à des cyberattaques potentielles.

Ainsi, la clarification des rôles et des responsabilités est cruciale pour éviter ces conflits et lacunes. Une collaboration étroite et une communication efficace entre les auditeurs internes et les RSSI sont nécessaires pour assurer une gestion cohérente et robuste de la cybersécurité, renforçant ainsi la résilience du secteur bancaire face aux menaces cybernétiques.

5.3.1.3 L’audit interne comme révélateur de situations lacunaires : émergence éventuelle de nouvelles professions pour assister à la gestion de la cybersécurité

Durant leur mission sur le département informatique, les auditeurs internes ont observé des lacunes dans le système informatique au niveau opérationnel. Le rapport d’audit a recommandé l’embauche d’un second RSSI pour renforcer le service informatique dans l’assurance de la cybersécurité. Dans ce sens, l’ANSSI et la BCE ont proposé de nouveaux postes à intégrer au sein du département informatique pour assister les auditeurs internes et le RSSI à être plus préparer face aux cyberattaques. La création des postes de DPO (Data Protection Officer), RSSI-G (RSSI groupe BPCE qui unit tous les RSSI...) sont mis en œuvre suite à ce rapport d’audit.

Tableau 21 : l'émergence éventuelle de nouvelles professions pour assister à la gestion de la cybersécurité

Observations perçues	**Extraits des Verbatim**	
Profession	**RSSI**	
Superviseur d'audit	*L'éclatement de la juridiction : une juridiction plus élargit.*	*« La cyber sécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue.... »*
Chef de mission d'audit interne		*« Ils ont trouvé que ce n'est pas suffisant… c'est le résultat de l'audit qui a dit attention un demi collaborateur et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevé c'est que justement le RSSI n'est pas suffisamment pro actif… » « Une deuxième personne et ça été une suite à notre mission qu'on a fait l'année dernière. Ils ont pris la décision effectivement »*

Cette recommandation d'embauche d'un second RSSI ainsi que l'émergence de nouvelles professions soulignent la reconnaissance de la nécessité de renforcer les compétences et les ressources en matière de cybersécurité. Elles viennent résoudre le manque d'expertise et de compétences au niveau du RSSI en fournissant un soutien supplémentaire pour faire face aux menaces de plus en plus sophistiquées et à garantir la conformité réglementaire. Du point de vue juridictionnel, ces nouvelles professions vont avoir un impact sur la répartition des responsabilités. Le DPO, par exemple, est chargé de veiller à la protection des données personnelles conformément au règlement général sur la protection des données (RGPD). Son rôle implique des tâches liées à la cybersécurité. Il devient essentiel de définir clairement les limites de son autorité et de collaborer avec le RSSI et les auditeurs internes pour éviter les chevauchements ou les conflits de compétence.

La création des postes de RSSI-G qui regroupent les RSSI de l'ensemble du groupe BPCE indique également une volonté de centraliser la gouvernance de la cybersécurité. Cette approche vise à renforcer la coordination et la collaboration entre les différentes entités bancaires, tout en facilitant le partage des meilleures pratiques et des ressources.

En conclusion, l'émergence de ces nouvelles professions et la proposition de renforcement des équipes de cybersécurité reflètent la reconnaissance croissante de l'importance de la protection des systèmes d'information dans le secteur bancaire. Pour éviter les conflits juridictionnels, il est essentiel de clarifier les responsabilités et de promouvoir la coopération entre les différents

acteurs, tout en veillant à ce que chaque profession ait une compréhension claire de son mandat et des objectifs spécifiques qui lui sont assignés.

5.3.1.4 La juridiction du RSSI et la cybersécurité : l'ombre d'un doute

Nous avons remarqué que les RSSI se ne considèrent finalement pas totalement des experts dans la gestion de la cybersécurité. Ils recourent à des prestataires externes spécialisés pour leur assister parce qu'ils n'ont pas les compétences en interne sur certains sujets cyber. Les experts avec des compétences techniques spécialisés en cybersécurité se heurtent aux juridictions d'autres RSSI.

Tableau 29 : l'identité professionnelle du RSSI et l'ensemble du dispositif organisationnel façonne la juridiction du RSSI

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Superviseur d'audit	*L'identité professionnelle du RSSI et l'ensemble du dispositif organisationnel façonne la juridiction du RSSI*	*« La cyber sécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue.... »*
Chef de mission d'audit interne		*« Ils ont trouvé que ce n'est pas suffisant… c'est le résultat de l'audit qui a dit attention un demi collaborateur et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevé c'est que justement le RSSI n'est pas suffisamment proactif… » « Une deuxième personne et ça été une suite à notre mission qu'on a fait l'année dernière. Ils ont pris la décision effectivement »*

Les RSSI reconnaît ses limites et celles de ses pairs et fait appel à des prestataires externes spécialisés pour obtenir une assistance dans des domaines où il n'a pas les compétences techniques requises. Cette dépendance à l'égard des prestataires externes peut découler de la complexité croissante des menaces et des technologies liées à la cybersécurité. Les experts spécialisés en cybersécurité apportent des connaissances pointues et une expertise technique avancée sur des sujets spécifiques comme le **PENTEST**[9]. Cependant, leur intervention se heurte aux juridictions du RSSI, créant ainsi des tensions et des conflits potentiels.

Le RSSI de la BPVF a engagé une société spécialisée en tests d'intrusion **(PENTEST)** pour évaluer la résilience de l'infrastructure informatique de la BPVF en 2019. Bien que ces experts en cybersécurité apportent des connaissances pointues et une expertise technique avancée, leur intervention peut parfois se heurter aux prérogatives du RSSI. Par exemple, lorsqu'un pentest

[9] C'est un test visant à déployer des attaques ciblées contre un système d'information afin d'évaluer sa résistance aux vulnérabilités. L'expert en tests d'intrusion, également appelé pentester, utilise des méthodes similaires à celles des hackers et des pirates informatiques pour identifier et corriger les failles de sécurité (Cyberjobs, 2021).

révèle des vulnérabilités majeures nécessitant des changements significatifs dans l'organisation des systèmes informatiques, le RSSI pourrait être confronté à des défis internes, tels que des contraintes budgétaires ou des résistances opérationnelles, qui peuvent créer des tensions et des conflits potentiels entre les parties impliquées.

Dans ce contexte, la juridiction des RSSI devient réduite et fragile. Les prestataires externes peuvent gagner en autorité, remettant en question les rôles et les responsabilités des titulaires. Le RSSI doit faire face à des défis pour maintenir une position solide en tant que responsable de la sécurité des systèmes d'information au sein de la BPVF.

L'identité professionnelle du RSSI et l'ensemble du dispositif organisationnel jouent un rôle clé dans la définition de leur juridiction. L'identité professionnelle du RSSI est façonnée par ses compétences, son expérience et son autorité au sein de l'organisation.

Nous soulignons que la juridiction du RSSI est influencée par sa dépendance à l'égard des prestataires externes spécialisés et par les tensions avec d'autres acteurs. La consolidation de l'identité professionnelle du RSSI, le renforcement de ses compétences et la communication proactive au sein de l'organisation sont des éléments clés pour maintenir une juridiction solide et efficace dans le domaine de la cybersécurité.

5.3.1.5 L'externalisation partielle de la fonction de cybersécurité en partie crée une dépendance nouvelle règlementée par l'ANSSI

La banque fait appel à des sous-traitants spécialisés pour traiter des questions cruciales et sensibles telles que la cybersécurité. Le RSSI collabore avec ces cabinets externes en invoquant le manque de compétences techniques nécessaires pour faire face aux cyberattaques. Cette externalisation partielle de la fonction de cybersécurité crée une nouvelle dépendance pour la BPVF. Cependant cette pratique est règlementée par l'ANSSI en France. Les prestataires externes doivent être agréés par l'ANSSI au niveau national.

Tableau 30 : l'externalisation de la fonction de cybersécurité en partie crée une dépendance nouvelle règlementée par l'ANSSI

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Chef de mission d'audit interne	*L'externalisation de la fonction de cybersécurité en partie crée une dépendance nouvelle mais qui est règlementé par l'ANSSI*	*« Après la mission qu'on a fait avec le cabinet « ITEKIA ». « …c'est avec un cabinet on a intervenu pour rédiger le rapport…»*
Directeur des risques conformité et contrôle permanent		*« On n'a pas les gens compétents, et quand on ne les a pas, on fait appel à un cabinet…» « un cabinet pour nous alerter sur le fait des tests d'intrusion, qui sont sur la partie technique, et c'est un constat mais sur la partie technique, pas sur la partie organisation…»*
Superviseur d'audit interne		*« On a envisagé un expert métier, un cabinet spécialisé. Donc, on les a assistés, on a participé avec eux dans leurs missions… » « on a amené ce cabinet. Je pense, je ne peux pas vous dire, je n'ai pas participé au choix du cabinet, ma direction je pense qu'ils ont dû avoir un choix de plusieurs personnes, de plusieurs cabinets. Et voilà, donc, s'il demande de la banque, et aussi par rapport au groupe, c'est-à-dire que ce cabinet-là, nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP… »*

Cette externalisation partielle de la cybersécurité permet d'accéder à une expertise spécialisée et à des ressources supplémentaires qui plus efficaces pour faire face aux menaces croissantes de cybersécurité. De plus, en s'appuyant sur des prestataires externes agréés par l'ANSSI, la BPVF s'assure que les normes de sécurité élevées sont respectées. En revanche, cette dépendance à l'égard des prestataires externes soulève également des questions. La BPVF doit s'assurer de sélectionner des prestataires fiables, dotés de solides compétences et d'une expérience avérée en cybersécurité en mettant en place des mécanismes de suivi et de contrôle pour garantir que ces prestataires externes respectent les exigences de sécurité et fournissent les services attendus. La réglementation de l'ANSSI joue donc un rôle essentiel dans la gestion de cette dépendance. L'externalisation partielle de la fonction de cybersécurité de la BPVF représente une approche réglementée par l'ANSSI pour répondre aux besoins en matière de compétences techniques et de ressources spécialisées. Cependant, il est important de gérer cette dépendance avec prudence en s'assurant de choisir des prestataires externes de confiance et en

mettant en place des mécanismes de suivi et de contrôle adéquats pour maintenir un niveau de sécurité optimal.

En conclusion, malgré l'externalisation partielle, la BPVF conserve la responsabilité ultime de la sécurité de ses systèmes d'information. Elle doit s'assurer que les contrats avec les prestataires externes incluent des dispositions appropriées en termes de confidentialité, de gestion des risques et de conformité réglementaire.

5.3.1.6 La juridiction de la profession de cybersécurité devient centrale dans le dispositif de cybersécurité

La gestion de la cybersécurité révèle des conflits entre les différentes fonctions. En l'état actuel – du moins au moment de la recherche, elle suscite des questions structurantes, liées à l'expansion ou à l'éclatement du périmètre de responsabilité. Les compétences requises ne se limitent plus à des fonctions d'experts stricts, mais nécessitent également des compétences de gestion.

Tableau 22 : la juridiction de la profession de cybersécurité doit être centrale dans l'organisation au niveau du dispositif de cybersécurité

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Chef de mission d'audit interne	*La juridiction de la profession de cybersécurité doit être centrale dans l'organisation au niveau du dispositif de cybersécurité.*	*« il doit avoir de bonnes capacités de communication et de présentation…»*
Directeur des risques conformité et contrôle permanent		*« Le RSSI doit exercer une influence directe sur le service d'informatique…Il doit jouer le rôle de leader…capable de diriger une équipe et de motiver les employés.»*
Directeur d'audit interne		*«Comme je vous l'ai dit, il y a une nouvelle personne qui est venu qui a des compétences techniques en plus… le RSSI doit être plus opérationnel et plus relationnel pour savoir exprimer son besoin auprès des dirigeants… »*

La nouvelle gestion de la cybersécurité est en train de reconfigurer la profession en introduisant de nouvelles perspectives et en élargissant les responsabilités. Le RSSI doit non seulement

posséder une expertise technique approfondie, mais également avoir des compétences de gestion pour prendre des décisions éclairées et coordonner efficacement les actions nécessaires pour prévenir et répondre aux cyberattaques. Dans cette reconfiguration, il devient crucial d'établir une juridiction claire pour le RSSI au sein de l'organisation. Cette juridiction devrait être centrale et bien intégrée dans le dispositif de cybersécurité global. Cela implique que le RSSI ait une autorité et une influence significatives dans les décisions stratégiques, les politiques et les procédures liées à la sécurité des systèmes d'information.

La juridiction de la profession du RSSI doit également être en lien avec d'autres parties prenantes de l'organisation, telles que les auditeurs internes et les dirigeants, pour garantir une collaboration efficace et une compréhension mutuelle des enjeux et des responsabilités.

Nous concluons que la gestion de la cybersécurité met en lumière les conflits et les questions liées à l'élargissement ou à l'éclatement de la juridiction. Les compétences requises pour la cybersécurité vont au-delà de l'expertise technique et incluent des compétences de gestion. La reconfiguration de la profession de RSSI nécessite une juridiction centrale, intégrée et bien définie au sein du dispositif de cybersécurité de l'organisation. Cela permettra de garantir une coordination efficace et une prise de décision éclairée pour faire face aux défis croissants de la cybersécurité.

5.3.1.7 Le conflit entre les deux professions ne conduit finalement pas à l'émergence d'une nouvelle fonction

La gestion de la cybersécurité met en évidence la nécessité d'une nouvelle organisation plus adaptée pour faire face aux cyberattaques. Dans cette nouvelle organisation, le RSSI doit évoluer pour occuper une position centrale au sein de l'organisation et collaborer étroitement avec les auditeurs internes. Plutôt que de conduire à l'émergence d'une nouvelle fonction distincte, le conflit entre l'audit interne et le RSSI conduit à une réorganisation des fonctions existantes et à une collaboration approfondie entre les deux professions. Cette collaboration renforcée vise à tirer des compétences et des perspectives complémentaires de chaque profession pour améliorer la gestion de la cybersécurité.

Tableau 23 : le conflit entre les deux professions d'audit interne et de RSSI ne conduit pas à l'émergence d'une nouvelle fonction mais plutôt à une réorganisation des fonctions et une collaboration approfondie

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Chef de mission d'audit interne	*Le conflit entre les deux professions d'audit interne et de RSSI ne conduit pas à l'émergence d'une nouvelle fonction mais plutôt à une réorganisation des fonctions et une collaboration approfondie*	*« Nous on n'est en 3ième niveau. Nous on vient vérifier que c'est bien fait mais nous on intervient en 3ième rideau donc pour moi ce n'est pas nous de maintenir tous seul la cybersécurité c'est avec la direction des risques, c'est avec les autres services avec les services qui développent des applications, des services informatiques mais il y a pas que l'audit nous on vient en derrière c'est ce que je puisse dire donc on n'est pas, ce n'est pas que à nous de les faire.…»*
Directeur des risques conformité et contrôle permanent		*« L'audit interne c'est du niveau 3. Le niveau 3 est opérationnel. Moi je suis en niveau 2, moi je ne peux pas être opérationnel. C'est au niveau 1 de l'être. » « Le contrôle permanent de niveau 3, le contrôle permanent de niveau 2 c'est moi, et le contrôle de niveau 3 c'est l'audit. Le niveau 3 il fait des missions ponctuelles, des missions qui peuvent être sur la cyber criminalité. Mais un rôle d'audit ni un rôle de contrôle ni un rôle de gérer l'opérationnel.»*
Responsable informatique		*« Mais la détection à notre niveau, elle est toujours après quoi. On ne peut rien anticiper, on ne peut rien mesurer. Donc pour moi, à mon niveau, ça va être la sensibilisation, la communication ou bien la gestion de la crise quand il y a une attaque et du coup donc … »*

Sur le plan juridictionnel, cette évolution implique que le RSSI doit assumer une position centrale dans le dispositif de cybersécurité de l'organisation. Il est responsable de la coordination et de la mise en œuvre des mesures de sécurité, tout en collaborant étroitement avec les auditeurs internes pour évaluer l'efficacité des politiques et des procédures de sécurité en place.

La collaboration entre le RSSI et les auditeurs internes permet de combiner l'expertise technique du RSSI avec la perspective objective de l'audit interne, favorisant ainsi une meilleure compréhension des risques et une identification plus précise des lacunes de sécurité. Cela peut également engendrer des recommandations plus solides et une prise de décision plus éclairée pour renforcer la cybersécurité.

Nous concluons que la gestion de la cybersécurité nécessite une nouvelle organisation plus adaptée, où le RSSI occupe une position centrale et collabore étroitement avec les auditeurs internes. Cette réorganisation vise à tirer parti des compétences complémentaires des deux professions et à améliorer la gestion globale de la cybersécurité. La clarté des responsabilités et

la collaboration ouverte sont essentielles pour assurer une coordination efficace et une prise de décision éclairée dans le domaine de la cybersécurité.

5.3.1.8 L'audit interne : du tiers conflictuel à l'arbitre juridictionnel

Nous avons observé que l'audit interne joue *in fine* un rôle d'arbitre juridictionnel dans le contexte de la gestion de la cybersécurité. En tant qu'entité indépendante au sein de l'organisation, l'audit interne est chargé d'évaluer les politiques, les procédures et les contrôles internes, y compris ceux liés à la cybersécurité. Dans ce rôle, l'audit interne contribue à résoudre les conflits de juridiction qui peuvent survenir entre les différentes parties prenantes impliquées dans la cybersécurité, tels que le RSSI et les auditeurs internes. L'audit interne peut examiner objectivement les domaines de chevauchement ou de désaccord, et formuler des recommandations pour clarifier les responsabilités et établir des lignes directrices claires.

Tableau 24 : l'audit interne comme un arbitre juridictionnel

Observations perçues		**Extraits des Verbatim**
Profession		**RSSI**
Chef de mission d'audit interne	*L'audit interne comme un arbitre juridictionnel*	*« suite au rapport d'audit, le cabinet externe a trouvé que justement on ne prenais pas suffisamment compte la sécurité du système d'information pour développer des application privatives… » « le RSSI n'est pas suffisamment pro actif... »*
Directeur d'audit interne		*« La cybersécurité est un sujet primordiale sensible qui doit être gérer par la confidentialité des rapports et la sensibilisation en permanence des employés.»*

En tant qu'arbitre juridictionnel, l'audit interne aide à garantir que les décisions et les actions entreprises dans le domaine de la cybersécurité sont conformes aux réglementations en vigueur, aux normes du secteur bancaire et aux meilleures pratiques. Il évalue la conformité et l'efficacité des mesures de sécurité mises en place, et fournit des informations impartiales sur l'état de la cybersécurité au sein de la BPVF.

L'audit interne joue donc un rôle important dans la définition et la clarification des juridictions liées à la cybersécurité. En se basant sur des principes d'indépendance, d'objectivité et de compétence, l'audit interne peut aider à établir un équilibre et une collaboration efficace entre les différentes parties prenantes impliquées.

La fonction d'arbitre juridictionnel de l'audit interne ne remplace pas les responsabilités

individuelles des acteurs impliqués dans la cybersécurité. Au contraire, elle vise à faciliter la coordination et à fournir des conseils impartiaux pour résoudre les conflits et garantir une gouvernance solide de la cybersécurité au sein de l'organisation.

Nous concluons que l'audit interne peut remplir le rôle d'arbitre juridictionnel dans le domaine de la cybersécurité. Il peut contribuer à résoudre les conflits de juridiction, établir des lignes directrices claires et évaluer l'efficacité des mesures de sécurité. En agissant de manière indépendante et objective, l'audit interne favorise une gouvernance solide de la cybersécurité et assure la conformité aux réglementations et aux normes applicables.

5.3.2 Résultats de recherche : les banques libanaises

Nous admettons que la cybersécurité des banques libanaises s'inscrit dans une question de cybersécurité nationale puisque le contexte libanais est un contexte conflictuel. Les questions d'autonomie et sur le contexte dans lequel aujourd'hui nos gouvernants inscrivent la question de la cybersécurité bancaire. La question s'est perdue dans la déferlante de la crise systématique qui affecte la banque libanaise aujourd'hui. Le gouvernement libanais annonce des spécificités et des procédures pour assurer la cybersécurité du pays mais on ne sait pas comment. La crise économique, monétaire et financière au Liban, remet à plus tard les questions de cybersécurité.

Nous avons observé que les dépenses en cybersécurité dans les banques libanaises chutent. La cybersécurité est un risque opérationnel et les banques libanaises sont affrontés à un risque systématique à cause de la crise du secteur bancaire libanais. Donc, le risque de cybersécurité sera un risque mineur faisant face à un risque majeur systématique.

Au sein de la BPVF, nous avons pu récupérer ces résultats de recherche.

5.3.2.1 La prégnance d'autres libertés crée des juridictions ouvertes

La cybersécurité est envisagée en situation de conflit puisque le terrain bancaire libanaise fait face à une crise économique, financière et monétaire. Les dispositifs observés sont en suspens et le secteur bancaire libanais risque de s'effondrer à tout moment.

Tableau 25 : les banques libanaises ne priorisent pas le risque de cybersécurité

Observations perçues	Extraits des Verbatim
Les banques libanaises semblent avoir d'autres priorités que la cybersécurité	*« La cybersécurité, ce n'est pas une priorité pour nous… »* *« Le cadre de réglementation et de contrôle prudentiel du système bancaire libanais présente un degré élevé de conformité avec les principes définis par le Comité de Bâle. Mais cette situation s'est fortement dégradée dans le contexte de la récente crise politique que connaît le Liban. »*

Nous remarquons que la cybersécurité n'est pas une priorité au Liban mais ce qui est primordial c'est la survie du secteur bancaire durant cette crise.

5.3.2.2 Les banques libanaises sont en retard à l'échelle mondiale de cybersécurité par manques de moyens techniques et financiers

Malgré de nombreux efforts réalisés, mais de façon éparpillée, nous avons observé que le Liban demeure en retard par rapport à l'échelle mondiale en cybersécurité.

Tableau 35 : les banques libanaises sont en retard à l'échelle mondiale de cybersécurité par manques de moyens techniques et financières

Observations perçues	Extraits des Verbatim
Le secteur bancaire libanais est en retard par rapport à l'échelle mondiale en cybersécurité	*« Le Liban est classé 118e sur 164 selon l'indice mondiale de cybersécurité. »*

Le Liban est classé 118^{ième} sur 164 selon l'indice mondial de cybersécurité de l'Union internationale des télécommunications. Les banques libanaises ne possèdent pas encore les moyens techniques nécessaires pour identifier les cybers attaques (Babin, 2019).

5.3.2.3 L'absence d'une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité

Nous remarquons l'absence d'une stratégie claire en matière de cybersécurité entre les différents organismes même les banques privées ce qui rend difficile la défense et la prévention des cyberattaques. Nous préconisons le besoin du secteur bancaire libanais d'avoir une agence nationale de cybersécurité mais sa mise en œuvre est confrontée à plusieurs facteurs tel que

l’absence de lois et de réglementations gouvernant la cybercriminalité.

Tableau 26 : l' absence d’une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité

Observations perçues	Extraits des Verbatim
L’absence d’une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité	*« Chaque banque a sa propre vision et ses procédures en matière de sécurité, qui peuvent être efficaces dans sa situation courante, mais rendent plus difficile la collaboration sans critères bien définis et, plus important encore, le partage d'informations et un cadre commun au plus haut niveau. »* *« Au Liban, il n’y a pas de lois et de réglementations qui protège les institutions gouvernementales et les banques dans le domaine numérique en définissant clairement les actes criminels. Donc, les conséquences et les implications de ces actes criminels ne sont pas claires. »* *« Aucune agence de cybersécurité existe ni fasse respecter les lois relatives à la cybersécurité, ou collabore avec des personnes possédant l'expertise nécessaire pour aider les organisations à configurer leurs cadres de sécurité. De plus, le pays souffre également d’un manque d’offre au niveau des formations, ainsi que d’un soutien inexistant à la recherche et au développement. De même, l’absence d’organisme qui doit assurer la continuité des programmes de sensibilisation à la cybersécurité. »*

L’absence de stratégie claire en matière de cybersécurité entre les différents organismes même les banques privées ce qui rend difficile la défense et la prévention des cyberattaques. Nous préconisons le besoin du secteur bancaire libanais d’avoir une agence nationale de cybersécurité mais sa mise en œuvre est confrontée à plusieurs facteurs tel que l’absence de lois et de réglementations gouvernant la cybercriminalité.

Nous résumons que la gouvernance des banques libanaises doit pleinement prendre en compte le thème de la cybersécurité. Leur inévitable transformation numérique, et leur existence même, en dépendent.

Les autorités libanaises doivent également faire de leur mieux pour contribuer à limiter les risques en sensibilisant le public aux dangers de la cybercriminalité, et notamment en renforçant la législation dans ce domaine. Un moyen efficace d'y parvenir est de créer une agence de prévention et de contrôle sur le modèle de l’ANSSI (Boutros, 2017).

5.3.2.4 La corruption entame la mise en œuvre de la cybersécurité dans les banques libanaises

Tableau 37: la corruption menace la mise en œuvre de la cybersécurité

Observations perçues	Extraits des Verbatim
La lutte contre la corruption dans l'économie numérique	*« Le Liban a maintenu son rang élevé parmi les pays corrompus en 2018… La corruption et l'économie numérique sont diamétralement opposées, la corruption étant la principale menace contre la mise en œuvre de la cybersécurité, alors que l'économie numérique peut potentiellement détruire ou au mieux perturber les schémas de corruption habituels. »*

Après la guerre civile, une génération complète de libanais a grandi dans une société dépourvue de toute forme d'organisation ou de réglementation. Au lieu de rétablir les valeurs traditionnelles de la culture libanaise d'avant-guerre, qui étaient basées sur l'honnêteté, le respect et l'aptitude, cette génération est sortie de la confrontation en exprimant son désir de compensation après de longues années de privation. Les employés corrompus sont impliqués dans des cyberattaques passives, directes ou indirectes, internes ou externes, visant à rendre inopérants les services fournis par l'infrastructure de l'économie numérique nationale. Leur but est d'alléguer l'inefficacité des services numériques fournis afin de se rabattre sur les opérations manuelles précédentes, sous lesquelles les schémas de corruption ne pouvaient pas être tracés. Nous soulignons que cette stratégie peut être suivi dans le secteur bancaire libanais.

5.3.2.5 Le contexte sociodémographique complique la cybersécurité

La création d'une agence de prévention et de contrôle sur le modèle de l'ANSSI demeure aussi une question de contexte sociodémographique.

Tableau 27 : le contexte sociodémographique entrave la cybersécurité au niveau national libanais

Observations perçues	Extraits des Verbatim
Le contexte sociodémographique aux multiples facettes	*« Le Liban repose sur une démocratie qui préserve l'équité des droits entre ses multiples communautés religieuses. Le pluralisme est un élément unique et distinctif de la nation et pourrait être utilisée pour déstabiliser tous les domaines de la vie publique et démocratique… »*

Par exemple, les quatre vice-gouverneurs de la BDL sont élus selon le respect du contexte sociodémographique : un chrétien maronite, un musulman sunnite, un musulman chiite et un chrétien catholique.

La coopération, le partage des moyens et l'utilisation de qualifications appropriées sont entravés car les multiples entités qui composent la société libanaise se tournent vers l'isolationnisme et l'individualisme, ce qui priverait la nation des compétences nécessaires au bon fonctionnement de la société et affecterait la résilience globale construite sur la collaboration entre les acteurs. Pour arrêter la propagation d'une telle menace, il faut prendre des mesures coordonnées et globales, en associant toutes les parties prenantes concernées, à l'aide d'une expertise fiable et d'un large éventail d'outils de lutte contre cette forme de criminalité.

5.3.2.6 Le manque de collaboration entre les banques au niveau national

Nous constatons que chaque banque libanaise travaille sur sa sécurité séparément, sans un cadre clair pour la collaboration avec d'autres banques, alors que nous soulignons que le partage d'informations et de données sera bénéficiaire à chaque banque.

Tableau 39 : manque de collaboration sur le terrain bancaire libanais

Observations perçues	Extraits des Verbatim
Absence de collaboration entre les banques libanaises au niveau national	*« Nous avons notre propre système de sécurité qui est exclusif à notre réseau, notre banque et nos filiales… »* *« il s'agit d'une compétition au niveau internationale… avoir plus de clients sur le terrain bancaire libanais… »*

Nous remarquons le manque de collaboration et de coopération entre les différents départements de la même banque, en particulier dans le domaine de la cybersécurité. Chaque département et chaque unité agissent et travaillent de manière indépendante au lieu de coopérer pour sécuriser l'ensemble de l'organisation auxquelles ils appartiennent. Nous revenons à l'idée que la cybersécurité n'est pas bien appréhender dans le secteur bancaire libanais.

5.3.2.7 L'absence d'initiative pour un système national d'information et une stratégie de transformation numérique au plus haut niveau

Nous soulignons que le Liban est toujours dépourvu d'une vision nationale avec une approche interinstitutionnelle coopérative.

Tableau 40 : l'absence d'initiative sur le terrain bancaire libanais

Observations perçues	Extraits des Verbatim
Absence de collaboration entre les banques libanaises au niveau national	*« Depuis toujours, le Liban était dépourvu d'une vision nationale avec une approche interinstitutionnelle coopérative … »* *« l'environnement compromet la cybersécurité… »*

Nous observons un déséquilibre important entre les institutions. Par contre, la gestion coordonnée des technologies de l'information et de la communication (TIC) n'est pas institutionnalisée au plus haut niveau, ce qui rend très difficile la détection, l'identification et la gestion des cyberincidents. Dans un tel environnement, l'efficacité de la cybersécurité et de la cyberdéfense pour protéger les citoyens et les organisations publiques ou privées ciblés par les cyberattaques est gravement compromise.

5.3.2.8 La pénurie d'experts en cybersécurité au terrain bancaire libanais

Les organisations, les administrations et les universités libanaises nécessitent des campagnes de sensibilisation continus en termes de cybersécurité en s'appuyant sur des programmes éducatifs à tous les niveaux (universités, emplois, conférences, ...).

Tableau 41 : une pénurie d'experts en cybersécurité en plus de leur difficulté d'adaptation aux changements rapides

Observations perçues	Extraits des Verbatim
Absence d'experts en cybersécurité et une difficulté d'adaptation aux changements rapides	*« Nous avons un manque de personnes possédant des expertises techniques spécialisés en cybersécurité… »* *« il faut former les gens…leur proposer des formations ou des cursus en cybersécurité… »*

Cependant, les formations en cybersécurité sont limitées à certains domaines dans les universités et les communautés avec des programmes respectifs. Nous soulignons le recours à une approche auto-éducative dans ce domaine où il existe une absence de cursus et de programme de formation appropriés en cybersécurité. Il est important de mettre ne place des

programmes ciblés qui fournissent les ressources humaines nécessaires pour irriguer tous les secteurs libanais exposés à la cybercriminalité.

Nous concluons que la cybersécurité au Liban n'est pas bien structurée au niveau national et manque de coopération et de coordination entre les organisations des secteurs public et privé et au niveau international pour répondre aux besoins fondamentaux de ses citoyens en matière de sécurité et de confidentialité.

Conclusion intermédiaire

Dans la section 5.3, nous avons montré que la cybersécurité dans le secteur bancaire présente des défis complexes, notamment en ce qui concerne la délimitation des responsabilités et des compétences entre les RSSI, les auditeurs internes et d'autres professionnels de la cybersécurité. Ces conflits de juridiction peuvent se produire, compromettant la sécurité des systèmes d'information. Pour résoudre ces problèmes, il est nécessaire de trouver un équilibre entre les différentes parties prenantes et de favoriser la collaboration.

Une prise de conscience croissante de l'importance de la sécurité des systèmes d'information dans le secteur bancaire se traduit également par l'émergence de nouveaux métiers de cybersécurité, comme celui de DPO, d'analystes cyber et par la création de postes de RSSI-G. La gestion des conflits potentiels doit toutefois être proactive et les rôles doivent être clairement définis.

En raison de la situation économique et sociopolitique du Liban, la cybersécurité dans le contexte spécifique des banques libanaises est confrontée à des difficultés supplémentaires. En raison de la crise financière, la sécurité informatique n'est pas une priorité absolue ; cependant, des mesures doivent être prises pour améliorer la cybersécurité, notamment la création d'une agence nationale de prévention et de contrôle de la cybersécurité.

5.4 Synthèse des résultats du terrain bancaire en termes cybersécurité

Nous présentons dans cette section la synthèse des résultats ressortis au niveau d'une approche positive de l'identité des auditeurs internes et des RSSI, d'une approche relative inspirée par le travail de Dubar et d'une approche juridictionnelle imposée par Abbott. Nous présentons une synthèse de ces résultats à travers un tableau récapitulatif. Nous détaillons les résultats du terrain bancaire français et libanais au niveau de ces trois approches.

Nous résumons cette partie 5.4 par une synthèse sur la base des points commun entre la BPVF et les banques libanaises.

5.4.1 Synthèse sur le secteur bancaire

Nous présentons tout d'abord une synthèse des résultats de recherche selon les trois approches sur le terrain bancaire libanais et français qui se résume à travers le tableau ci-dessous.

Tableau 28 : les résultats du terrain bancaire en cybersécurité

Description	Partie A	Partie B	Partie C
Section1 / Section 2	Traits saillants des identités professionnelles	Le regard réflexif des acteurs quant à leur capacité de répondre à des attaques.	L'auditeur interne est généraliste. Il n'est pas en capacité d'agir au moment de la crise. Le RSSI se questionne sur sa compétence en cybersécurité.
	Approche relative	Le regard externe (pour Autrui) sur cette capacité de répondre aux attaques.	Résultat de terrain : Auditeur interne apporte de la valeur ajoutée. Il est indépendant, règlementaire, objectif et certifié en Audit interne. (Identité pour Soi) Il est reconnu comme un contrôleur ou policier sérieux (Identité par Autrui). Le RSSI possède des compétences et expertise spécialisé. (Identité par Soi) Il est reconnu comme Geek. (Identité par Autrui)
Section 3	Approche juridictionnelle	Le positionnement des professions dans les rôles à jouer face à une attaque.	Le RSSI n'est pas expert en sécurité informatique. Les conflits entre les auditeurs internes et les RSSI portent sur les attributions des uns et des autres. L'émergence de nouvelles professions pour renforcer les équipes de cybersécurité. La juridiction du RSSI est influencée par sa dépendance à l'égard des prestataires externes spécialisés et par les tensions avec d'autres acteurs. Les compétences requises pour la cybersécurité vont au-delà de l'expertise technique et incluent des compétences de gestion. La cybersécurité nécessite une nouvelle organisation plus adaptée. L'audit interne favorise une gouvernance solide de la cybersécurité. La cybersécurité n'est pas une priorité pour les banques libanaises qui sont déjà en retard à l'échelle mondiale de cybersécurité par manques de moyens techniques et financières. La corruption, le manque de profils compétents et le contexte sociodémographique inhibent la mise en œuvre de la cybersécurité.

5.4.2 Synthèse spécifique au terrain bancaire français

Les identités professionnelles des auditeurs internes et des RSSI met en évidence plusieurs facteurs importants comme la compétence, l'absence de crédibilité du RSSI et les regards externes. Nous résumons les résultats sur le terrain bancaire français par le tableau ci-dessous.

Tableau 29 : les points clés sur le terrain bancaire français

BPVF	Résultats obtenus
Priorité	La cybersécurité devient une priorité absolue pour BPVF qui a mis en place un certain nombre de fonctionnalités et de services pour assurer la sécurité de ses systèmes informatiques et de ses données
Trois lignes de défense	L'audit interne n'intervient pas directement dans la gestion de la cybersécurité. Les auditeurs internes agissent en troisième niveau de défense.
Les traits saillants de l'identité professionnelle des auditeurs internes et des RSSI	• Généraliste non technique versus Technique et expertise spécialisée : Absence des expertises spécialisés en sécurité informatique chez les auditeurs internes • Valeur ajoutée versus Leadership en Stress : Absence des compétences de Leadership chez les RSSI. • Absence de crédibilité du RSSI : Manque d'expertise spécialisée en sécurité informatique chez le RSSI. • L'indépendance des auditeurs internes créent un espace de confiance au près des différents acteurs. • L'objectivité renforce l'identité professionnelle des auditeurs internes en tant qu'experts fiables et impartiaux • L'identité professionnelle des auditeurs internes saillantes est renforcée par l'expertise réglementaire, la responsabilité de conformité et la sensibilisation à la gestion des risques : L'audit interne est une obligation règlementaire au niveau de la BPVF. • Les auditeurs internes sont perçus comme des gendarmes et des contrôleurs dans la BPVF : Les auditeurs internes font face à des braquages lors de leurs missions d'audit.
Impact organisationnel des identités professionnelles au regard de la gestion des risques et des juridictions	• La profession revendique une juridiction : les RSSI définissent les contours de leur juridiction de manière discrétionnaire, ils ne sont pas des experts en sécurité informatique. • Le manque de répartition des rôles conduit à des chevauchements ou à des vides en matière de responsabilités. Les auditeurs internes se retrouvent confrontés à des situations où ils estiment que les mesures de sécurité proposées par les RSSI sont insuffisantes et inappropriées, tandis que les RSSI perçoivent les auditeurs internes incompétent comme n'ayant pas une compréhension suffisante des enjeux techniques et opérationnels comme la cybersécurité. • L'émergence éventuelle de nouvelles professions pour assister à la gestion de la cybersécurité : DPO, RSSI-Groupe… • L'identité professionnelle du RSSI est façonnée par ses compétences, son expérience et son autorité au sein de l'organisation. Pour préserver une juridiction solide, il est crucial

	que les RSSI continuent de développer leurs compétences et leurs connaissances en cybersécurité. • La juridiction du RSSI est influencée par sa dépendance à l'égard des prestataires externes spécialisés et par les tensions avec d'autres acteurs. • L'externalisation de la fonction de cybersécurité en partie crée une dépendance nouvelle mais qui est règlementé par l'ANSSI. • Les compétences requises pour la cybersécurité vont au-delà de l'expertise technique et incluent des compétences de gestion. • La gestion de la cybersécurité met en évidence la nécessité d'une nouvelle organisation plus adaptée pour faire face aux cyberattaques. • L'audit interne joue donc un rôle important dans la définition et la clarification des juridictions liées à la cybersécurité.

5.4.3 Synthèse spécifique au terrain bancaire Libanais

La cybersécurité n'est pas considérée comme une priorité pour les banques libanaises pour plusieurs raisons tels que des ressources limitées, des priorités concurrentes et un manque de sensibilisation quant aux risques de sécurité informatique. Mais le facteur principal demeure la crise économique et financière qui touche le secteur bancaire libanais. Nous résumons les résultats sur le terrain bancaire libanais par le tableau ci-dessous.

Tableau 44 : les points clés sur le terrain bancaire libanais

Banques libanaises	Résultats obtenus
Priorité	La cybersécurité n'est pas considérée comme une priorité pour les banques libanaises vue la crise économique et financière qui frappe le Liban. Leur objectif principal demeure une question de survie et de continuité.
Trois lignes de défense	L'audit interne intervient en troisième niveau de défense.
Les traits saillants de l'identité professionnelle des auditeurs internes et des RSSI	• Absence d'identité professionnelle parce que la profession n'est pas encore structurée dans le secteur bancaire libanais. • Intégration de la cybersécurité demeure un élément essentiel des identités professionnelles des acteurs clés pour renforcer la résilience des banques libanaises face aux cybermenaces. • La collaboration entre les auditeurs internes et les RSSI, ainsi qu'avec d'autres parties prenantes, est essentielle pour établir une identité professionnelle solide. • La cybersécurité des banques libanaises s'inscrit dans une question de cybersécurité nationale puisque le contexte libanais est un contexte conflictuel.
Impact organisationnel des identités professionnelles au regard de la gestion des risques et des juridictions	• Les banques libanaises sont en retard à l'échelle mondiale de cybersécurité par manques de moyens techniques et financières. • Chaque banque a sa propre vision et ses procédures en matière de sécurité. • Absence d'une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité. • La corruption menace la mise en œuvre de la cybersécurité. • Le contexte sociodémographique entrave la cybersécurité au niveau national libanais. • Le Liban est toujours dépourvu d'une vision nationale avec une approche interinstitutionnelle coopérative. • La cybersécurité au Liban n'est pas bien structurée au niveau national et manque de coopération et de coordination entre les organisations des secteurs public et privé et au niveau international pour répondre aux besoins fondamentaux de ses citoyens en matière de sécurité et de confidentialité.

5.4.4 Rapprochement des terrains

Nous présentons à travers le tableau ci-dessous une synthèse sur la base des points communs et opposés entre la BPVF et les banques françaises au niveau de l'assurance de la cybersécurité.

Tableau 45: la synthèse sur la base des points communs et opposés sur les terrains bancaires français et libanais

<table>
<tr><th>Résultats obtenus</th><th>BPVF</th><th>Banques Libanaises</th></tr>
<tr><td>Priorité</td><td>• La cybersécurité est une priorité</td><td>• La cybersécurité n’est pas une priorité</td></tr>
<tr><td>Trois lignes de défense</td><td colspan="2">• L’audit interne intervient en troisième niveau de défense.</td></tr>
<tr><td rowspan="3">Les traits saillants de l’identité professionnelle des auditeurs internes et des RSSI</td><td>• Le contexte français est un contexte pacifier internationale.
• Absence des compétences de Leadership et de crédibilité chez les RSSI.
• L’indépendance des auditeurs internes créent un espace de confiance au près des différents acteurs.
• L’objectivité renforce l’identité professionnelle des auditeurs internes en tant qu’experts fiables et impartiaux
• L’identité professionnelle des auditeurs internes saillantes est renforcée par l’expertise réglementaire, la responsabilité de conformité et la sensibilisation à la gestion des risques : L’audit interne est une obligation règlementaire au niveau de la BPVF.</td><td>• Absence d’identité professionnelle parce que la profession n’est pas encore structurée dans le secteur bancaire libanais.
• La cybersécurité s’inscrit dans une question de cybersécurité nationale puisque le contexte libanais est un contexte conflictuel.</td></tr>
<tr><td colspan="2">• Absence des expertises spécialisés en sécurité informatique chez les auditeurs internes</td></tr>
<tr><td colspan="2">• Les auditeurs internes sont perçus comme des gendarmes et des contrôleurs : Les auditeurs internes font face à des braquages lors de leurs missions d’audit.</td></tr>
<tr><td rowspan="4">Impact organisationnel des identités professionnelles au regard de la gestion des</td><td>• Le contexte français est un contexte pacifier internationale.</td><td>• Le contexte libanais est un contexte conflictuel.</td></tr>
<tr><td colspan="2">• Pénurie d'experts en cybersécurité</td></tr>
<tr><td>• La France est classé 9e sur 164 selon l’indice mondiale de cybersécurité.[10]</td><td>• Le Liban est classé 118e sur 164 selon l’indice mondiale de cybersécurité. [11]</td></tr>
<tr><td>• L’externalisation de la fonction de cybersécurité en partie crée une dépendance nouvelle mais qui est</td><td>• Absence d’une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité.</td></tr>
</table>

[10] [3] Indice mondial de cybersécurité 2020, Mesurer l’engagement en matière de cybersécurité, Union internationale des télécommunications (UIT), Publié en Suisse Genève, 2021. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-F.pdf

risques et des juridictions	règlementé par l'ANSSI.	
	• Le manque de répartition des rôles conduit à des chevauchements ou à des vides en matière de responsabilités.	• La corruption et le contexte sociodémographique entament la mise en œuvre de la cybersécurité.
	• L'audit interne joue donc un rôle important dans la définition et la clarification des juridictions liées à la cybersécurité.	• L'audit interne agit en troisième niveau de contrôle.
	• Le conflit entre l'audit interne et le RSSI conduit à une réorganisation des fonctions existantes et à une collaboration approfondie entre les deux professions. Cette collaboration renforcée vise à tirer des compétences et des perspectives complémentaires de chaque profession pour améliorer la gestion de la cybersécurité.	• Manque de collaboration sur le terrain bancaire libanais entre les professions.

Ce tableau de synthèse met en évidence les disparités significatives dans les pratiques de sécurité informatique entre les secteurs bancaires français et libanais.

En France, la cybersécurité est clairement établie comme une priorité, soutenue par un cadre réglementaire strict et la présence d'une agence nationale spécialisée (ANSSI). Cette orientation favorise une collaboration renforcée entre l'audit interne et les responsables de la sécurité des systèmes d'information (RSSI), facilitant ainsi une gestion intégrée des risques cybernétiques. L'indépendance et l'objectivité des auditeurs internes jouent un rôle crucial en renforçant la confiance des parties prenantes, appuyées par leur expertise réglementaire et leur responsabilité en matière de conformité. En contraste, au Liban, la cybersécurité n'est pas aussi rigoureusement priorisée dans le secteur bancaire en raison de défis structurels et socio-économiques plus complexes, tels que la corruption et les conflits internes. L'absence d'une agence nationale dédiée à la cybersécurité et le déficit d'expertise spécialisée parmi les auditeurs internes limitent la capacité du pays à répondre efficacement aux menaces numériques croissantes. Cette situation crée des tensions et des lacunes dans la définition des rôles et des responsabilités, compromettant ainsi la sécurité des systèmes d'information des banques libanaises.

En conclusion, ces différences soulignent l'importance critique d'un cadre réglementaire robuste et d'une collaboration harmonieuse entre les différentes fonctions (audit interne, RSSI) pour renforcer la résilience face aux menaces cybernétiques. La situation en France reflète un modèle plus mature et intégré, tandis que le Liban expose les défis persistants rencontrés dans les environnements où la cybersécurité ne bénéficie pas d'une priorité nationale clairement définie.

En comparant les pratiques de sécurité informatique dans les secteurs bancaires français et

libanais, chacun est typique de certaines caractéristiques nationales et régionales spécifiques.

La France est typique d'une approche où la cybersécurité est intégrée dans le cadre réglementaire national avec la présence d'une agence spécialisée (ANSSI). Cela reflète une gouvernance robuste et une coordination étroite entre les autorités réglementaires, les auditeurs internes et les RSSI. Le Liban représente des défis rencontrés dans les contextes où la cybersécurité n'est pas une priorité nationale clairement établie. Les difficultés structurelles, socio-économiques comme la corruption et les conflits internes, entravent la mise en œuvre efficace de mesures de sécurité robustes.

Exemplaire des limites dues à l'absence d'une agence nationale dédiée à la cybersécurité et d'une expertise spécialisée parmi les auditeurs internes, ce qui conduit à des lacunes dans la définition des responsabilités et à une capacité réduite à gérer les risques cybernétiques.

Ainsi, la France illustre un modèle où la cybersécurité est intégrée dans le tissu réglementaire et institutionnel, favorisant une gestion proactive des risques. En revanche, le Liban expose les défis persistants associés à des environnements où la cybersécurité est moins priorisée, influencée par des contextes nationaux et des infrastructures gouvernementales moins développées.

Conclusion intermédiaire

La section 5.4 du chapitre 5 nous amène à examiner les identités professionnelles des auditeurs internes et des RSSI sous trois approches distinctes : positive, relative et juridictionnelle. Les résultats mettent en évidence des différences significatives entre le contexte français, représenté par le BPVF, et le contexte libanais, caractérisé par des enjeux plus complexes.

En France, la cybersécurité est une priorité du BPVF, tandis qu'au Liban elle est souvent reléguée au second plan en raison de ressources limitées et de priorités concurrentes. Les auditeurs internes jouent un rôle clé de troisième ligne de défense en France, mais cette position est moins importante au Liban. Dans les deux cas, les RSSI manquent de leadership et de crédibilité, mais en France l'indépendance des auditeurs internes crée un espace de confiance. L'expertise réglementaire, les responsabilités en matière de conformité et la sensibilisation à la gestion des risques renforcent l'identité professionnelle de l'auditeur interne en France, alors que cette profession n'est pas encore solidement implantée au Liban. La cybersécurité s'inscrit en France dans un contexte international apaisé, tandis qu'au Liban elle est liée aux enjeux nationaux de cybersécurité dans un contexte conflictuel.

Il y a une pénurie de professionnels de la cybersécurité dans les deux contextes, mais la France

se classe bien plus haut dans l'indice mondial de cybersécurité. Il existe en France une externalisation de la fonction cybersécurité, réglementée par l'ANSSI. Elle est cependant absente au Liban, où se fait sentir l'absence d'une agence nationale de prévention et de contrôle de la cybersécurité.

Le manque de répartition des rôles entraîne des chevauchements et des écarts de responsabilités, notamment en France, où le conflit entre l'audit interne et le RSSI nécessite une réorganisation et une collaboration accrue. Au Liban, la coopération entre les métiers de la cybersécurité est insuffisante.

Nous concluons que la cybersécurité bancaire est abordée différemment en France et au Liban en raison de contextes nationaux et de priorités différentes. Il existe cependant des similitudes, comme la pénurie d'experts en cybersécurité et la nécessité de clarifier les rôles et les responsabilités. La collaboration entre l'audit interne et le RSSI apparaît comme une solution clé pour renforcer la gestion de la cybersécurité dans les deux contextes, en tirant parti des compétences complémentaires de chaque métier.

Synthèse du chapitre 5 : identités professionnelles et dynamiques interprofessionnelles dans le contexte de la cybersécurité

Le chapitre 5 nous a permis de présenter un aperçu complet des enjeux, des pratiques, et des résultats liés à la sécurité informatique en cybersécurité sur le terrain bancaire libanais et français.

Dans la partie 5.1, nous avons examiné les enjeux et défis de la cybersécurité dans le secteur bancaire et souligné l'importance cruciale de ce sujet dans le contexte de la numérisation croissante des services financiers. Les menaces sont de plus en plus sophistiquées et la nécessité de prévenir les attaques et de protéger les données des clients est au premier plan.

La partie 5.2 a approfondi l'analyse des pratiques de gestion de la cybersécurité dans les banques et a mis en évidence les différentes approches pour résoudre ce problème. De l'audit interne au RSSI, en passant par la réglementation et les normes de sécurité, nous avons examiné les stratégies utilisées pour renforcer la posture de sécurité des institutions financières.

La partie 5.3 a approfondi la question de l'identité professionnelle des acteurs de la cybersécurité dans les banques, en se concentrant sur les rôles et responsabilités des auditeurs internes et des RSSI. Nous avons constaté des différences significatives dans la manière dont ces acteurs sont perçus et agissent, selon le contexte national et l'importance accordée à la cybersécurité.

Enfin, dans la partie 5.4, les résultats de la recherche ont été synthétisés en comparant les réalités de la banque française BPVF avec celles des banques libanaises, mettant en évidence les différences majeures liées aux contextes nationaux, aux priorités et aux ressources disponibles.

Dans l'ensemble, ce chapitre montre que la cybersécurité dans le secteur bancaire est une question complexe et multiforme qui est fortement influencée par le contexte national et les ressources disponibles. Alors que certaines banques mettent en œuvre des stratégies avancées pour faire face aux menaces, d'autres sont confrontées à des défis majeurs liés aux crises économiques et financières. Cependant, des points communs émergent, notamment la nécessité de renforcer l'expertise en matière de cybersécurité, de clarifier les responsabilités et de promouvoir la collaboration entre les différentes parties prenantes. La cybersécurité reste un défi crucial pour les banques et nécessite une vigilance constante et une adaptation continue aux évolutions technologiques et aux nouvelles menaces.

CHAPITRE 6.

DISCUSSION ET PROPOS CONCLUSIF

Sommaire du chapitre 6. Discussion et propos conclusif

6. Discussion et propos conclusif

Ce chapitre se divise en trois sections respectives. La première partie revient sur l'intérêt d'aborder la question de la cybersécurité par les identités professionnelles de manière pratique et théorique. Nous rappelons les éléments probants des résultats de la BPVF ainsi que la remise en cause des schèmes spécifiques des banques libanaises. La deuxième partie consiste en une phase prospective qui détaille les résultats d'entretiens réalisés avec les leaders de cybersécurité qui viennent complétés nos résultats de recherche sur le terrain bancaire en cybersécurité. La troisième partie consiste en une phase conclusive qui englobe les apports théoriques en expliquant la complémentarité des cadres d'analyses des identités professionnelles ainsi que les limites de la recherche.

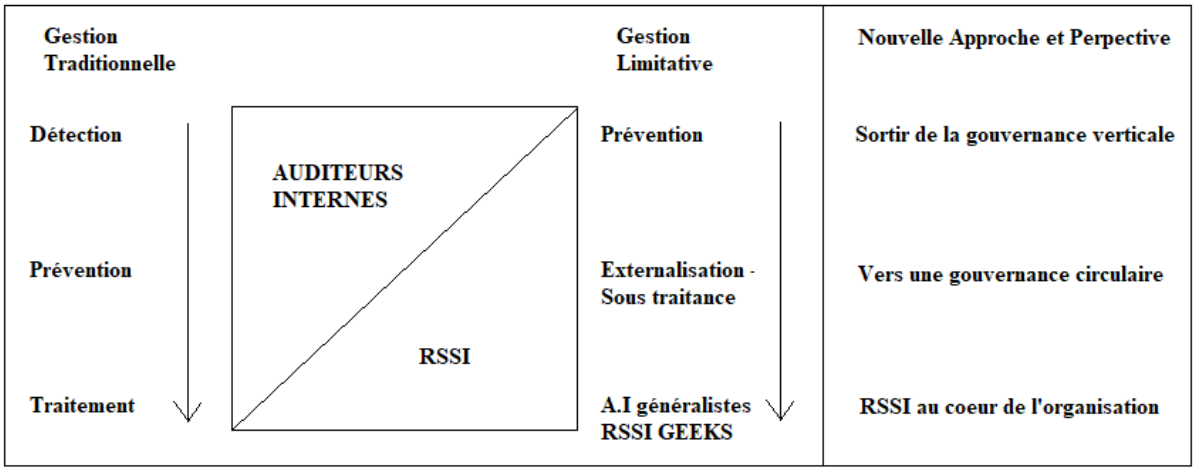


Figure 20 : les perspective de la gestion de la cybersécurité

Source : élaboration personnelle

Nous schématisons la gestion de la cybersécurité selon deux perspectives essentielles : la gestion traditionnelle qui consiste en une vision fondée sur la prévention et le traitement donc détection prévention puis traitement et la gestion limitative où les auditeurs internes sont généralistes et sous traitent la cybersécurité versus RSSI qualifiés comme GEEK. L'auditeur interne joue un rôle de généraliste central, tandis que le RSSI, bien que partiellement expert, assume principalement un rôle d'animateur. Cette dualité de généralistes soulève la question de la redondance de compétences dans l'organisation.

6.1 La cybersécurité par les identités professionnelles de manière théorique et pratique

L'analyse des identités professionnelles montre que la gestion des risques cybernétiques constitue un enjeu majeur, souvent amplifié par des conflits de juridiction dans un contexte organisationnel lacunaire. Cette perspective offre une compréhension renouvelée de la gestion des risques dans le secteur bancaire.

L'approche de la cybersécurité par les identités professionnelles permet de dévoiler différentes couches de risques et vulnérabilités auxquelles sont exposées la BPVF et les banques libanaises. En examinant les identités professionnelles des auditeurs internes et des RSSI, nous comprenons mieux comment leurs rôles et responsabilités interagissent avec les systèmes informatiques et les données sensibles. Cela met en lumière les points d'accès potentiels aux attaques et guide l'élaboration de stratégies de cybersécurité plus efficaces. Nous réexaminons les schémas spécifiques du terrain bancaire libanais à partir des résultats obtenus.

6.1.1 Un rappel des éléments probants des résultats sur le terrain bancaire français

Nous avons présenté nos résultats de recherche sur le terrain bancaire français suivant trois axes organisationnelle, juridictionnelle et au niveau des identités professionnelles. Nous rappelons tout d'abord à travers le tableau récapitulatif ci-dessous les éléments probants des résultats ressortis sur le terrain bancaire français :

Tableau 30 : les éléments probants des résultats sur le terrain bancaire français

Aspect Organisationnel	- L'audit interne agit en 3ième ligne de défense. - Le RSSI est mal positionné et limité en compétences de sécurité informatique. - La gestion des risques demeure une affaire des moyens financiers. - La cybersécurité n'est pas qualifié comme risque majeur au sein de la BPVF. - La cybersécurité restaure la confiance des clients en préservant le capital de la banque. - A la réalité : la cybersécurité est sous-traitée. - La mise en place d'une défense à niveaux 1, 2 et 3 clairement définis est primordiale pour réduire les risques et les menaces en cybersécurité.
Identités professionnelles	- Les compétences techniques en cybersécurité sont primordiales et nécessitent une collaboration étroite entre les acteurs internes et externes pour garantir la sécurité. - Le RSSI doit développer ses compétences et ses stratégies de collaboration et de gestion des risques... - L'internalisation de la cybersécurité demeure une contrainte budgétaire.

	- L'externalisation la cybersécurité est appliquée pour le manque de compétences techniques au niveau des auditeurs internes et des RSSI. - Le RSSI est limité à un rôle de sensibilisation, de réunion de la cellule de crise et de liaison de cette cellule avec les opérateurs informatiques. - La Recommandation du rapport d'audit interne de 2018 exige d'embaucher un second RSSI pour renforcer la cybersécurité et couvrir tous les secteurs à temps plein dans la BPVF. - Absence des expertises spécialisés en sécurité informatique chez les auditeurs internes
Aspect juridictionnel	- La profession revendique une juridiction : le RSSI n'est pas expert en sécurité informatique… - L'éclatement de la juridiction, une juridiction plus élargit : le manque de répartition des rôles conduit à des chevauchements ou à des vides en matière de responsabilités. - Le manque de répartition des rôles conduit à des chevauchements ou à des vides en matière de responsabilités : le DPO… - L'identité professionnelle du RSSI et l'ensemble du dispositif organisationnel façonne la juridiction du RSSI : la juridiction du RSSI est influencée par sa dépendance à l'égard des prestataires externes spécialisés et par les tensions avec d'autres acteurs… - L'externalisation de la fonction de cybersécurité en partie crée une dépendance nouvelle mais qui est règlementé par l'ANSSI. - La juridiction de la profession de cybersécurité doit être centrale dans l'organisation au niveau du dispositif de cybersécurité - La gestion de la cybersécurité est en train de reconfigurer la profession en introduisant de nouvelles perspectives et en élargissant les responsabilités. Le RSSI doit non seulement posséder une expertise technique approfondie, mais également avoir des compétences de gestion pour prendre des décisions éclairées… - Le conflit entre les deux professions ne conduit pas à l'émergence d'une nouvelle fonction : le conflit entre l'audit interne et le RSSI conduit à une réorganisation des fonctions existantes et à une collaboration approfondie entre les deux professions… - L'audit interne agit comme un arbitre juridictionnel en aidant à garantir que les décisions et les actions entreprises dans le domaine de la cybersécurité sont conformes aux réglementations en vigueur…

Nous concluons par une synthèse des résultats de notre recherche sur le terrain bancaire français en matière de cybersécurité. Au niveau organisationnel, l'audit interne joue un rôle central

comme troisième ligne de défense, tandis que le RSSI occupe une position souvent marginalisée, limitée par des compétences spécifiques en cybersécurité et par des contraintes budgétaires. La gestion des risques repose fortement sur les ressources financières disponibles, et bien que la cybersécurité soit essentielle pour la confiance des clients et la résilience de la banque, elle est rarement reconnue comme un risque majeur. Par ailleurs, l'externalisation de la cybersécurité est fréquente en raison du manque d'expertise interne, nécessitant une structure de défense en trois niveaux (1, 2 et 3) pour atténuer les menaces. Sur le plan des identités professionnelles, les compétences en cybersécurité étant dispersées, la collaboration entre acteurs internes et externes s'avère primordiale pour une réponse efficace. Le RSSI doit non seulement développer ses compétences techniques, mais aussi renforcer ses capacités de gestion des risques et de collaboration. Toutefois, les contraintes budgétaires limitent l'intégration interne des compétences, imposant une dépendance vis-à-vis de prestataires externes. Le renforcement des effectifs, avec l'ajout d'un deuxième RSSI, est ainsi recommandé pour une couverture complète des besoins en cybersécurité. L'absence de spécialistes en cybersécurité au sein de l'audit interne pose également des défis supplémentaires. Au niveau juridictionnel, la clarification des rôles et des responsabilités dans la cybersécurité reste un enjeu majeur. Le rôle du RSSI, souvent limité par une expertise technique incomplète et une dépendance vis-à-vis de prestataires externes, révèle des tensions et des recouvrements juridictionnels, exacerbés par le manque de spécialisation. Cette fragmentation est partiellement encadrée par l'ANSSI, mais l'absence d'une fonction dédiée conduit à une réorganisation des rôles existants et à une intensification de la collaboration entre l'audit interne et le RSSI. L'audit interne se positionne alors comme un arbitre juridictionnel pour garantir que la réponse aux cybermenaces respecte les régulations en vigueur.

Les résultats de notre recherche révèlent que la cybersécurité dans le secteur bancaire français est loin de se limiter à une question technique : elle constitue un défi organisationnel et identitaire complexe, influencé par les rôles, les compétences et les interactions entre divers acteurs professionnels, en particulier le RSSI et l'audit interne. Cette complexité révèle plusieurs points de friction et de collaboration, qui méritent une gouvernance circulaire et intégrée.

6.1.1.1 Le défi organisationnel : au-delà des silos, vers une gouvernance partagée

D'un point de vue organisationnel, la cybersécurité est encore souvent perçue comme une fonction isolée, déléguée en partie à des prestataires externes en raison de contraintes budgétaires ou de limitations internes en expertise technique. Cette segmentation des

responsabilités, particulièrement visible entre les rôles du RSSI et de l'audit interne, fragilise la résilience cyber de l'institution. Le RSSI, bien qu'étant le référent en sécurité, se retrouve souvent confiné à des tâches de sensibilisation et de liaison entre les équipes techniques, sans réelle autonomie stratégique, du fait de la dépendance aux prestataires externes et du manque de compétences spécialisées en interne. De plus, l'audit interne, censé assurer une fonction de contrôle, souffre également d'un déficit d'expertise en cybersécurité, limitant ainsi son efficacité en tant que troisième ligne de défense. Pour renforcer la sécurité organisationnelle, il est essentiel de dépasser cette organisation en silos et de promouvoir une gouvernance circulaire, dans laquelle les responsabilités sont partagées et les décisions stratégiques sont co-construites par les différents départements. Une telle gouvernance repose sur une vision systémique de la cybersécurité, intégrant les dimensions financières, humaines et techniques, et mobilisant un réseau de compétences internes et externes pour une réponse adaptative et coordonnée aux risques cyber.

6.1.1.2 La dimension des identités professionnelles : vers une intégration interprofessionnelle

Les identités professionnelles du RSSI et de l'audit interne, ainsi que leurs pratiques, influencent fortement l'organisation de la réponse aux risques cyber. Le RSSI, dont le rôle est souvent réduit à des fonctions techniques ou de sensibilisation, pourrait se voir confier des responsabilités plus stratégiques, à condition de développer ses compétences en gestion des risques et en collaboration interdisciplinaire. Parallèlement, l'audit interne, en tant que troisième ligne de défense, pourrait mieux accompagner le RSSI en développant des compétences en cybersécurité. Cependant, les identités actuelles de ces acteurs freinent cette collaboration, chacun ayant tendance à défendre son propre périmètre de responsabilité. La création d'une culture organisationnelle qui valorise la collaboration interprofessionnelle est ici cruciale. En effet, la cybersécurité n'est pas uniquement une question de technologie mais aussi une question de dynamique d'équipe et d'échange entre expertises. L'instauration d'une culture de sécurité partagée permettrait au RSSI et à l'audit interne de mieux coordonner leurs actions et de mutualiser leurs compétences pour une meilleure réactivité face aux cybermenaces. Cette coopération renforcerait ainsi leur capacité collective à répondre aux menaces tout en respectant les spécificités de chaque identité professionnelle.

6.1.1.3 Vers une gouvernance circulaire pour une gestion renforcée des risques cyber

Les résultats soulignent également l'importance d'une gouvernance circulaire, fondée sur

l’interconnexion des fonctions, la fluidité des échanges et une responsabilité partagée. Dans ce modèle, les décisions en matière de cybersécurité ne relèvent plus d'une seule entité, mais sont distribuées à travers une structure collaborative, où chaque acteur contribue à la résilience globale de l'organisation. Une gouvernance circulaire favoriserait une meilleure articulation des identités professionnelles et permettrait de lever les obstacles juridiques et organisationnels qui freinent actuellement la réponse aux risques cyber. Cette gouvernance intégrée implique une redéfinition des rôles et une clarification des responsabilités pour éviter les chevauchements et les vides juridiques, et pour permettre aux acteurs de la cybersécurité d'exercer pleinement leur rôle. Cela suppose également un engagement de la direction à allouer les ressources nécessaires pour le développement des compétences en cybersécurité, tant pour le RSSI que pour les auditeurs internes. En plaçant le RSSI au centre des décisions stratégiques et en renforçant la compétence de l’audit interne en matière de cybersécurité, la banque peut construire une réponse plus agile et plus résiliente face aux cybermenaces. En conclusion, nos recherches mettent en lumière le besoin de dépasser les modèles organisationnels traditionnels pour favoriser une gouvernance circulaire et intégrée dans la gestion des risques cyber. Une telle approche permettrait de mobiliser les identités professionnelles en vue d’une réponse cohérente, interconnectée et agile face aux cybermenaces.

6.1.2 Une remise en cause des schèmes spécifiques du terrain bancaire libanais

Nous rappelons que le secteur bancaire libanais est en crise monétaire et économique. La gestion de la cybersécurité varie d'une banque à l'autre en raison de l'autonomie, de la diversité organisationnelle, de la taille, de la complexité, de la réglementation, de la perception des risques, de la culture organisationnelle et du leadership différents au sein de ces institutions. Nous avons présenté nos résultats de recherche sur le terrain bancaire libanais suivant trois axes organisationnelle, juridictionnelle et au niveau des identités professionnelles. Désormais, nous n’avons pas pu repérer les identités professionnelles des auditeurs internes et des RSSI sur le terrain bancaire libanais qui est en contexte de crise. Nous rappelons tout d’abord à travers le tableau récapitulatif ci-dessous les éléments probants des résultats ressortis sur le terrain bancaire libanais :

Tableau 31 : les éléments probants des résultats sur le terrain bancaire libanais

Aspect organisationnel	- Les banques libanaises sont autonomes. Dans environnement bancaire libéral, chaque banque est autonome et dispose de sa propre gouvernance et de sa propre stratégie organisationnelle. - Les banques libanaises varient considérablement en termes de taille, de structure et de complexité organisationnelle où chaque banque suit une différente politique pour gérer la cybersécurité. - Chaque banque interprète les réglementations et les directives émises par la Banque du Liban à sa propre en matière de cybersécurité. - Les banques envisagent les risques et des menaces liées à la cybersécurité de manière différente. - La culture organisationnelle et le leadership influencent la gestion de la cybersécurité.
Identités professionnelles	- Pas de résultats au niveau des identités professionnelles vu le contexte compliqué du secteur bancaire libanais en crise.
Aspect juridictionnel	- Les banques libanaises ne priorisent pas le risque de cybersécurité. - Les banques libanaises sont en retard à l'échelle mondiale de cybersécurité par manques de moyens techniques et financières. - Absence d'une agence nationale de prévention et contrôle au niveau national libanais en cybersécurité. - La corruption menace la mise en œuvre de la cybersécurité. - Le contexte sociodémographique entrave la cybersécurité au niveau national libanais. - Manque de collaboration sur le terrain bancaire libanais. - Pénurie d'experts en cybersécurité en plus de leur difficulté d'adaptation aux changements rapides ce d'initiative sur le terrain bancaire libanais en cybersécurité.

Nous avons présenté une synthèse récapitulative des résultats de notre recherche sur le terrain bancaire libanais en matière de cybersécurité. Sur le plan organisationnel, les banques libanaises se distinguent par leur autonomie et leur diversité en termes de taille, de structure et de stratégie organisationnelle. Cette diversité entraîne des approches variées pour la gestion de la cybersécurité, chaque banque interprétant les réglementations de manière différente. De plus, la culture et le leadership au sein de chaque institution influencent significativement la gestion de la cybersécurité. Concernant les identités professionnelles, le contexte complexe et la crise économique du secteur bancaire libanais n'ont pas permis d'obtenir des résultats significatifs sur les identités professionnelles liées à la cybersécurité. Au niveau juridictionnel, les banques

libanaises sont confrontées à plusieurs défis. Elles affichent une faible priorisation du risque de cybersécurité et accusent un retard par rapport aux standards mondiaux, en raison de limitations techniques et financières. Il n'existe pas d'agence nationale dédiée à la prévention et au contrôle de la cybersécurité, ce qui aggrave la situation. La menace de la corruption pèse également sur la mise en œuvre de mesures de cybersécurité.

Par ailleurs, des contraintes sociodémographiques entravent les efforts de cybersécurité à l'échelle nationale. Le secteur bancaire libanais souffre d'un manque de collaboration en matière de cybersécurité, ainsi que d'une pénurie d'experts et de difficultés d'adaptation aux évolutions rapides de ce domaine. Ces résultats soulignent la complexité et les défis uniques auxquels le secteur bancaire libanais est confronté en matière de cybersécurité. Ils mettent en évidence la nécessité d'une approche plus cohérente et coordonnée pour faire face à ces enjeux, en particulier dans un contexte de crise économique et monétaire.

6.1.3 Approches pour surmonter les divergences de priorités en cybersécurité

L’analyse des entretiens a révélé des cas où les identités professionnelles des acteurs de la cybersécurité ont influencé leurs capacités de collaboration et parfois limité leur efficacité. Un exemple, est celui du directeur d’audit qui a évoqué la complexité de sa relation de travail avec le RSSI, citant une divergence de perceptions concernant la gravité et les priorités des menaces de cybersécurité. En effet, les identités professionnelles distinctes de ces acteurs entraînent souvent une différence d’appréciation des risques : là où le RSSI voit une menace technique immédiate, le directeur d’audit peut plutôt évaluer les impacts selon des critères de conformité et de gouvernance à long terme. Cette divergence dans les priorités et les perceptions, bien que compréhensible compte tenu des rôles distincts, peut créer des lacunes dans la réponse organisationnelle aux incidents de cybersécurité. Les décisions cruciales de sécurité sont alors influencées non seulement par les analyses de risque, mais aussi par les biais et les perceptions propres à chaque identité professionnelle. Pour renforcer la collaboration et la réactivité, une approche de formation croisée est proposée, visant à aligner les perceptions des risques entre le RSSI et les autres acteurs, comme le directeur d’audit. Cette formation croisée permettrait aux responsables de comprendre les enjeux propres à chaque rôle et les priorités de leurs collaborateurs, favorisant ainsi une réponse plus homogène et coordonnée.

En outre, la mise en place de sessions régulières d’échanges et de simulations de crise entre le RSSI, les auditeurs et les autres parties prenantes pourrait aider à identifier et réduire les divergences de perceptions en amont. De telles sessions contribueraient également à instaurer

une culture de la cybersécurité intégrée et partagée, où chaque acteur, bien que guidé par son expertise propre, est sensibilisé aux priorités et contraintes des autres services.

6.1.4 Identités professionnelles et collaboration RSSI-Auditeurs internes : un levier pour la cybersécurité bancaire

Les identités professionnelles des RSSI et des auditeurs internes, dans les banques libanaises et françaises, offrent une perspective unique sur les défis de la cybersécurité. Cette compréhension approfondie aide à renforcer la posture de sécurité globale des banques en répondant de manière proactive aux exigences de cybersécurité.

En analysant l'interaction de ces deux professions, nous abordons la cybersécurité sous plusieurs aspects : expertise technique, gestion des risques, conformité réglementaire, gestion des incidents et sensibilisation à la sécurité. Cette perspective offre une vue holistique de la manière dont ces acteurs, par leurs rôles et compétences spécifiques, contribuent à la sécurisation des systèmes bancaires.

L'étude des identités professionnelles permet de comprendre comment les auditeurs internes et les RSSI gèrent des enjeux spécifiques, comme la protection des données financières sensibles et la prévention des fraudes. Leur collaboration, influencée par leurs identités professionnelles, est cruciale pour répondre aux attentes des parties prenantes.

Nous constatons que l'ANSSI impose des réglementations strictes, notamment au groupe BPCE et à la BPVF. Les auditeurs internes veillent au respect de ces réglementations, tandis que les RSSI en assurent l'application. Leur identité professionnelle influence donc leur démarche de conformité, ainsi que leur capacité à gérer les risques financiers associés aux failles de sécurité. En cas d'incident, le RSSI doit réagir rapidement, et son identité professionnelle conditionne son efficacité dans ces situations de crise.

Face à des identités professionnelles rigides, nous proposons plusieurs leviers pour encourager une meilleure collaboration à travers :

- Des formations croisées et ateliers collaboratifs en sensibiliser les RSSI aux bénéfices apportés par les auditeurs internes ;
- Un renforcement des compétences techniques des auditeurs internes en développant leur expertise en cybersécurité pour crédibiliser leur rôle auprès des RSSI.
- Des politiques et procédures claires en définissant précisément les rôles et les responsabilités, et en établissant des canaux de communication structurés.
- Un soutien actif de la direction qui favoriser une culture d'ouverture et d'intégration

entre les différentes fonctions.

Conclusion intermédiaire

La partie 6.1 nous a permis d'examiner en détail les résultats de la recherche sur la cybersécurité dans le secteur bancaire, en mettant l'accent sur l'identité professionnelle des auditeurs internes et des RSSI. Cette partie souligne l'importance de comprendre comment ces acteurs influencent la sécurité informatique dans le contexte spécifique des banques.

L'approche de l'identité professionnelle fournit des informations complètes pour l'analyse de la cybersécurité car elle prend en compte les compétences, les rôles, les responsabilités et les valeurs de ces professionnels. Cette approche a permis de mettre en évidence les défis et les opportunités associés à la gestion de la cybersécurité, tant au niveau organisationnel que juridictionnel.

La discussion met également en lumière les différences entre les secteurs bancaires français et libanais en matière de cybersécurité. En France, l'audit interne joue un rôle clé en tant que troisième ligne de défense, tandis que les RSSI manquent parfois d'expertise technique en cybersécurité. Au Liban cependant, la diversité des banques et la crise économique créent des différences importantes dans la gestion de la cybersécurité.

Nous soulignons la nécessité d'une approche plus cohérente et coordonnée pour résoudre les problèmes de cybersécurité dans le secteur bancaire, en particulier au Liban. Développer les compétences techniques, clarifier les rôles et les responsabilités et sensibiliser aux enjeux de cybersécurité sont essentiels pour garantir la sécurité des données financières et la confiance des parties prenantes.

La cybersécurité représente un défi organisationnel autant que technique, où les identités professionnelles formées peuvent renforcer des structures en silos, limitant ainsi l'efficacité globale face aux cybermenaces. Pour améliorer la gestion des risques cyber, il est primordial de remettre en question cette gouvernance en silos et d'adopter une approche intégrée et collaborative. Cela nécessite de promouvoir une culture de collaboration interdisciplinaire, de créer des équipes transversales et de renforcer les compétences techniques et de gestion au sein des départements. En développant des formations croisées et des programmes de sensibilisation, et en favorisant une coopération étroite entre tous les acteurs, les banques libanaises et françaises pourront mieux anticiper et répondre aux cybermenaces. La transition vers une gouvernance plus holistique demeure essentielle pour renforcer la résilience du secteur bancaire face aux défis actuels

6.2 Vers une gouvernance circulaire

Les banques doivent dépasser la culture de défense traditionnelle pour adopter une structure de cybersécurité plus prospective et agile, capable de répondre aux menaces émergentes. Nos analyses ont mis en évidence un conflit juridictionnel récurrent entre les RSSI et les auditeurs internes, en raison notamment de l'absence d'une expertise partagée sur les enjeux techniques de la cybersécurité. Les RSSI exploitent souvent le manque de compétences des auditeurs internes dans ce domaine spécifique, sous-estimant ainsi leur rôle dans la lutte contre les cyberattaques. Nous avons collecté des données en trois phases :

- Observation des organisations bancaires libanaises et de leurs activités quotidiennes ;
- Quarante entretiens biographiques sur le terrain bancaire ;
- Huit entretiens de discussion libre avec des leaders en cybersécurité, menés dans des cabinets d'audit internationaux (Big Four) et des agences nationales de sécurité informatique en France, afin de compléter nos observations sur les pratiques bancaires et identifier les lacunes.

Nous détaillons ici les contextes des interviewés et les résultats relatifs à la cybersécurité.

6.2.1 Réformes pour une cyber sécurité plus efficace dans le secteur bancaire

Il est paradoxal que les décisions en matière de cybersécurité soient souvent prises par des managers ne disposant pas d'une expertise technique suffisante. Pour remédier à cela, un modèle de gouvernance participative est essentiel, impliquant toutes les parties prenantes : experts en sécurité informatique, managers, auditeurs internes, utilisateurs finaux et cadres dirigeants. Une telle approche favorise une communication ouverte, une collaboration renforcée et une responsabilité partagée, indispensables pour garantir la sécurité organisationnelle des banques (Trouchaud, 2018).

Le rôle du RSSI au sein du groupe BPCE illustre cette nouvelle dynamique : il doit être à la fois un leader et un consultant interne, offrant son expertise pour éclairer la prise de décisions stratégiques. L'adoption d'une gouvernance circulaire dans ce cadre permet d'optimiser la gestion des risques cyber. Cela implique de concilier expertise technique et objectivité professionnelle, en tenant compte de l'absence d'une identité professionnelle clairement définie dans certains contextes, comme celui du Liban. Pour une cybersécurité bancaire efficace, une collaboration renforcée entre les auditeurs internes et les RSSI est cruciale. Cela nécessite de clarifier les rôles de chacun, d'améliorer la communication et d'encourager un échange

d'informations fructueux, tout en valorisant l'expertise de chaque fonction. La formation continue et la participation à des réseaux d'experts sont également des leviers essentiels pour renforcer l'efficacité des RSSI (Trouchaud, 2018).

6.2.2 Perspectives des leaders de la cybersécurité sur la gouvernance circulaire

Les entretiens réalisés qui font partie de la troisième vague ont pour but de saturer nos résultats de recherche en complétant les données avec huit entretiens de discussion libre avec les leaders de la cybersécurité en France. Nous présentons une description de nos interviewés à travers le tableau ci-dessous :

Tableau 32 : les leaders mondiaux de la cybersécurité

Personne interviewée	Compte Rendu
Gerard Peliks	- Président de l'association CyberEdu (créée par l ANSSI), - Président de l'atelier sécurité et VP de Forum ATENA, - Ingénieur diplômé, il a travaillé pour Airbus Défense & Space Cybersécurité. - Cyberdéfense auprès du citoyen en organisant des présentations pédagogiques de tous niveaux et en écrivant des articles de vulgarisation sur les dangers du cyberespace et sur les contre-mesures pour en diminuer les risques. - Lieutenant-colonel de gendarmerie dans la Réserve Citoyenne de Cyberdéfense (DGGN) et membre du Conseil d'administration de l'association des Réservistes du Chiffre et de la Sécurité de l'information (ARCSI), il co-organise, sur une base mensuelle, les Lundi de la cybersécurité. - Chargé de cours sur la cybercriminalité / cybersécurité dans des mastères d'écoles d'ingénieurs, en particulier à l'institut Mines-Télécom, et directeur adjoint du MBA Management de la Sécurité des Données Numériques de l'institut Léonard de Vinci.
Philippe Lavault	- Chef des Ressources extérieures de l'ANSSI. - Membre au ministère des Armées. - Enseignant au département de recherche sur les Menaces Criminelles Contemporaines à Parsi 2. - Il a exécuté la refonte du système de gouvernance tripartite de la réserve cyber, en collaboration avec le COMCYBER et la DGGN. - Il a créé un club de réflexion atypique et multidisciplinaire, l'AGORA41, qui après une année de gestation, commence à trouver une vitesse de croisière et un seuil de productivité prochain. - Auditeur de la seconde session nationale « Souveraineté numérique et Cybersécurité » de l'INHESJ – IHEDN. - Directeur d'un groupe de travail « cyber » de l'école de Guerre Economique EGE.

Jean-Louis Desvignes	- Président de l'ARCSI (Association des réservistes du chiffre et de la sécurité de l'information). - Ancien chef du service central de la sécurité des systèmes d'information et actuel commandant de l'Ecole supérieure et d'application des transmissions (l'ESAT, chargée de former les informaticiens de l'armée). - Responsable du service central de la sécurité des systèmes d'information, le bureau, dépendant du Premier ministre, qui doit appliquer la récente réglementation sur le chiffrement (agrément, enregistrement, etc.).
Vincent Maret	- Associé, Responsable du pôle Cybersécurité et Protection des données personnelles au cabinet KPMG. - 20 ans d'expérience en conseil et en audit dans les domaines de la cybersécurité et de la protection des données personnelles, sur des sujets opérationnels, de technologie et de gouvernance.
Imad el Baraka	- Associé Risk Advisory, en charge des activités de cybersécurité à Deloitte. - Managing Partner spécialiste du Cyber Risk au sein de Deloitte France et Francophone Afrique.
Philippe Trouchaud	- Associé chez PWC, responsable du développement des activités de cybersécurité pour la région EMEA. - Consultant Expert en transformations liées aux technologies et fort d'une expérience de plus de 20 ans. - Auteur et conférencier.
Ludovic Lecompte	- RSSI et DPO d'Innova Software. - Consultant et Professeur à l'institut supérieur du commerce de Paris ISC.
Benoît Fuzeau	- Responsable de la Sécurité des systèmes d'information à la CASDEN Banque populaire. - Président du Club de la sécurité de l'information français (Clusif).

Nous notons le contexte riche de ces différents acteurs dans le domaine de la cybersécurité en France. De par leur expérience en cybersécurité, ils sont des experts dans ce domaine et méritent cette nomination de *Cybersecurity Leaders*. Leur expérience solide dans le domaine de la cybersécurité leur permet de proposer une approche novatrice qui redéfinit la manière dont nous percevons la gestion de la cybersécurité au niveau organisationnel. Nous présentons les résultats de recherche issues de ces entretiens qui viennent saturés nos résultats de recherche trouvés sur le terrain bancaire français et libanais. Une nouvelle approche, que nous allons nommer *gouvernance circulaire*, introduit de nouvelles normes et pratiques pour les RSSI et les auditeurs internes afin d'assurer la cybersécurité.

6.2.3 Analyse et présentation des résultats sur la gouvernance circulaire en cybersécurité

Nous présentons les résultats de recherche issues de ces entretiens à travers le tableau récapitulatif suivant :

Acteur	Positionnement traditionnel du RSSI	Nouveau Positionnement du RSSI	Rôle traditionnel du RSSI	Nouveau rôle du RSSI	Compétences traditionnelles	Nouvelles compétences	Trois lignes de défense	Nouvelles perspectives		
Gerard PELIKS	Il ne doit pas dépendre de la DSI. C'est un métier traditionnel qui n'a pas les juridictions nécessaires en cybersécurité.	Etre au centre de l'organisation, lié à la DG, direction des risques, DPO, SOCLE…	Le RSSI est borné, il ne comprend pas les lois. Il est très technique et ne sait pas exprimer ses besoins au près de la DG.	Il faut qu'il soit le chef d'orchestre. Il faut qu'il possède des compétences juridiques, éthique, informatique, sociale et financière.	Le RSSI est technique seulement. Il est considéré comme Pompier de la cybersécurité.	Il doit développer des compétences juridiques, éthiques, sociales et financières pour savoir communiquer avec tous les postes et exprimer ses besoins.	Le Socle ne suffit pas pour se défendre contre les attaques. L'audit interne doit se penser dans une optique métier.	Le risque de sous traitance de la cybersécurité en externe est garanti par les SLA au niveau juridique. (Security Level Agreements)	La cybersécurité est un problème collectif. Il faut agir en cerveau partagé collectif, collaborer contre les attaques.	Création d'un poste de DPO Data Protection Officer qui soit responsable de la protection des données et qui dépend du RSSI.
Imad El BARAKA	Il ne doit pas être attaché à la DSI. Il n'est pas rattaché à la direction des risques et ça pose un problème de dépendance.	Il doit être rattaché à la direction des risques et à la DG.	Il est limité à un rôle de contrôle et de supervision.	Il doit en plus définir la stratégie de cybersécurité.	Le RSSI doit avoir une connaissance métier.	Le RSSI doit en plus avoir une vision sur les risques.	Respecter les lignes de défenses en ayant une équipe opérationnelle technique, RSSI lié à la DG et direction des risques et l'audit interne en 3ième niveau	Accepter qu'on a pas les experts en Interne et qu'ils n'ont pas les qualités requises en cybersécurité.	Accepter les expertises externes managériales qui apportent leurs expériences et expertises : Il a déjà fait la mission il connait les contraintes.	Création d'un poste DPO pour mieux gérer la cybersécurité.
Jean-louis DESVIGNES	Il est mal placé parce qu'il est soumis à la DSI.	Il faut qu'il soit branché directement à la DG.	RSSI joue le rôle de chasseurs en oubliant d'établir une stratégie de défense.	Il doit avoir plus d'autorité sur la prise de décision sur la gouvernance et stratégie de cybersécurité.	Approprié négatif que le RSSI doit avoir seulement des compétences techniques.	Le RSSI doit avoir des compétences plus managériales même que techniques et à savoir prendre les décisions stratégiques.	Les trois lignes de défenses sont primordiales pour obtenir une cybersécurité efficace.	Accepter d'externaliser et de faire recours à des prestataires externes parce qu'on n'a pas les profils en interne.	Parler d'un cercle vertueux, un réseau de défense et une culture de défense collective.	Partager un reporting vitale entre les grandes entreprises de tous les cyberattaques qui va servir de preuve et de documentation.
Vincent MARET	Le positionnement du RSSI en banque est contraint. Pas de ligne de défense, le RSSI est rattaché à la DSI.	Il faut qu'il soit rattaché à la direction des risques. Il faut qu'il cartographie les risques.	La cybersécurité n'était pas un sujet de Top management. Le RSSI seul faisait face aux cyberattaques. Il ne doit pas se laisser faire des tâches opérationnelles (Ne pas être en 1ièr niveau) ne pas gérer les antivirus.	Il doit mettre en place un ROAD MAP, planifier la cybersécurité qui est traité comme un sujet très technique.	Les auditeurs internes ne savaient pas faire. Ils sous traitaient en externe soient ils faisaient confiance aux RSSI. Leur indépendance est menacée puisque les RSSI réalisaient les audits techniques de sécurité informatique et partageaient les tâches avec les auditeurs internes.		Règlementation sous trois niveaux où les rôles sont clairs : Première ligne de défense les responsables informatiques sont en surveillance et en action corrective. Deuxième ligne de défense les RSSI définissent les règles de sécurité, surveillent et réalisent les tests d'intrusion. Troisième ligne de défense les auditeurs internes en rôle de gouvernance vérifient que tous sont bien.	L'audit de cybersécurité réalise un diagnostic, un rôle de conseil en s'assurant que les politiques, les procédures et les outils en sécurité informatique sont bien suivis.	La cybersécurité est un sujet stratégique, politique et technologique où l'audit est un audit de gouvernance qui réalise des tests d'intrusion.	Mettre en place un SOC qui assiste le RSSI dans la gestion de la cybersécurité.
Philippe TROUCHAUD	Autre que son mal positionnement au sein de l'organisation, le RSSI est souvent placés dans les grilles de rémunération informatiques.	Le RSSI se positionne comme consultant interne au cœur de l'organisation. Il faut qu'il soit placé à un niveau exécutif.	Le RSSI ne doit pas être considéré comme une sorte de garde-barrière qui administre les firewalls. Il ne doit pas être comme un censeur…	Le RSSI sera un accompagnateur dans la prise de risque comme un guide de montagne…	Le RSSI possèdait un rôle coercitif dans l'organisation. Il était en chasse à la recherche du dernier pare-feu.	Le RSSI devient un RSSI communiquant qui développe la dimension stratégique de son poste. Il doit posséder des quasi militaires de gestion de crise.	Le RSSI doit gérer en plus de son périmètre d'entreprise celui de ses partenaires.	En réinvestissant l'approche des riques, le RSSI permettra aux directions générales de mieux définir leurs stratégie cyber. C'est l'enjeu d'une collaboration et d'une gouvernance circulaire.	Le manque de compétences informatiques en cybersécurité chez le RSSI demeure une contrainte au niveau des ressources humaines qui n'arrivent pas recruter le talent ou à le valoriser au sein de l'organisation.	Une nouvelle dimension deu management du cyberrisque doit s'accompagner avec la mise en place d'une gouvernance circulaire…
Philippe LAVAULT	Le RSSI est souvent mal placé près du DSI ce qui n'est pas bon.	Il doit être au cœur de l'organisation, plus proche du directeur des risques.	RSSI n'a pas de plan de carrière. Il a un contexte informatique et agit à travers la surveillance et la sensibilisation des employés.	Il faut envisager la cybersécurité d'une manière holistique et détachée.	Le RSSI a le nez dans le réseau, il ne sait pas exprimer ses besoins.	Il doit avoir des compétences managériales et savoir exprimer son besoin auprès des directeurs.	L'ANSSI vise la cybersécurité au niveau national et amène les organisations à respecter les rôles et les recommendations à travers les trois niveaux de défense.	La France ne dispose pas des même compétences en cybersécurité que la Russie, les états-unis et la Chine.	L'audit interne doit dépasser son rôle de gendarme permanent de la sécurité et agir plus sur la sensibilisation et que les procédures de sécurité sont bien respectées.	Toutes les entreprises ne considèrent pas la cybersécurité de la même manière. Il faut introduite une nouvelle fonction de cybersécurité en bien définissant les rôles.
Benoit FUZEAU	Les indicateurs de performance cybersécurité sont omniprésents dans l'activité des RSSI : Cyber Rating pour l'évaluation des fournisseurs, Cyber score de services web pour augmenter la confiance des utilisateurs.	Cette cartographie du risque global est difficile à obtenir si la SSI reste coincée sous le plafond de verre de la DSI.	Les RSSI sont en effet à la recherche de nouveaux moyens de faire passer leurs messages, fatigués qu'ils sont de voir leurs alertes et leurs actions de sensibilisation régulièrement mises en échec par de mauvaises pratiques.		Le RSSI possède dans son cœur de métier originel, technique par nature.	Le RSSI joue le rôle d'un chef d'orchestre centré sur la protection de l'information.	Depuis plusieurs années, les grandes entreprises ont ainsi vu le RSSI (groupe) se rapprocher de la direction, pour assurer un rôle de conseil et d'orientation, bien loin de sa réputation de pur technicien.	Rapprocher les équipes de cybersécurité des autres métiers de l'entreprise pour renforcer la sensibilisation sur le sujet.	La cybersécurité est partie prenante de l'organisation, elle doit davantage s'impliquer dans les processus organisationnels pour participer aux arbitrages.	Créer des tableaux de bord sécurité informatique : les indicateurs servent à l'amélioration continue de la sécurité et dans la communication avec la direction des organisations.
Ludovic LECOMPTE	Le RSSI est mal positionné dans l'organisation. Il est toujours attaché à la DSI.	Le RSSI doit être lié à la direction générale et à la direction des risques. Il ne doit pas dépendant de la DSI.	Le RSSI n'est pas aisé. Les ressources et budgets sont très limités et il faut sans cesse réaliser des optimisations sur les coûts de la maîtrise des risques.	Le RSSI doit nécessairement soutenir une "Roadmap" sécurité et des objectifs sur plusieurs année.	Le RSSI se limite à des compétences techniques et présente des faibles compétences en Leadership.	Le RSSI doit acquérir de nouvelles compétences techniques, juridiques, financières et managériales.	77% des plans d'audit incluent la cybersécurité. L'audit interne agit en 3ième ligne de défense.	Le programme de Mentorat du CESIN aide les RSSI. La confrontation des pratiques dans différents domaines d'activités, des entreprises de taille variable, avec des enjeux et objectifs parfois très différents, est extrêmement riche.	Obtenir la certification ISO27001 pour implémenter un système de management de la sécurité de l'information.	Plus de budgets en cybersécurité, les dirigeants sont responsables aussi et confie aux opérateurs et RSSI la cybersécurité et à l'audit interne de s'assurer que les choses sont bien définis et les risques sont cartographiés.

Figure 21 : les résultats de recherche issue des entretiens avec les leaders de la cybersécurité

Source : élaboration personnelle

Notre analyse des entretiens avec les leaders de la cybersécurité repose particulièrement sur les enjeux organisationnelles, juridictionnelles ainsi que les identités professionnelles des auditeurs internes et des RSSI dans le secteur bancaire. Ces résultats enrichissent nos résultats de recherche et propose une nouvelle gestion de la cybersécurité bancaire.

6.2.3.1 Le repositionnement stratégique du RSSI face aux défis organisationnels en cybersécurité

Les résultats des entretiens montrent une remise en question du statut actuel du RSSI, souvent perçu comme dépendant de la direction des systèmes d'information (DSI). Un repositionnement stratégique du RSSI est nécessaire : celui-ci doit être placé au cœur de l'organisation, avec une coopération renforcée avec la direction générale (DG), la direction des risques et d'autres acteurs clés. Cette réorientation vise à renforcer son rôle dans la gestion des risques de cybersécurité, à encourager une prise de décision plus proactive et à lui offrir une plus grande autonomie. Le RSSI doit évoluer d'un rôle technique vers un rôle stratégique, impliqué dans la définition et la mise en œuvre de la stratégie cyber.

6.2.3.2 La nécessité des trois lignes de défense

Le modèle des trois lignes de défense demeure fondamental pour garantir une cybersécurité efficace dans les organisations bancaires. La première ligne comprend les opérateurs chargés de la surveillance et de la réaction aux incidents. La deuxième ligne regroupe les RSSI, responsables de la définition des règles de sécurité. Enfin, la troisième ligne, incarnée par les auditeurs internes, assure un rôle de gouvernance et de vérification. Ce modèle est essentiel pour structurer les responsabilités et éviter les chevauchements de compétences. L'intégration de la cybersécurité dans les plans d'audit, aujourd'hui appliquée par 77 % des banques, souligne l'importance croissante de l'audit interne dans la cybersécurité.

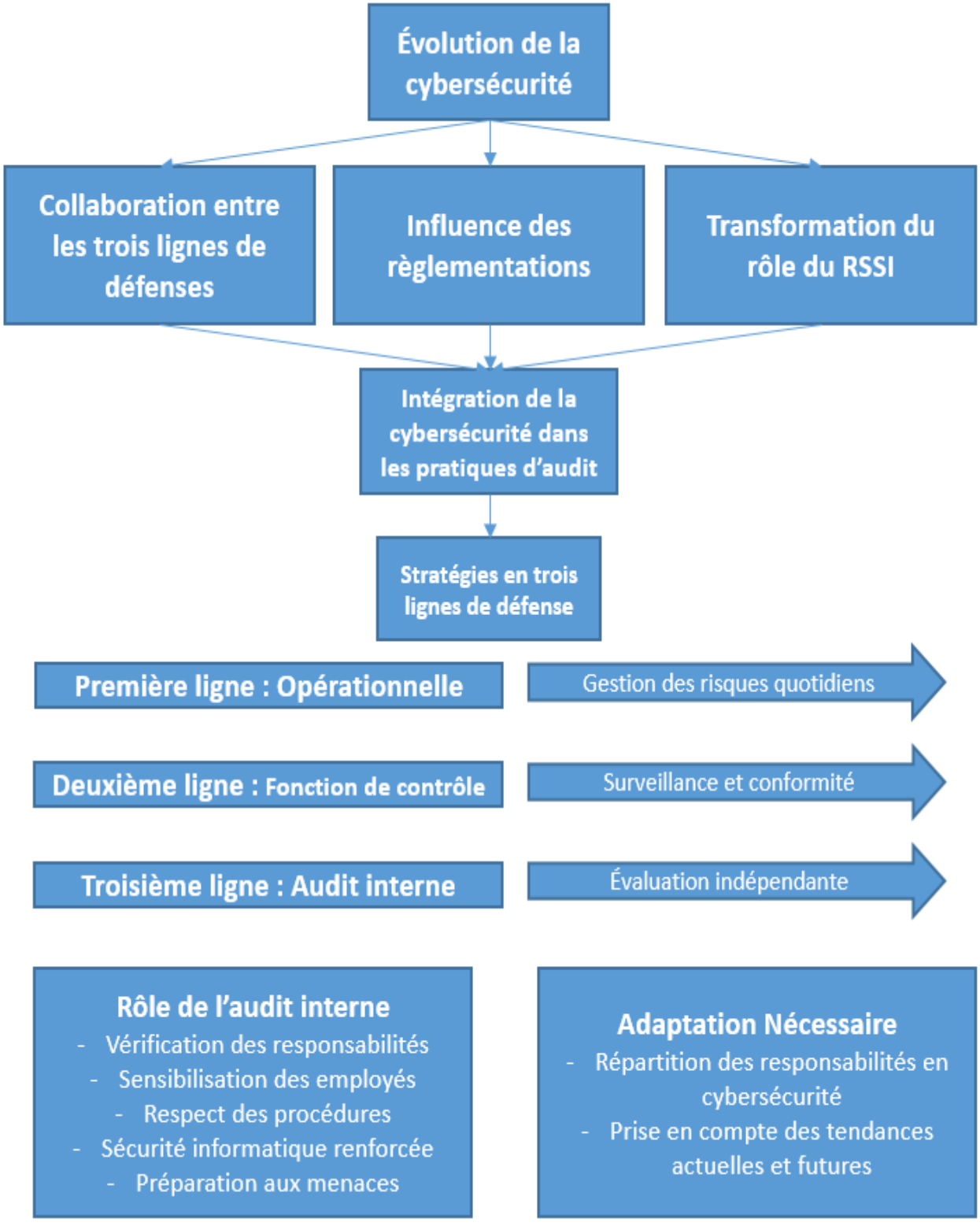


Figure 22 : modèle intégré de cybersécurité dans le secteur bancaire : interaction entre les trois lignes de défense et rôle de l'audit interne

Source : élaboration personnelle

6.2.3.3 Vers une identité négative du RSSI

Notre analyse sur les commentaires des leaders de la cybersécurité concernant l'identité professionnelle du RSSI met en évidence des défis et des perceptions qui sont au cœur de la profession. Au niveau de la limitation technique et de la compréhension des lois, le RSSI peut être excessivement axé sur les aspects techniques de la cybersécurité, ce qui peut limiter sa compréhension des dimensions juridiques et réglementaires. Cette limitation peut rendre difficile la communication de ses besoins et de ses préoccupations à la direction générale. Nous notons que la cybersécurité n'a pas toujours été une priorité du Top Management (Même constat dans le rapport d'audit de la BPVF en 2018), ce qui a laissé le RSSI seul face aux cyberattaques. Le RSSI s'implique dans des tâches opérationnelles de bas niveau et gérer directement les antivirus. Le RSSI doit éviter le rôle de garde-barrière et ne doit pas être vu comme un simple administrateur de pare-feu ou un censeur, mais plutôt comme un acteur stratégique dans la gestion des risques de cybersécurité. Le RSSI est parfois perçu comme étant principalement axé sur le contrôle et la supervision, ce qui peut limiter sa capacité à élaborer une stratégie de défense proactive. Ils se concentrer sur la chasse aux menaces au détriment de l'établissement d'une stratégie globale de défense, ce qui peut entraîner des lacunes dans la sécurité. Il est perçu aussi comme pompier de la cybersécurité en intervenant en première en urgence lors d'incidents.

La contrainte budgétaire nuit son identité professionnelle. Il fait face à des ressources et à des budgets limités, ce qui nécessite une optimisation constante des coûts liés à la gestion des risques.

Comme nos résultats de recherche sur le terrain bancaire français le montrent aussi, l'identité professionnelle d'un RSSI est perçue de manière négative en raison de certains stéréotypes ou de préjugés associés à ce rôle. Nous validons qu'ils sont vu comme des techniciens obsédés par les détails techniques de la cybersécurité, incapable de communiquer efficacement avec des non-initiés ou la direction générale. Cette perception a créé une barrière entre le RSSI et les auditeurs internes au niveau de la BPVF. (RSSI Geeks…)

Nous retenons l'aspect réactionnaire plutôt que proactif du RSSI. (Rapport d'audit interne 2018 BPVF)

Dans ce sens, l'identité du RSSI est perçue comme réactive plutôt que proactive, se concentrant davantage sur la gestion des incidents que sur la prévention des menaces. En synthèse, l'identité professionnelle d'un RSSI est complexe et en constante évolution dans la gestion traditionnelle de la cybersécurité.

6.2.3.4 L’évolution de l’identité professionnelle du RSSI

Les commentaires des leaders en cybersécurité soulignent les défis auxquels sont confrontés les RSSI et leur rôle croissant dans la gestion des risques de cybersécurité au sein de leurs organisations. Ces réflexions mettent en évidence une évolution positive de l'identité professionnelle du RSSI, qui tend à se transformer en un rôle de plus en plus stratégique et holistique. Cette transformation repose sur l’élargissement des compétences nécessaires pour exercer cette fonction. Le RSSI doit désormais posséder une palette diversifiée de compétences : au-delà des compétences techniques, il doit aussi maîtriser des aspects juridiques, éthiques, sociaux et financiers, illustrant ainsi la complexité croissante du domaine de la cybersécurité.

Cette évolution indique que le RSSI doit jouer un rôle crucial dans la définition et l'élaboration de la stratégie de cybersécurité de l'organisation. Il devient ainsi un contributeur stratégique à la protection des actifs numériques de l'entreprise. Les commentaires recueillis insistent sur la nécessité de renforcer l’autorité du RSSI en matière de gouvernance et de stratégie. Le RSSI doit désormais disposer d'une place à la table des décisions stratégiques, étant impliqué activement dans les choix relatifs à la sécurité. En ce sens, l'image du RSSI comme guide de gestion des risques – comparable à celle d'un guide de montagne – reflète bien son rôle consultatif et d'accompagnement dans la prise de décisions liées à la cybersécurité.

En somme, le RSSI doit continuer à adapter son identité professionnelle pour répondre aux défis d’un paysage de plus en plus complexe. Il doit allier compétences techniques, juridiques et stratégiques, tout en équilibrant les rôles de supervision et de sensibilisation. Nos résultats de recherche orientent l’identité professionnelle du RSSI vers un rôle plus stratégique et influent, reflet d’une reconnaissance croissante de l'importance de la cybersécurité dans le secteur bancaire. Le RSSI devient ainsi un acteur central dans la protection des actifs numériques et dans la prise de décisions critiques pour la cybersécurité.

6.2.3.5 L’aspect juridictionnel fait face à plusieurs défis

Sur le plan juridictionnel, nos analyses des discours des leaders de la cybersécurité révèlent plusieurs défis relatifs à la répartition des responsabilités et à l’indépendance des acteurs au sein des organisations. Les réflexions des experts soulignent la complexité du rôle du RSSI, souvent perçu comme un acteur technique focalisé principalement sur les aspects techniques de la sécurité, un « pompier de la cybersécurité ». Toutefois, certains estiment que le RSSI doit élargir son champ de compétences pour mieux comprendre et gérer les risques globaux de l'organisation.

Certains commentaires font également ressortir des préoccupations concernant l'indépendance des auditeurs internes. Ceux-ci, en raison de leurs compétences techniques limitées dans le domaine de la cybersécurité, peuvent être amenés à sous-traiter cette expertise ou à s'appuyer sur les RSSI pour réaliser les audits techniques. Cela pose la question de leur capacité à exercer pleinement leur rôle d'audit indépendant. Parfois, les RSSI réalisent eux-mêmes ces audits techniques de sécurité, ce qui peut interroger leur indépendance, puisqu'ils sont également responsables de la mise en œuvre des mesures de sécurité. Cette situation génère des tensions potentielles sur le plan de la gouvernance et de la conformité.

Nos recherches montrent que le conflit entre les compétences techniques du RSSI et son aptitude au leadership est un enjeu majeur. Les commentaires suggèrent que certains RSSI se concentrent excessivement sur les aspects techniques au détriment du développement de compétences managériales et stratégiques. Le rôle du RSSI dans la gestion de la cybersécurité, ainsi que dans la prise de décisions stratégiques, gagnerait à être mieux défini et à s'aligner sur les objectifs globaux de l'organisation.

6.2.3.6 Vers une juridiction plus élargie

Nos analyses des propositions des leaders de la cybersécurité concernant la gouvernance et la gestion de la cybersécurité révèlent plusieurs recommandations visant à améliorer l'efficacité du RSSI dans son rôle. Ces recommandations mettent l'accent sur l'aspect juridictionnel et sur la nécessité pour le RSSI d'élargir ses compétences à des domaines tels que le juridique, l'éthique, le social et le financier. Ces compétences transversales sont essentielles pour faciliter la communication avec les autres départements et pour exprimer clairement les besoins en matière de cybersécurité.

Il est impératif pour le RSSI de développer une vision globale des risques, dépassant les seuls enjeux techniques. L'approche doit être stratégique : le RSSI doit être en mesure de communiquer de manière claire et précise les enjeux et recommandations de cybersécurité aux dirigeants, et d'aligner les actions de sécurité avec les objectifs globaux de l'entreprise. En plus de son expertise technique, le RSSI doit être un communicateur efficace, capable de transmettre des informations stratégiques à la direction. Ses compétences en gestion de crise et en présentation sont désormais des atouts clés.

Le RSSI devient ainsi un véritable chef d'orchestre, coordonnant les efforts à tous les niveaux pour assurer la sécurité de l'information. Afin de rester compétitif dans le secteur de la cybersécurité, il doit continuer à acquérir de nouvelles compétences, tant techniques que managériales. Cela inclut une compréhension approfondie des enjeux juridiques, financiers et

organisationnels. En conclusion, nous affirmons que le RSSI doit développer un large éventail de compétences et prendre des décisions plus stratégiques. Cette évolution renforcera ses capacités à gérer la cybersécurité de manière proactive, tout en garantissant une communication fluide avec toutes les parties prenantes. Une approche plus intégrée et stratégique de la cybersécurité est essentielle pour protéger l'entreprise contre les perturbations numériques et assurer une gouvernance efficace.

6.2.4 Convergence des résultats du terrain bancaire français avec les perspectives des leaders en cybersécurité

Les résultats présentés sur le terrain bancaire français et libanais complète les commentaires et analyses exposés par les leaders de cybersécurité au niveau organisationnelle (Positionnement contraint du RSSI), au niveau de l'identité professionnelle (RSSI Geek) et au niveau juridictionnel (Absence d'expertise et de compétence informatiques)

La BPVF adopte une gouvernance verticale, un modèle hiérarchique traditionnel dans lequel les décisions sont prises par une personne ou un groupe de personnes au sommet de la hiérarchie. Le RSSI se limite au rôle de sensibilisation des collaborateurs et de la réunion de la cellule de crise en cas de cyberattaque. Il fait le lien entre les opérateurs informatiques et la cellule de crise afin que les décisions stratégiques soient menées après par la direction générale. Dans ce sens, les responsables informatiques confirment l'observation d'un rôle limité du RSSI en cybersécurité.

En cybersécurité, les décisions sont prises par les managers qui ne connaissent pas les risques cyber. Un nouveau modèle de gouvernance participative doit naitre où les décisions sont prises par toutes les parties prenantes d'une organisation, y compris les experts en sécurité informatique, les managers, les auditeurs internes et les utilisateurs finaux et les cadres. Le modèle implique une communication ouverte, une collaboration et une responsabilité partagée pour la sécurité organisationnelle de la banque. Selon le rapport d'audit publié en 2022, nous avons observé que la BPCE débute les premiers pas vers une nouvelle gouvernance de la cybersécurité en adoptant une approche plus globale de la sécurité de l'information qui couvre l'ensemble de l'organisation y inclus la BPVF. Nous soulignons que cette approche doit être soutenue par une culture de la sécurité qui encourage la participation active de tous les employés, les managers jusqu'aux utilisateurs finaux, en passant par les responsables de la sécurité informatique. Dans ce sens, la BPCE commence à mettre en place un comité de sécurité de l'information composé de représentants de toutes les parties du groupe qui se réunissent

régulièrement pour discuter des risques de sécurité et des stratégies de prévention. Ce comité est géré par le responsable de la sécurité des systèmes d'information groupe RSSI-G.

La fonction de RSSI doit acquérir de nouvelle juridiction où le RSSI se rattache directement à la direction générale de la banque à la place de la direction informatique et plus proche des directions des risques. Il doit avoir des compétences plus managériales même que technique à savoir prendre les décisions stratégiques importantes pour protéger les données les plus sensibles de la banque.

6.2.5 Une cybersécurité collective, humaine et raisonnée

Les leaders de la cybersécurité ont proposé une nouvelle approche pour mieux gérer la sécurité informatique au sein de l'organisation. Nous présentons une synthèse récapitulative de leurs postulats, tout en examinant les défis posés par les identités professionnelles déjà établies qui pourraient résister aux changements nécessaires pour une mise en œuvre efficace de cette nouvelle approche.

6.2.5.1 L'externalisation sous garantie juridique : les SLA en cybersécurité

La sous-traitance de la cybersécurité à des prestataires externes spécialisés doit s'établir à travers un *Service Level Agreements* (SLA) solide qui garantit un niveau de sécurité convenu et protège les données sensibles contre tout accès non autorisé.

Le SLA est défini comme un contrat entre un fournisseur de services et ses clients qui documente les services que le fournisseur fournira et définit les normes de service que le fournisseur est tenu de respecter (Rosencrance, 2021).

Nos interprétations des entretiens soulignent que l'ANSSI préconise des références au niveau nationale pour sélectionner les prestataires spécialisés en cybersécurité. Donc la sous-traitance est règlementé par l'ANSSI à travers les SLA ce qui permet de définir clairement les attentes et les objectifs à travers des normes et des indicateurs de performance précis tels que les temps de réponse en cas d'incident, les niveaux de disponibilité des services, et les mesures de sécurité spécifiques. Les SLA décrivent en détail les rôles et les responsabilités y compris les mesures de sécurité spécifiques que le prestataire doit mettre en œuvre. Elles incluent des clauses spécifiques sur la sécurité des données, telles que la protection contre les intrusions, la gestion des vulnérabilités et les procédures en cas de violation de données. Nous notons que ces garanties prouvent que la cybersécurité est une priorité pour le sous-traitant.

Au niveau des pénalités, les SLA introduisent des pénalités en cas de non-respect des engagements de sécurité ou d'autres aspects du contrat. Nous signalons que les SLA doivent

être révisés périodiquement pour s'adapter à l'évolution des menaces et des besoins de chaque organisation.

La conformité à l'ANSSI est attestée par la qualification d'un prestataire de service. Elle évalue la capacité d'un prestataire de services à long terme et lui permet de démontrer sa capacité à reconnaître et gérer les menaces et les risques afin de répondre aux exigences des référentiels métiers. De plus, l'ANSSI exige le recours à l'usage des SLA.

Nous admettons que ces SLA résolvent le risque d'autonomie de la sous-traitance en créant un cadre contractuel clair, en définissant des attentes précises, en imposant des responsabilités explicites, en fournissant des garanties de sécurité, en introduisant des mécanismes de contrôle et de sanctions et en permettant une adaptation continue. Cela permettra à l'organisation de maintenir un contrôle efficace sur sa cybersécurité, même si elle externalise certaines de ses tâches. (The National cybersecurity society, 2023)

6.2.5.2 La cybersécurité demeure une responsabilité collective

Les entreprises doivent collaborer et partager des informations pour mieux se défendre contre les cyberattaques. Il s'agit d'une dynamique nouvelle, une nouvelle voie et façon de prévoir une politique de défense des entreprises. Nous notons que la collaboration et la création d'une capitalisation du savoir et de prospective autour des incidents de cybersécurité augmentera le niveau de sécurité globale de façon mécanique. La naissance d'un système de défense collectif où chaque organisation peut venir puiser dans une base de données communes des différentes attaques pour mieux se défendre. Nous soutenons l'émergence de cette culture de défense collective, un cerveau collectif disposant d'une meilleure mise à niveau des informations liées aux différentes attaques.

Trouchaud (2018) suggère le recours à un tiers de confiance qui a pour mission de collecter les caractéristiques des incidents, les traiter et les anonymiser pour enfin restituer des synthèses aux différents acteurs économiques. En plus du partage des incidents passés et présents, il prévoit de mettre en place des systèmes d'analyses prédictifs pour anticiper les futures menaces. Il s'agit de tirer les leçons des incidents survenus et d'être capable de faire de la prospective sur les futures menaces à venir. Mieux, les organisations vont trouver également un soutien opérationnel en cas de crise. Ce tiers de confiance peut aussi assister les organisations à mettre en place leur stratégie de défense en cybersécurité. L'idéal serai de créer un écosystème qui permet de mieux gérer les attaques, de mieux les comprendre et de mieux les prévoir.

6.2.5.3 La création de poste auxiliaire à la gestion de la cybersécurité

Nous remarquons d'après ces entretiens avec les leaders de cybersécurité la nécessité de créer des postes complémentaires au RSSI pour lui assister dans sa mission d'assurance de la cybersécurité. La création des postes suivants demeure une obligation pour une cybersécurité efficace :

- Le Data Protection Officer (DPO), sous la responsabilité du RSSI, renforce la protection des données et la conformité réglementaire.
- Le data scientiste qui est capable d'avoir une vision d'ensemble de données d'une organisation, de connaitre lesquelles sont réellement stratégiques en les mettant en valeur pour les expliquer clairement à la DG. Il appréhende les algorithmes, les statiques et exploite la donnée pour l'enrichir et lui donner une valeur.
- L'ingénieur de sécurité qui possède un profil plus classique en sécurité qui doit savoir les mécanismes d'attaque et de protection.
- Le superviseur ou contrôleur de données qui détient un profil hybride pour surveiller les données. Il dispose d'une double compétence pour appliquer aux données de sécurité elles-mêmes les nouveaux outils d'analyse en mettant en place une surveillance pointue.

Nous concluons que les organisations s'adaptent à l'évolution de la cybersécurité en créent de nouveaux postes d'assistance au RSSI pour réduire les menaces.

6.2.5.4 Le recours à des expertises externes n'est pas un point faible

Nous notons que le recours à des expertises externes en matière de cybersécurité repose sur le fait que les banques observées ne disposent pas en interne des compétences et de l'expérience nécessaires pour faire face efficacement aux menaces et aux défis de sécurité informatique. Les banques reconnaissent leurs propres lacunes en matière de compétences internes en cybersécurité pour un manque de talents, un manque de ressources pour la formation et du fait que la cybersécurité est un domaine en constante évolution qui nécessite une expertise spécialisée.

Nous signalons que l'acceptation des expertises externes repose à embaucher des professionnels de la cybersécurité externes à l'organisation qui ont déjà acquis une expérience utile en traitant des problèmes similaires dans d'autres contextes. Ces experts sont familiers avec les types d'attaques, les vulnérabilités courantes et les méthodes les plus efficaces pour les contrer. Ainsi, ils sont capables de fournir des solutions éprouvées à des problèmes complexes.

Nous notons que la formation interne peut être utile, mais elle peut prendre du temps et ne

toujours pas suffire pour répondre rapidement aux menaces. En faisant appel à des professionnels externes, la banque peut immédiatement bénéficier de leur expertise et de leur expérience en réduisant les risques. Dans le contexte observé, l'acceptation des expertises externes en cybersécurité demeure une stratégie pragmatique pour répondre aux défis de sécurité, en tenant compte du manque de compétences internes et de l'importance de l'expérience dans la gestion des menaces numériques. Cela permet à l'organisation de tirer parti des connaissances et des compétences d'experts externes pour renforcer sa sécurité informatique de manière efficace et efficiente.

6.2.5.5 L’audit et la sensibilisation

Nous argumentons que l’audit interne ne doit pas se limiter à la vérification de la conformité aux réglementations et aux politiques mais doit également inclure une évaluation approfondie du respect des procédures de sécurité et de la sensibilisation à la sécurité.

Nous avons observé que la sensibilisation à la sécurité est un élément crucial de la cybersécurité. En tant que première ligne de défense contre les cybermenaces, les employés doivent être informés des risques et des procédures de sécurité recommandées. L'audit interne peut évaluer la manière dont une organisation éduque et forme son personnel à la sécurité, garantissant ainsi le succès des campagnes de sensibilisation. L’audit interne s’assure que les politiques et procédures de sécurité doivent être suivies : si elles ne sont pas correctement suivies, les politiques et procédures de sécurité sont inutiles. L'audit interne doit vérifier que les membres du personnel adhèrent aux protocoles de sécurité définis. Cela couvre des éléments tels que la gestion des droits d'accès, la mise à jour fréquente des logiciels et l'utilisation de mots de passe forts. L’audit interne peut renforcer l’évaluation de la culture de sécurité de l'organisation où les employés sont encouragés à être proactifs dans la protection des informations sensibles et à signaler les activités suspectes lorsqu'une culture de sécurité positive est en place. Si cette culture existe et est soutenue par la direction, elle peut être découverte grâce à l'audit.

Nous avons remarqué aussi que l'audit interne peut localiser les lacunes en matière de formation et de communication en analysant la sensibilisation à la sécurité et le respect des politiques. Grâce à des initiatives de formation spécialisées et à des changements de procédures, ces lacunes peuvent être comblées. Quand la sensibilisation à la sécurité est accrue et les pratiques de sécurité organisationnelles sont respectées, les violations de données et les incidents de sécurité seront ainsi moins probables.

L’audit interne ne doit pas se concentrer uniquement sur la conformité, mais également évaluer la sensibilisation à la sécurité et le respect des protocoles de sécurité. En conséquence, les

employés sont informés des menaces de cybersécurité et impliqués activement dans la protection des données et des systèmes, garantissant ainsi que l'organisation est bien préparée à y faire face.

6.2.5.6 Les compétences en cybersécurité

Les organisations et les banques en particulier sont confrontées à de nombreuses difficultés pour trouver et développer des talents en cybersécurité. La cybersécurité est un domaine en constante évolution et de nouvelles menaces apparaissent constamment. En conséquence, les professionnels qualifiés en cybersécurité sont rares dans le monde. Afin de gérer efficacement les risques de cybersécurité, les organisations ont du mal à trouver et à recruter des candidats possédant l'expertise technique requise. Pour remédier à la pénurie de talents, les banques doivent consacrer de l'argent à l'éducation et à la formation en matière de cybersécurité. Cela pourrait impliquer l'embauche de stagiaires ou de jeunes talents pour former, le recyclage des employés actuels et le développement de programmes de sensibilisation à la sécurité pour l'ensemble de l'entreprise. Il est essentiel de valoriser les compétences en cybersécurité une fois celles-ci présentes au sein de l'organisation.

Cela implique d'honorer et de rémunérer les experts en cybersécurité pour leurs connaissances et leur contribution à la sécurité de l'entreprise. Les experts en cybersécurité sont encouragés à rester dans la banque et à se consacrer pleinement à leur rôle lorsqu'ils sont correctement rémunérés.

Nous notons qu'une approche proactive demeure primordiale en matière de ressources humaines pour trouver des talents en cybersécurité. Afin d'attirer les meilleurs candidats, cela implique de collaborer avec des agences de recrutement spécialisées, de participer à des conférences et à des événements sur la cybersécurité et de bâtir une marque employeur forte. Pour fidéliser les professionnels de la cybersécurité et encourager leur maintien dans l'emploi de la banque, il est essentiel d'établir des parcours de carrière clairs pour eux. Pour faire simple, les banques qui souhaitent se défendre efficacement contre les menaces informatiques doivent investir dans le développement de compétences en cybersécurité.

6.2.5.7 L'évaluation de l'allocation des ressources financières en cybersécurité

Nous notons la question des budgets alloués est un élément qui démontre la faible maturité des organisations sur la cybersécurité. La protection des systèmes d'information et des données sensibles d'une organisation dépend fortement de l'allocation de budgets adéquats à la cybersécurité. Nous avons observé plusieurs acteurs se plaindre des budgets fournis en cybersécurité dans les banques. Les cybermenaces évoluent constamment et deviennent de plus

en plus complexes. En investissant dans des technologies de sécurité de pointe, des systèmes de détection d'intrusion et des systèmes de prévention, les banques peuvent mieux se préparer à faire face à ces nouvelles menaces. Nous avons observé la réputation d'une banque détruite par une violation de données ou une cyberattaque réussie. La banque pourrait perdre la confiance des clients et des collaborateurs. Les dépenses en matière de cybersécurité contribuent à éviter ces événements et à préserver la réputation de la banque. En général, il est moins coûteux d'investir dans la protection contre les cyberattaques que dans la lutte contre les attaques après qu'elles ont déjà eu lieu. Dépenser suffisamment d'argent pour la cybersécurité peut contribuer à éviter des incidents coûteux et dommageables.

Nous soulignons l'importance d'allouer des budgets suffisants à la cybersécurité puisque ça demeure un investissement stratégique qui permet aux banques de se défendre contre les cybermenaces, de respecter les exigences légales, de préserver leur réputation et de soutenir leur croissance. Pour garantir une cybersécurité fiable et efficace, il s'agit d'une étape cruciale.

Mais n'oublions pas que même si le budget est disponible, mais la banque ne connait pas combien est dépensé en cybersécurité et sur quoi portent les dépenses, alors il est d'expérience quasi certain que la banque gère mal ses risques.

La cybersécurité est un enjeu majeur pour les banques, et les perspectives proposées mettent en lumière l'importance de l'externalisation, de la collaboration, de la sensibilisation, de la gouvernance, de la certification, et de l'investissement financier pour relever ces défis. Une approche collective et une implication de l'ensemble de la banque sont essentielles pour assurer une cybersécurité efficace à l'ère des menaces numériques croissantes.

6.2.6 L'émergence d'une gouvernance circulaire

Le contexte général de la cybersécurité sur le terrain bancaire français et libanais révèlent une part d'autonomie et une part de risque où la cybersécurité est traitée comme un risque parmi d'autres et la gestion des risques est toujours dépendantes des ressources. Les banques ne peuvent plus vivre dans une culture défensive traditionnelle, mais doivent améliorer leurs défenses vers l'avant et être plus flexibles pour faire face à de nouvelles attaques. Les nouvelles vagues de technologie et de stratégie changent radicalement la relation des individus avec l'environnement et la relation d'une banque avec sa chaîne de valeur. La collaboration entre les différents acteurs renforcera chaque chaîne de valeur. Dans ce cadre, nous fusionnons tous les résultats obtenus du terrain bancaire français et libanais avec les interprétations des leaders de la cybersécurité. Cette union d'appréhender la cybersécurité sous une nouvelle vision nous

amène à une gouvernance circulaire.

Nous retenons les paroles de Nicolas Dufour, professeur à la Paris School of Business dans un article paru dans la *Harvard Business Review*[12] : *« la vie du RSSI est complexe dans l'organisation. La remontée d'information sur les risques, parce qu'il s'agit d'une matière hautement sensible, suppose une réelle diplomatie et un sens aigu du relationnel de la part du risk manager quand il se retrouve face aux responsables d'activité. Il lui faut en effet cartographier les principaux risques (risques stratégiques, risques de fraudes, risques RH, risques de gouvernance…), définir les périmètres susceptibles d'être touchés, identifier les failles de l'organisation ou les faiblesses d'un responsable métier, récupérer les acteurs capables d'apporter des solutions et surtout faire comprendre à chacun son rôle et le niveau d'implication qui est attendu de lui, et proposer, en accord avec les métiers, des actions concrètes.* » D'après ce chercheur la valeur ajoutée du *risk manager* réside dans sa mission d'alerte propre à sa fonction ce qui lui autorise de se situer au plus près des directions générales.

Nous positionnons le RSSI dans cette gouvernance circulaire au cœur de l'organisation comme consultant interne qui assiste les managers à arbitrer entre les opportunités à saisir et celle à laisser de côté. Le RSSI propose des clés pour réussir et réduire les menaces.

Le positionnement du RSSI doit s'accompagner avec la mise en place de la gouvernance circulaire, une organisation souple et efficace dans laquelle tous les acteurs collaborent afin de mieux gérer la cybersécurité. Le RSSI au cœur de l'entreprise doit s'assurer d'avoir dans chacune des entités des relais sur le sujet de la sécurité. Nous notons que la divergence vers cette nouvelle dimension du management du cyber risque exige des compétences humaines, des investissements financiers et une nouvelle organisation. Cette nouvelle manœuvre tant managériale qu'organisationnelle accordera une gestion sereine de la cybersécurité. Il s'agit d'une coopération entre les ressources humaines et les entités informatiques et digitales pour faire circuler les informations afin que les collaborateurs soient formés aux risques ce qui va développer une culture de sûreté.

Il faut donc sortir de la gouvernance verticale vers une gouvernance circulaire. Nous prévoyons dans l'organigramme du comité de direction un poste de référant qui sera le responsable de la sécurité globale de l'information au sein de l'organisation. Il sera en charge de la stratégie de sécurité globale de l'entreprise et placé au cœur de l'organisation.

[12] Nicolas Dufour, Harvard Business Review, « Communiquer sur les risques en entreprises : entre diplomatie et devoir d'alerte », https://www.hbrfrance.fr/chroniques-experts/2015/04/6628-communiquer-sur-les-risques-en-entreprise-entre-diplomatie-et-devoir-dalerte/

La stratégie circulaire exige la naissance d'un comité de sécurité d'information comme le premier maillon de la chaine, qu'il irriguera vers les autres comités de finances, ressources humaines, commercial, communication… Nous retenons que chaque direction appliquera un processus de sécurité identique et partagera son expérience avec les autres dans le but d'une amélioration globale de la cybersécurité de l'organisation. En appliquant les mêmes politiques de contrôles, d'évaluation et d'alerte, la gestion circulaire permet une souplesse importante quant aux choix des données à protéger. Le comité de sécurité de l'information à travers cette gouvernance circulaire informe tous les acteurs à la criticité des données et à leurs mécanismes de protection. Dans ce sens, chaque direction détermine quels sont les éléments cruciaux à protéger et devient responsable de la sécurité de ses propres données grâce à une harmonie globale. Si une direction fait défaut alors toute la chaine va se trouver exposer à une potentielle attaque. L'important est la collaboration entre les directions à travers l'échange des expérimentations, des repérages, des innovations et des alertes des autres où chaque direction possède aussi une responsabilité propre. La gestion de la cybersécurité demeure un enjeu collectif en pratique et la gouvernance de la sécurité devient plus près des opérations.

Nous notons que cette gouvernance circulaire reste à l'heure actuelle complexe et requiert beaucoup d'effort supplémentaire pour l'organisation. L'élaboration de la stratégie globale de cybersécurité n'est pas une vérité révélée mais réellement le résultat d'un travail collectif. Le RSSI pourrait s'appuyer sur les éléments apportés par les directions en cas d'attaque.

La gestion de la cybersécurité implique une démarche disruptive et participative où les banques doivent évoluer leurs visions et investir pour être mieux protégés et donc plus performantes.

Conclusion intermédiaire

La partie 6.2 du chapitre 6 nous amène dans un monde complexe et en constante évolution : celui de la cybersécurité dans le secteur bancaire français et libanais. À travers des entretiens avec des experts et des dirigeants en cybersécurité, nous avons examiné différents aspects de cette discipline importante, de la gouvernance à l'identité professionnelle des RSSI, en passant par l'externalisation, la gestion des talents et les budgets alloués.

De cette analyse approfondie, nous pouvons conclure que la cybersécurité est plus que jamais au cœur des préoccupations des organismes bancaires. Les menaces numériques évoluent constamment et deviennent de plus en plus sophistiquées, et les problèmes de sécurité sont devenus essentiels à la confiance des clients, à la protection des données et au maintien de la réputation des institutions financières.

L’une des principales tendances mises en évidence est l’évolution du rôle du RSSI, passant de technicien à stratège et gestionnaire. Les RSSI doivent développer des compétences diversifiées qui vont au-delà des aspects techniques pour inclure les aspects juridiques, éthiques, sociaux et financiers. Ils doivent devenir des acteurs clés dans la définition de la stratégie de cybersécurité de leur organisation et participer activement aux décisions clés en matière de sécurité.

La cybersécurité nécessite un modèle de gouvernance participative où toutes les parties prenantes collaborent pour surmonter les défis liés aux risques cyber. Le RSSI doit jouer un rôle central, équilibrant expérience et objectivité, tout en favorisant une coopération efficace et en clarifiant les rôles pour éviter les chevauchements et renforcer la résilience organisationnelle.

La gouvernance circulaire émerge en réponse à la complexité croissante de la cybersécurité. Elle repose sur la collaboration de toutes les parties prenantes de l'entreprise, de la direction aux différents services spécialisés, pour créer une culture de sécurité et partager les responsabilités en matière de protection des données et de gestion des risques.

En fin de compte, cette partie nous rappelle que la cybersécurité est un défi permanent et nécessite des investissements, des compétences diversifiées et une approche proactive. Les organisations bancaires doivent continuellement s’adapter pour relever ces défis, adopter des pratiques modernes, collaborer avec des experts externes et allouer des budgets adéquats pour assurer leur résilience face aux menaces numériques. La sécurité informatique n’est plus une simple question technique, mais un élément essentiel de la gestion globale des risques et de la stratégie commerciale.

6.3 Les Apports théoriques : la complémentarité des cadres d'analyses des identités professionnelles

Notre étude a intégré et mis en perspective les théories et cadres d'analyse abordés dans les chapitres précédents pour explorer les identités professionnelles dans le domaine de la cybersécurité bancaire. Nous avons notamment mobilisé des cadres théoriques sur les identités professionnelles et les dynamiques interprofessionnelles pour analyser comment les différents acteurs — directeurs d'audit, RSSI, responsables informatiques, chefs et superviseurs d'équipe d'audit, ainsi qu'informaticiens — construisent et adaptent leur identité professionnelle au sein des institutions bancaires françaises (BPVF) et libanaises (8 banques). Cette approche met en lumière la manière dont ces cadres, en se complétant, permettent d'analyser de façon approfondie les mécanismes par lesquels les professionnels de la cybersécurité construisent et ajustent leur identité au sein de l'organisation bancaire, face aux enjeux sécuritaires. Les professionnels construisent, ajustent et redéfinissent leur rôle au sein de l'organisation. L'objectif est d'éclairer le lien essentiel entre ces identités et les défis de la cybersécurité, dans un contexte où les menaces sont de plus en plus complexes et évolutives.

6.3.1 Perspectives et recommandations d'experts en Cybersécurité : approches innovantes pour la gouvernance bancaire

Dans le contexte des défis croissants en cybersécurité, il est essentiel de replacer cette recherche dans la perspective des recommandations des experts. Nos entretiens ont révélé des observations récurrentes autour des compétences, du positionnement et du rôle évolutif du RSSI. Ces experts soulignent des besoins critiques en termes d'adaptation structurelle et de gouvernance dans les institutions bancaires pour renforcer leur résilience face aux menaces cybernétiques. Une analyse approfondie de ces recommandations est réalisée en structurant les observations des experts qui reflètent les tendances actuelles en cybersécurité et soulignent l'importance de la valorisation des identités professionnelles.

Le positionnement hiérarchique du RSSI est perçu comme une limite structurelle par plusieurs experts. Selon Peliks, l'autonomie du RSSI est compromise lorsqu'il est rattaché au département informatique, ce qui entraîne une dépendance potentiellement problématique. Cette configuration limite la capacité du RSSI à développer une ligne de défense indépendante. Maret renforce cette idée en affirmant que cette dépendance hiérarchique affecte la capacité du RSSI à instaurer des mesures de sécurité proactives. Trouchaud, de son côté, met en évidence une autre forme de dépendance en remarquant que les RSSI sont souvent mal positionnés dans

les grilles salariales, ce qui reflète une sous-valorisation de leur rôle stratégique dans les institutions bancaires. Les experts préconisent un repositionnement stratégique du RSSI au sein de la direction générale. Peliks et El Baraka proposent un rattachement direct du RSSI à la direction générale, aux départements de gestion des risques et à des instances de gouvernance clés comme le DPO et le SOCLE, soulignant ainsi l'importance d'une coordination transversale. Trouchaud évoque l'idée d'un RSSI agissant comme consultant interne, implanté au cœur de l'organisation, jouissant d'une visibilité accrue et intégré dans le processus de décision stratégique. Les experts dépeignent souvent le rôle traditionnel du RSSI comme strictement technique et limité à des tâches de contrôle. Pour Peliks et El Baraka, les RSSI sont fréquemment contraints à un rôle de supervision sans réelle capacité d'influence stratégique, agissant comme des « gardiens de pare-feu » ou des « chasseurs » en quête de vulnérabilités (Desvignes). Cette perception du RSSI comme simple exécutant réduit son impact potentiel dans la définition d'une stratégie de cybersécurité globale.

Les avis des experts révèlent que les RSSI sont souvent perçus comme des techniciens « pompiers de la cybersécurité », limités à une expertise technique sans vision d'ensemble. Pour El Baraka et Trouchaud, le RSSI manque de compétences métier et de capacités de leadership, ce qui limite leur influence sur la prise de décision. Lecompte soutient cette observation en mentionnant que ces compétences techniques prédominantes laissent peu de place à une vision stratégique et managériale. En conséquence, les experts s'accordent à dire que le RSSI doit désormais acquérir des compétences stratégiques et managériales. Pour Peliks et Desvignes, le RSSI doit intégrer des compétences juridiques et sociales pour mieux naviguer dans les nouvelles réglementations et assumer des responsabilités décisionnelles accrues. Trouchaud renforce cette idée en soulignant la nécessité pour le RSSI de devenir un communicant efficace, doté de compétences en gestion de crise, afin de renforcer la résilience cybernétique de l'organisation. Les trois lignes de défense, un modèle de gouvernance fondamental, sont largement soutenues par les experts en cybersécurité. Pour El Baraka et Desvignes, une collaboration étroite entre la direction générale, le RSSI, le département des risques et l'audit interne est essentielle pour garantir une cybersécurité efficace et durable. Lavault rappelle que l'ANSSI, l'organisme national de cybersécurité, encourage cette approche pour promouvoir une culture de gouvernance basée sur des lignes de défense interconnectées.

Dans une vision plus prospective, les experts appellent à une transformation culturelle vers une cybersécurité collective et une gouvernance circulaire. Peliks et Desvignes mettent en avant l'importance de construire une culture de défense partagée, où la cybersécurité est perçue

comme une responsabilité collective. El Baraka souligne l'importance des expertises externes pour apporter des perspectives nouvelles et complémentaires. Trouchaud propose de repenser la gouvernance traditionnelle vers une gouvernance circulaire, favorisant une vision plus collaborative et inclusive de la sécurité. Enfin, Lecompte insiste sur la nécessité de suivre des standards de certification comme l'ISO27001 pour institutionnaliser un cadre de management de la sécurité de l'information. Ces recommandations révèlent une redéfinition fondamentale des rôles et des compétences du RSSI, intégrant à la fois une dimension technique, managériale et stratégique. Les entretiens montrent que le RSSI est amené à jouer un rôle clé dans la gouvernance des risques et la résilience organisationnelle, en tant que pivot d'une stratégie interprofessionnelle. L'adoption de modèles de gouvernance innovants comme la gouvernance circulaire, combinée aux trois lignes de défense et au renforcement des identités professionnelles, offre une perspective structurée et holistique pour répondre aux enjeux de la cybersécurité dans le secteur bancaire.

6.3.2 Retour réflexif sur la recherche

Une perspective nouvelle et structurante émerge de notre analyse, qui met en avant trois piliers organisationnels essentiels pour renforcer la cybersécurité : un système de surveillance et d'alerte en temps réel, une gouvernance circulaire et participative, et une stratégie globale de cybersécurité intégrée et proactive. Ces éléments répondent aux besoins identifiés sur le terrain et illustrent comment les identités professionnelles et la structure organisationnelle s'interconnectent pour adapter et renforcer la réponse aux risques cyber dans le secteur bancaire.

En ce qui concerne le système de surveillance et d'alerte en temps réel, la cybersécurité exige une surveillance continue, permettant de détecter les anomalies et de réagir rapidement aux menaces. Un tel système de suivi est conçu pour repérer tout comportement suspect ou tout événement inhabituel en temps réel, fournissant une alerte immédiate qui favorise la réactivité de l'organisation. Cette surveillance proactive renforce l'identité du RSSI et des équipes de sécurité comme acteurs de première ligne, impliqués activement dans la protection du périmètre de sécurité, et contribue ainsi à une gestion plus dynamique et moins compartimentée des risques.

Pour la gouvernance circulaire et collaborative, notre recherche montre que la cybersécurité en milieu bancaire nécessite une gouvernance basée sur des échanges continus, une communication transparente et une implication de toutes les parties prenantes. Cette gouvernance circulaire encourage les interactions entre les différents niveaux de l'organisation,

apportant une dimension participative aux décisions en matière de sécurité et évitant les silos souvent observés dans les structures traditionnelles. En favorisant une prise de décision partagée, ce modèle de gouvernance optimise la distribution des responsabilités, renforce la transparence organisationnelle et améliore la cohésion entre les différents départements. Un exemple concret des interactions entre le RSSI et l'audit interne dans ce cadre circulaire illustrerait leur collaboration en matière de cybersécurité, montrant comment ils contribuent en tant que garants techniques et facilitateurs de la coordination stratégique.

Quant à la stratégie globale et proactive de cybersécurité, il est essentiel d'avoir une approche unifiée et proactive avec des objectifs clairs, des mesures concrètes, et une vision à long terme pour protéger les actifs numériques de l'organisation. Cette stratégie crée un cadre commun qui permet à chaque identité professionnelle de s'aligner et de contribuer de manière structurée à la sécurisation des opérations bancaires. En fixant des priorités claires, elle aide à anticiper les évolutions des risques et à orienter les efforts en fonction des nouvelles menaces, tout en valorisant les expertises de chaque acteur au sein d'un objectif commun.

Cependant, ces trois éléments — surveillance, gouvernance et stratégie globale — ne sont pas suffisants à eux seuls pour créer une réponse complète aux cybermenaces. Ils sont essentiels pour instaurer une dynamique d'adaptation continue, nécessitant la participation active de chaque identité professionnelle impliquée. La cybersécurité doit être envisagée comme un processus en constante évolution, avec une évaluation continue et une actualisation régulière des dispositifs de sécurité. Par exemple, un processus de check-up périodique, impliquant le RSSI, les auditeurs internes, les responsables informatiques, et les équipes d'audit, pourrait être mis en place pour examiner régulièrement les systèmes et politiques de sécurité, assurer leur alignement avec les nouvelles menaces et adapter les pratiques en conséquence. Cette collaboration continue renforce non seulement la sécurité mais également la culture de cybersécurité au sein de l'organisation. Ce suivi continu, fondé sur un modèle circulaire et co-construit, améliore la transparence organisationnelle et permet à l'organisation de démontrer à ses clients et partenaires un engagement constant en faveur de la cybersécurité, ce qui est crucial pour bâtir et maintenir la confiance.

Notre recherche met en avant une approche proactive et en constante adaptation de la cybersécurité, qui inclut la surveillance en temps réel, une gouvernance participative, une stratégie globale et une évaluation continue des systèmes de sécurité. L'intégration de ces piliers souligne la reconnaissance de la cybersécurité comme un défi permanent et multidimensionnel, qui exige une vigilance soutenue et une collaboration interprofessionnelle pour s'adapter aux

menaces changeantes. Cette dynamique de transparence et d'évolution continue répond directement aux attentes des parties prenantes et s'inscrit dans une gouvernance de cybersécurité plus cohérente avec les besoins spécifiques du secteur bancaire.

6.3.3 Les limites de la recherche

Nous abordons les limites de la recherche et proposons des recommandations pour améliorer la collaboration entre les auditeurs internes et les RSSI dans le secteur bancaire. Nous mettons en lumière les principales limites de notre recherche et proposons des recommandations visant à renforcer cette collaboration. L'objectif est d'identifier les obstacles actuels à une collaboration efficace et de suggérer des pistes d'amélioration pour faciliter l'intégration des rôles et des expertises de chaque acteur dans une gestion de la cybersécurité plus cohérente et proactive.

Tout d'abord, nous avons pu repérer deux formes d'articulation dans les récits des acteurs. Cela peut signifier qu'il existe des différences dans la manière dont les acteurs perçoivent et communiquent les problèmes liés à la cybersécurité et aux identités professionnelles. Il serait intéressant d'explorer davantage ces différences pour mieux comprendre les perceptions et les préoccupations de chaque groupe.

6.3.3.1 L'évolution rapide des techniques et dispositifs vs. Une inertie des identités professionnelles

Nous soulignons une divergence importante. Les techniques et les dispositifs de cybersécurité évoluent rapidement en réponse aux nouvelles menaces et aux avancées technologiques. En revanche, les identités professionnelles semblent évoluer beaucoup plus lentement, voire pas du tout. Cela peut entraîner des déséquilibres dans la manière dont les acteurs perçoivent et gèrent les risques liés à la cybersécurité. Par exemple, les RSSI, dont le rôle est d'anticiper les menaces et d'adapter rapidement les stratégies de sécurité, peuvent percevoir comme prioritaires des mesures réactives face aux nouvelles menaces (Trouchaud, 2016). Cependant, les autres acteurs de l'organisation, moins exposés à l'évolution rapide des risques, peuvent accorder davantage de poids aux pratiques établies, entraînant des divergences dans les priorités et les approches de gestion des risques.

6.3.3.2 Les implications précoces des RSSI dans les audits internes

Nous recommandons d'impliquer les RSSI dès les premières phases de planification des audits internes. Cette démarche permet aux RSSI de partager leur expertise en matière de cybersécurité, d'identifier les risques potentiels et d'évaluer les contrôles de sécurité. Cette collaboration dès le début du processus d'audit peut garantir que la perspective de la

cybersécurité est intégrée dès le départ.

Les RSSI doivent être ouverts aux recommandations et aux suggestions des auditeurs internes. Il est essentiel qu'ils reconnaissent la valeur de la perspective objective des auditeurs internes ainsi que leur expertise en matière de conformité réglementaire. Cette ouverture facilitera la communication et la coopération entre les deux groupes.

Pour éviter les conflits de juridiction et renforcer la gestion de la cybersécurité, il est crucial de promouvoir la collaboration et la complémentarité entre l'audit interne et les RSSI. Cela peut être réalisé par une meilleure définition des rôles et des responsabilités de chaque groupe, une communication ouverte et transparente, ainsi qu'une reconnaissance mutuelle de l'expertise de chaque partie.

Nous mentionnons le concept de ***No man's land***, qui représente potentiellement une zone de conflit ou de confusion entre les responsabilités de l'audit interne et des RSSI. Ce ***No man's land*** engendre des ambiguïtés qui risquent de compromettre l'efficacité des stratégies de cybersécurité

Pour améliorer la sécurité des systèmes d'information, il est essentiel de clarifier cette zone et de définir clairement les domaines de responsabilité de chaque groupe.

En résumé, cette partie de la conclusion met en évidence les défis liés à la gestion de la cybersécurité dans le secteur bancaire, en mettant en avant les différences entre l'évolution rapide des technologies de cybersécurité et l'inertie des identités professionnelles. Les recommandations visent à favoriser une collaboration plus étroite entre les auditeurs internes et les RSSI pour surmonter ces défis et renforcer la sécurité des systèmes d'information.

6.3.4 Influence de la culture organisationnelle sur la cybersécurité : théories et pratiques

Il serait pertinent d'examiner les théories organisationnelles et culturelles appliquées à la cybersécurité. À cet égard, l'introduction de concepts issus de la sociologie des organisations et de la gestion du changement permettrait d'expliquer de manière approfondie comment la culture d'entreprise influe sur les pratiques de cybersécurité. Plus spécifiquement, les travaux d'Edgar Schein (2021) sur la culture organisationnelle pourraient être mobilisés afin d'illustrer comment les valeurs et comportements partagés au sein d'une organisation façonnent les pratiques et décisions relatives à la cybersécurité.

Par ailleurs, dans le cadre de la gouvernance de la cybersécurité, il serait judicieux de rappeler les approches théoriques qui relient directement la culture organisationnelle à la gestion de la

cybersécurité, telles que le modèle Cybersecurity Culture Framework, ainsi que les recherches sur les comportements de sécurité. Ces travaux offrent un cadre d'analyse pertinent pour examiner dans quelle mesure la culture d'une organisation influence les pratiques quotidiennes et les choix stratégiques en matière de cybersécurité.

Enfin, il pourrait être éclairant d'étudier l'impact de la culture organisationnelle sur la gestion des risques en cybersécurité, en particulier en explorant comment cette culture affecte non seulement la réactivité face aux incidents de cybersécurité, mais également la prévention. Une telle approche permettrait de souligner l'importance de cultiver des comportements de vigilance et de responsabilité personnelle en matière de sécurité informatique au sein de l'organisation.

Conclusion intermédiaire

Cette partie nous a fourni une perspective théorique générale sur la manière dont les identités professionnelles dans le domaine de la cybersécurité bancaire sont construites et influencées par différents cadres analytiques. Elle souligne l'importance de combiner ces cadres pour acquérir une compréhension plus complète de ce processus. Ces insights théoriques offrent des perspectives intégratives pour renforcer la cybersécurité dans les institutions bancaires.

La phase finale de cette partie met en évidence les éléments clés nécessaires pour renforcer la cybersécurité au sein d'une organisation, notamment un système de surveillance et d'alerte efficace, une gouvernance circulaire et une stratégie globale de cybersécurité.

Cependant, nous soulignons également la nécessité d'une évaluation continue et collaborative du périmètre de sécurité et l'évolution constante de la cybersécurité en tant que processus dynamique.

Les limites de notre recherche mettent en évidence les défis auxquels sont confrontés les acteurs de la cybersécurité, notamment le décalage entre l'évolution rapide des technologies et l'inertie des identités professionnelles.

Notre recommandation vise à promouvoir une collaboration plus étroite entre les auditeurs internes et les RSSI pour relever ces défis et améliorer la gestion de la cybersécurité.

En bref, nous soulignons l'importance d'une compréhension et d'une adaptation continues dans le domaine de la cybersécurité bancaire, tout en encourageant la coopération et la complémentarité entre les différentes parties prenantes pour assurer la sécurité des systèmes bancaires.

Synthèse du chapitre 6 et de la thèse : perspectives intégratives sur la cybersécurité et la dynamique des identités professionnelles

Le chapitre 6 de cette thèse propose une synthèse approfondie des apports de la recherche, axée sur l'analyse de la cybersécurité dans le secteur bancaire et sur l'influence des identités professionnelles sur les pratiques sécuritaires. En mettant en avant les dynamiques interprofessionnelles et les responsabilités spécifiques des acteurs clés tels que les auditeurs internes et les RSSI, ce chapitre enrichit la compréhension de la cybersécurité non seulement comme un défi technique, mais comme un enjeu stratégique au cœur de la gouvernance des institutions financières.

Dans la première partie (6.1), nous avons identifié l'importance cruciale de comprendre comment les identités professionnelles influencent la sécurité informatique dans les banques. L'approche de l'identité professionnelle a fourni un cadre riche pour analyser les compétences, les rôles, les responsabilités et les valeurs des professionnels de la cybersécurité, tout en mettant en lumière les différences significatives entre les secteurs bancaires français et libanais. Les résultats ont souligné la nécessité d'une approche plus cohérente et coordonnée pour résoudre les problèmes de cybersécurité dans le secteur, en particulier au Liban.

La deuxième partie (6.2) nous a transportés dans l'univers complexe et en constante évolution de la cybersécurité bancaire, à travers des entretiens avec des experts et des dirigeants du secteur. Nous avons constaté que la cybersécurité est désormais au cœur des préoccupations des institutions financières, en raison de l'évolution rapide des menaces numériques et de leur impact sur la confiance des clients et la réputation des banques. Les RSSI jouent un rôle de plus en plus stratégique et doivent développer des compétences diversifiées pour guider la stratégie de cybersécurité de leur organisation. La gouvernance circulaire émerge comme une réponse à la complexité croissante de ce domaine.

La synthèse des résultats du chapitre 6 souligne une transformation profonde de la cybersécurité bancaire, qui dépasse son caractère strictement technique pour s'inscrire dans un cadre stratégique élargi. La cybersécurité devient une composante essentielle de la gestion des risques et de la stratégie commerciale des banques, nécessitant des investissements continus, des compétences diversifiées, et une approche proactive. Cette transition vers une gouvernance de la cybersécurité en tant que pilier stratégique exige une vision partagée entre les différents acteurs, impliquant une collaboration soutenue entre les auditeurs internes et les RSSI.

L'analyse met également en avant l'importance d'un système de gouvernance circulaire. Ce modèle favorise non seulement la transparence et la répartition équilibrée des responsabilités, mais également une meilleure compréhension des rôles et des priorités de chaque acteur dans l'écosystème de cybersécurité. La gouvernance circulaire encourage des interactions régulières et une prise de décision collective, éléments essentiels pour adapter les pratiques face aux menaces numériques en perpétuelle mutation.

Pour le secteur bancaire, notre étude recommande ainsi :

- Une intégration plus systématique des RSSI dans les processus d'audit dès les phases de planification, afin de renforcer la capacité d'anticipation des risques et d'optimiser les contrôles internes ;
- Une redéfinition des rôles et responsabilités de manière à limiter les zones d'ambiguïté et les éventuels "no man's lands" entre les différentes parties prenantes ;
- La mise en œuvre d'une évaluation continue et proactive de la sécurité, soutenue par un suivi régulier et une collaboration interprofessionnelle pour s'assurer que les dispositifs de cybersécurité évoluent au rythme des menaces.

Les résultats de cette recherche ouvrent de nouvelles perspectives pour l'étude de la cybersécurité dans le secteur bancaire. Tout d'abord, il serait bénéfique d'approfondir les recherches sur l'impact des technologies émergentes, telles que l'intelligence artificielle et la blockchain, sur les identités professionnelles et sur les pratiques de sécurité. Ces technologies offrent de nouveaux outils pour les RSSI et les auditeurs, mais elles requièrent également des compétences techniques et un cadre de gouvernance adaptés.

Ensuite, un axe de recherche complémentaire pourrait porter sur la formation continue en cybersécurité et sur le développement des compétences des professionnels, pour mieux harmoniser les perceptions et les priorités entre les différents acteurs. La formation pourrait être un levier pour renforcer la culture de cybersécurité et favoriser une compréhension commune des enjeux, des menaces et des bonnes pratiques.

Enfin, il serait judicieux d'explorer comment les organisations peuvent intégrer les retours d'expérience des crises de cybersécurité pour ajuster leurs stratégies et renforcer la résilience face à des menaces futures. Cette réflexion sur l'adaptabilité et l'innovation continue sera essentielle pour garantir non seulement la sécurité des données financières, mais aussi la pérennité de la confiance des parties prenantes dans un environnement de plus en plus numérique.

En conclusion, ce chapitre 6 et, plus largement, cette thèse, apportent une contribution substantielle à la compréhension de la cybersécurité dans le secteur bancaire, en particulier en ce qui concerne l'influence des identités professionnelles sur les pratiques sécuritaires et la gouvernance. La cybersécurité est désormais un enjeu multidimensionnel qui nécessite non seulement des solutions techniques, mais aussi une collaboration interprofessionnelle et une gouvernance agile. Ce travail offre ainsi des perspectives nouvelles pour la gouvernance de la cybersécurité, en proposant des stratégies d'intégration et de coopération pour les différents acteurs impliqués.

En fin de compte, cette thèse met en lumière la nécessité d'une adaptation continue et d'une innovation permanente dans le domaine de la cybersécurité bancaire. Garantir la protection des informations et des actifs numériques ne peut être réalisé sans un effort collectif, une vision stratégique partagée, et un engagement constant de l'ensemble des parties prenantes. C'est ce processus de construction collaborative, basé sur des identités professionnelles harmonisées et une gouvernance dynamique, qui constitue le cœur de la résilience des banques face aux défis numériques de demain.

BIBLIOGRAPHIE

Bibliographie

Abbott, A. (1988). The system of professions: An essay of the division of expert labor. University of Chicago Press.

Abbott, A. (2003). Écologies liées : à propos du système des professions. In Les professions et leurs analyses sociologiques (pp. 29-50). INED.

Abdolmohammadi, M. J., & Sarens, G. (2010). Factors associated with IT audits by the internal audit function. International Journal of Accounting Information Systems, 11(3), 140-151.

Abend, V., & Abend, V. (2008). Cyber security for the banking and finance sector. In Wiley Handbook of Science and Technology for Homeland Security. https://doi.org/10.1002/9780470087923.hhs460

Adams, T. L. (2004). Inter-professional conflict and professionalization: Dentistry and dental hygiene in Ontario. Social Science & Medicine, 58, 2243–2252.

Aggeri, F. (2016). La recherche-intervention : fondements et pratiques. In J. & Mottis (Eds.), A la pointe du management. Ce que la recherche apporte au manager (pp. 79-100). https://hal-mines-paristech.archives-ouvertes.fr/hal-01230457

AHIA & Deloitte. (2017). Cyber assurance: How internal audit, compliance, and information technology can fight the good fight together. Whitepaper Guidance for Healthcare Internal Auditors and Compliance Professionals.

Akerlof, G. A., & Kranton, R. E. (2010). Identity Economics: How Our Identities Shape Our Work, Wages, and Well-Being. Princeton University Press.

Al-Attar, S. (2020). Les dessous de la nouvelle ingénierie de Riad Salamé. Le Commerce du Levant.

Alvesson, M. (1994). Talking in organizations: Managing identity and impressions in an advertising agency. Organization Studies, 15(4), 535–563.

Alvesson, M. (2001). Knowledge work: Ambiguity, image, and identity. Human Relations, 54(7), 863–886.

Anderson, K. (2012). Cybersecurity: Public sector threats and responses. Auerbach Publications.

Anderson-Gough, F., Grey, C., & Robson, K. (1998). "Work Hard, Play Hard": The use of cliché in two accountancy practices. Organization, 5(4), 565–592.

Anderson-Gough, F., Grey, C., & Robson, K. (2001). Tests of time: Organizational time-reckoning and the making of accountants in two multinational accounting firms. Accounting, Organizations and Society, 26, 99–122.

Anderson-Gough, F., Grey, C., & Robson, K. (2006). Professionals, networking and the networked professional. Research in the Sociology of Organizations, 24, 231-256.

Annas, G. J. (2008). Military medical ethics—physician first, last, always. The New England Journal of Medicine, 359(2), 1087–1092.

Aranya, N., & Ferris, K. R. (1984). A reexamination of accountants' organizational-professional conflict. The Accounting Review, 59(1), 1–15.

Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. International Journal of Auditing, 13, 43-60.

Armstrong, P. (1985). Changing management control strategies: The role of competition

between accountancy and other organizational professions. Accounting, Organizations and Society, 10(2), 129–148.
Arora, B. (2017). Teaching cybersecurity to non-tech students. Politics, 1–14.
Arpagian, N. (2015). La cybersécurité. Presses Universitaires de France.
Ashforth, B. E., & Mael, F. (1989). Social identity theory and the organization. Academy of Management Review, 14(1), 20–39.
Autin, F. (2010). La théorie de l'identité sociale de Tajfel et Turner. In Préjugés & Stéréotypes.
Autorité de Contrôle Prudentiel et de Résolution (ACPR). (2020). Les chiffres du marché français de la banque et de l'assurance 2020. Dominique Laboureix.
Azure. (2022, August 2). Comment gérer ses systèmes d'information dans le cloud ? Retrieved from Axido: https://www.axido.fr/comment-gerer-ses-systemes-dinformation-dans-le-cloud/
Babin, J. (2022, September 16). Au Liban, les clients braquent les banques pour récupérer leur argent. Les Echos. https://www.lesechos.fr/finance-marches/banque-assurances/au-liban-les-clients-braquent-les-banques-pour-recuperer-leur-argent-1788502
Bachkad, J. (2004). L'audit des ressources humaines. Université Hassan I de Settat au Maroc.
Bagur, T., & Pichon, G. (2017). L'individu et l'interaction, entre rôle social et identité. Revue Européenne de Coaching, 2.
Banque Populaire Fédération Nationale. (2023, April 16). Récupéré de FNPB: https://www.fnbp.fr/notre-modele-cooperatif/notre-histoire/
Borthwick, A. M., & Adelaide, S. (2009). Achieving professional status: Australian podiatrists' perceptions. Journal of Foot and Ankle Research, 2, Article 8. https://doi.org/10.1186/1757-1146-2-8
Bourdieu, P., & Goffman, E. (2011). L'identité vue par Bourdieu et par Goffman. Paris: letudiant.fr.
Bourhis, R. Y., & Leyens, J.-P. (1999). Stéréotypes, discrimination et relations intergroupes. Sprimont, Belgique: Madaga.
Boyce, M. W., McNeese, M. D., & Riedel, M. (2011). Human performance in cybersecurity: A research agenda. Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting, 1115-1119.
Burt, T. L., & Ian, T. L. (2016). The impact of organizational identity and professional norm salience on internal auditors' assessments of internal control weaknesses. 2016 Canadian Academic Accounting Association (CAAA) Annual Conference, 1-36.
Cameron, D. (2011). Prime Minister's speech on cyberspace. London Conference on Cyberspace. 10 Downing Street, London: 2010 to 2015 Conservative and Liberal Democrat coalition government.
Capgemini, C. (2017). Information security benchmarking 2017. Capgemini Consulting, 1-26.
Carr, M. (2016). US power and the internet in international relations: The irony of the information age. Palgrave Macmillan.
Carson, D. G. (2001). Qualitative marketing research. SAGE.
Carter, A. (2015). The Department of Defense Cyber Strategy. Washington, DC.
Cartwright, J. E. (2011). Joint terminology for cyberspace operations. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Director of the Joint Staff Directorates. Washington, D.C. 20318-9999.
Castelli, C. J. (2008, May 23). Defense Department adopts new definition of 'cyberspace'. Inside

the Air Force.
Cattrysse, J. (2005). Reflections on corporate governance and the role of internal auditor. SSRN Electronic Journal, 1-64.
Cavetly, M. D. (2010). Cyber-security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies (pp. 58-74). London and New York: Taylor & Francis e-Library.
Chaffey, D. W. (2010). Business information management: Improving performance using information systems. Pearson Education.
Chaigne-Oudin, A.-L., & Emile, Y. (2010). Guerre civile libanaise. Les clés du Moyen-Orient.
Chambers, A. O. (2015). A new vision for internal audit. Managerial Auditing Journal, 30(1), 34-55. https://doi.org/10.1108/MAJ-08-2014-1073
Chambers, R. F. (2017). Internal audit's critical role in cybersecurity. Accounting Web.
Chambre de commerce et d'industrie. (2022, June 7). Stockage de données en entreprise : le cloud comme solution. Retrieved from les-aides.fr: https://les-aides.fr/actualites/c38/stockage-de-donnees-en-entreprise-le-cloud-comme-solution.html
Chang, S. E. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361. https://doi.org/10.1108/02635570610656161
Chapoulie, J.-M. (1973). Sur l'analyse sociologique des groupes professionnels. Revue française de sociologie, 14, 86-114.
Chava, C. (2014). Le premier ministre prononce un discours à l'ANSSI. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Pôle Stratégie, Médias et Communication. Hôtel de Matignon, Paris.
Cimpanu, C. (2020, February 13). Stress: Les RSSI restent en poste 26 mois en moyenne. Retrieved from ZDNet: https://www.zdnet.fr/actualites/stress-les-rssi-restent-en-poste-26-mois-en-moyenne-39899033.htm
Clemente, D. (2011). International security: Cyber security as a wicked problem. The World Today, 67(10), 15-17.
Cooke, N. J. (2012). Perspectives on the role of cognition in cyber security. Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting, 268-271.
Coram, P., Ferguson, C., & Moroney, R. (2008). Internal audit, alternative internal audit structures, and the level of misappropriation of assets fraud. Accounting and Finance, 48(4), 543-559.
Corkery, M. (2016). Once again, thieves enter Swift financial network and steal. The New York Times.
Costello, C. Y. (2004). Changing clothes: Gender inequality and professional socialization. NWSA Journal, 16(2), 138-155.
Covaleski, M. A. (2003). Jurisdictional disputes over professional work: The institutionalization of the global knowledge expert. Accounting, Organizations and Society, 28, 323–355.
Craigen, D. D.-T. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(7), 13-21.
Crawley, K. (2017). Information security, cybersecurity, IT security, computer security… What's the difference? The State of Security.
Cuomo, A. M. (2014). Report on cyber security in the banking sector. New York State, USA:

Department of Financial Services.
Cyber Security: An integrated governmental strategy for progress. (2011). In F. D. Kramer (Ed.), Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity (pp. 136-150). Georgetown University Press.
Cyert, R. M. (1963). A behavioral theory of the firm. University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship.
Dadouch, S. (2020). Unrest escalates in Lebanon as currency collapses and prospect of hunger grows. The Washington Post.
Danielle E. Warren, M. A. (2009). Ensuring independent auditors: Increasing the saliency of the professional identity. Group Decision and Negotiation, 18(1), 41-56.
Danielle Warren, M. A. (2008). Ensuring independent auditors: Increasing the saliency of the professional identity. Group Decision and Negotiation, 18(1), 41-56.
Darr, A. W. (2008). Assumptions, assertions, and the need for evidence debugging debates about knowledge workers. Current Sociology, 56(1), 25-45.
DE ROBERTIS, C. O. M. (2014). L'intervention sociale d'intérêt collectif: De la personne au territoire. Rennes: Presses de l'EHESP.
Deetz, S. (1996). Commentary: The positioning of the researcher in studies of organizations: De-hatching literary theory. Journal of Management Inquiry, 5(4), 387-391.
Deloitte. (2015). Cybersecurity: The changing role of audit committee and internal audit. Deloitte & Touche Enterprise Risk Services Pte Ltd.
Deloitte. (2018). The role of the audit committee. Deloitte Development LLC.
Demaret, J. (2014). Le processus de construction de légitimité des contrôleurs de gestion. Thèse de doctorat, Université François Rabelais.
Demazière, D. M. (2019). La socialisation professionnelle, au cœur des situations de travail. Octares Editions.
Denis, J. (2009). L'informatique et sa sécurité. Le souci de la fragilité technique. Réseaux, 2012(1), 161-187.
Denise Nicholson, E. (2016). Advances in human factors in cybersecurity. In Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity (pp. 169-171). Walt Disney World®, Florida, USA: Springer.
Dent, M. B.-L. (2016). The Routledge companion to the professions and professionalism. New York: Routledge.
Deslauriers, J.-P. (1991). Recherche qualitative: Guide pratique. McGraw-Hill.
Dibeh, G. (2002). The political economy of inflation and currency depreciation in Lebanon, 1984-92. Middle Eastern Studies, 38(1), 33-52.
Dimitra Petrakaki, E. K. (2014). Changes in healthcare professional work afforded by technology: The introduction of a national electronic patient record in an English hospital. Organization. The London School of Economics and Political Science, 24.
Dimnika, T. F. (2006). Accountant stereotypes in movies distributed in North America in the twentieth century. Accounting, Organizations and Society, 31(2), 129-155.
Donaldson, S. E. (2015). Managing a cybersecurity crisis. In S. G. Scott & E. Donaldson (Eds.), Cybersecurity: How to build a successful cyberdefense program against advanced threats (pp.

167-173). Berkeley, CA: Apress.
Donnelly, R. G. (2011). Does the UK have a ‘comparative institutional advantage’ that is supportive of the IT services sector? New Technology, Work and Employment, 26(2), 98-112.
Drouin-Hans, A. (2006). Identité. Le Télémaque, 29(1), 17-26.
Dubar, C. (1992). Formes identitaires et socialisation professionnelle. Revue française de sociologie, 505-529.
Dubar, C. (2015). La socialisation: Construction des identités sociales et professionnelles. Paris: Armand Colin.
Dubar, C. D. (1997). Analyser les entretiens biographiques: L’exemple des récits d’insertion. Paris: NATHAN.
Dubar, C., & Démazière, D. (1997). Analyser les entretiens biographiques: L'exemple de récits d'insertion. Paris: Les Presses de l’Université Laval.
Dupuis, J.-C. (2005). Sociologie de l’économie. Presses Universitaires de France.
Dupuy, B. (2014). Cyber-société et relations inter-organisationnelles. Socio-informatics et société de l’information, 14(2), 45-67.
Durkheim, E. (1985). The rules of sociological method. New York: The Free Press.
Dutta, A. M. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.
Dutton, J. E. (1994). Organizational image and member identification. Administrative Science Quarterly, 39, 239-263.
Dutton, J. E. (2010). Pathways for positive identity construction at work: Four positive identities and the building of social resources. The Academy of Management Review, 32(2), 265-293.
Dutton, J. R. (2010). Pathways for positive identity construction at work: Four types of positive identity and the building of social resources. The Academy of Management Review, 35(2), 265-293.
Eatough, V., & Smith, J. A. (2014). Stop helping me: Identity, recognition, and agency in the nexus of work and care. Organization, 21(1), 3-21.
Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2873-2882. Seoul, Republic of Korea — April 18-23, 2015.
Erikson, E. H. (1993). Childhood and society. New York, London: Norton Paperback.
ERMA. (2019). The role of internal audit in strengthening cybersecurity. Risk Management Article.
Ernst, Y. (2012). Fighting to close the gap: Key findings from EY’s Global Information Security Survey 2012. Insights on governance, risk and compliance, 1-28.
Eun, Y.-S. A. (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives, 20(4), 343-360.
Europe Research Services CFO. (2008). Are CFOs from Mars and CIOs from Venus? Overcoming the perception gap to enhance the finance-IT relationship. London: CFO Publishing Corporation.
européenne, L. P. (2001). Règlement (CE) N° 761/2001 du parlement européen et du conseil du 19 mars 2001 permettant la participation volontaire des organisations à un système communautaire de management environnemental et d'audit (EMAS). Revue Européenne de Droit de l’Environnement, 5(4), 475-488.

Ezingeard, J., & Smith, R. (2007). Triggers of change in information security management practices. Journal of General Management, 32(4), 53-72.
Ezzamel, M. B. (2005). Professional competition, economic value added, and management control strategies. Organization Studies, 26(5), 755-777.
Federal Bureau of Investigation. (2014). 2014 internet crime report. Internet Crime Complaint Center.
Federation of European Risk Management Associations. (2019). At the junction of corporate governance & cybersecurity. Brussels, Belgium. Retrieved from https://www.eciia.eu/wp-content/uploads/2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf
Filippone, D. (2020, February 14). Le stress perturbe les RSSI dans leur travail. Retrieved from Le Monde Informatique: https://www.lemondeinformatique.fr/actualites/lire-le-stress-perturbe-les-rssi-dans-leur-travail-78117.html
Fillol, C. (2007). Des choix méthodologiques à la production de connaissances opérationnelles : Propositions et illustration. Conférence internationale de l'Academy of Management (Division RMD). Lyon, France: ISEOR.
Fischer, E. A. (2009). Creating a national framework for cybersecurity: An analysis of issues and options. New York: Nova Science Publishers, Inc.
Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. Academy of Management Review, 32(4), 1180-1198.
Fogarty, T. L. (2000). An empirical evaluation of the interpersonal and organizational correlates of professionalism in internal auditing. Accounting and Business Research (Spring), 125-136.
Fourie, L. S. (2014). The global cybersecurity workforce - An ongoing human capital crisis. The Global Business and Technology Association, 173-184.
Francis, J. (1994). Auditing, hermeneutics, and subjectivity. Accounting, Organizations and Society, 19, 235-269.
Fray, A. P. (2010). Le diagnostic de l'identité professionnelle : une dimension essentielle pour la qualité au travail. Management & Avenir, 38, 72-88.
Freidson, E. (2001). Professionalism: The third logic. Chicago: University of Chicago Press.
Frunza, M.-C. (2016). Introduction to the theories and varieties of modern crime in financial markets (Vol. 978-0-12-801221-5). Oxford: Elsevier Inc.
Fuller, C. G.-B. (2013). Advanced skills teachers: Professional identity and status. Teachers and Teaching: Theory and Practice, 19(4), 463-474.
Galinec, D. S. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. 2017 IEEE 14th International Scientific Conference on Informatics, 1-34. Poprad, Slovakia: IEEE.
Galland, O. (2011). Sociologie de la jeunesse. Paris: Armand Collin.
Gay, G. H. (2011). Vulnerabilities in cyber security mean opportunities too. US Black Engineer and Information Technology, 35(4), 68-69.
Gendron, Y. S. (2010). Identity narratives under threat: A study of former members of Arthur Andersen. Accounting, Organizations and Society, 35(3), 275-300.
Gendron, Y., & Joffe, D. (2007). The construction of auditing expertise in measuring government performance. Accounting, Organizations and Society, 32(1-2), 101-129. https://doi.org/10.1016/j.aos.2006.07.002
Gercke, M. (2017). Red teaming and wargaming: How can management and supervisory board

members become more involved in cybersecurity? In F. Abolhassan (Ed.), Cyber Security. Simply. Make it Happen: Leveraging Digitization Through IT Security (pp. 27-28). Germany: Springer International Publishing.
Giddens, A. (1991). Modernity and self-identity. Cambridge: Polity.
Gilguy, C. (2010). Retrieved from https://www.lemoci.com/liban/
Gill, M. (2009). Accountant's truth: Knowledge and ethics in the financial world. New York: Oxford University Press.
Glover, S., Parawitt, S., & Romney, M. (1999). Implementing ERP. Internal Auditor (Feb), 40-47.
Goffman, E. S. (1975). Les usages sociaux des handicaps. Paris: Les Editions de Minuit.
Goodyear, M. G. (2010). Cybersecurity management in the states: The emerging role of Chief Information Security Officers. Strengthening Cybersecurity Series, 3-41.
Gordon, L. A. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. Journal of Accounting and Public Policy, 25(5), 503-530.
Grady, M. F., & Parisi, F. (2006). The law and economics of cybersecurity. Cambridge University Press.
Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cybersecurity behavior intentions. Computers & Security, 73, 345-358.
Grecs. (2014, May 5). Cyber security versus information security. Retrieved May 3, 2018, from NovaInfosec News, Events, & Resources for Infosec Professionals: https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/
Grey, C. (1994). Career as a project of the self and labour process discipline. Sociology, 28(2), 479-497.
Grey, C. (1998). On being a professional in a "big six" firm. Accounting, Organizations and Society, 23(5/6), 569-587.
Guéguen, H. (2014). Reconnaissance et légitimité: Analyse du sentiment de légitimité professionnelle à l'aune de la théorie de la reconnaissance. Vie sociale, 8(4), 67-82.
Gunz, H. G. (2007). Hired professional to hired gun: An identity theory approach to understanding the ethical behaviour of professionals in non-professional organizations. Human Relations, 60(6), 851-887.
Halliday, T. C. (1985). Knowledge mandates: Collective influence by scientific, normative, and syncretic professions. British Journal of Sociology, 36(3), 47-421.
Halpern, D. F. (2005). Psychology at the intersection of work and family: Recommendations for employers, working families, and policymakers. American Psychologist, 60(5), 397-409.
Halpern, D. F. (2005). Psychology at the intersection of work and family: Recommendations for employers, working families, and policymakers. American Psychologist, 60(5), 397.
Hamilton, S. (2013). Exploring professional identity: The perceptions of chartered accountant students. The British Accounting Review, 45, 37-49.
Hammond, P. G. (2016). National Cyber Security Strategy 2016-2021.
Hammond, P. G. (2016). National Cyber Security Strategy 2016-2021, 1-78.
Hani El-Chaarani, R. A. (2022). The impact of corporate governance and political connectedness on the financial performance of Lebanese Banks during the financial crisis of 2019-2021. Journal of Risk and Financial Management, 15, 203, 1-18.
Hani El-Chaarani, R. A. (2022). The impact of corporate governance and political

connectedness on the financial performance of Lebanese banks during the financial crisis of 2019-2021. Journal of Risk and Financial Management, 15(203), 1-18.
Harrison Stewart, J. J. (2017). Information security management and the human aspect in organizations. Information & Computer Security, 25(5), 494-534.
Harvey, T. (2016). COMPTIA launches training to stem biggest cause of data breaches. CompTIA.
Haslam, A. (2001). Psychology in organizations: The social identity approach. SAGE Publications Ltd.
Haslam, A. (2001). Psychology in organizations: The social identity approach. London: SAGE Publications.
Hathaway, O. A. (2012). The law of cyber-attack. California Law Review, 100(4), 817-885.
Hathaway, O. A. (2012, August). The law of cyber-attack. California Law Review, 100(4), 817-885.
Hatleback, E. N. (2018). The protoscience of cybersecurity. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 15(1), 5-12.
Hatzfeld, H. (2014). Au nom de quoi? Les revendications de légitimité, expressions de mutations sociales et politiques. Vie sociale, 8(4), 26-36.
Head, W. (2009). Current trends and issues facing internal audit. Internal Auditing, 24(5), 3-16.
Heckman, D. R. (2009). Effects of organizational and professional identification on the relationship between administrators' social influence and professional employees' adoption of new work behaviour. Journal of Applied Psychology, 94(5), 1325-1335.
Hochschild, A. R. (1983). The managed heart: Commercialization of human feeling. University of California Press.
Hogg, M. A. (2000). Social identity and self-categorization processes in organizational contexts. The Academy of Management Review, 25(1), 121-140.
Hotho, S. (2008). Professional identity–product of structure, product of choice: Linking changing professional identity and changing professions. Journal of Organizational Change Management, 21(6), 721-742.
Hu, Q. D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.
Huberty, P.-L. (2019). Addressing the fear of audit. Huberty Blog.
Hudson, B. (2002). Interprofessionality in health and social care: The Achilles' heel of partnership? Journal of Interprofessional Care, 16(1), 7-17.
Hudson, L. O. (1988). Alternative ways of seeking knowledge in consumer research. Journal of Consumer Research, 14(4), 508-521.
Hui, P., Zhang, B., & Wang, J. (2010). Towards efficient collaboration in cybersecurity. International Symposium on Collaborative Technologies and Systems (CTS), 489-498. Virginia.
Hyman, J. L. (2004). Needing a new programme? Union membership and attitudes towards unions amongst software workers. In W. Brown et al. (Eds.), The Future of Worker Representation (pp. 47-114).
Ialy, M. (2014). Les perceptions de l'audit interne par l'usage de métaphores (Master’s thesis). Université Catholique de Louvain, Louvain.

Ibarra, H. (1999). Provisional selves: Experimenting with image and identity in professional adaptation. Administrative Science Quarterly, 44(4), 764-791.
IBM Global Technology Services. (2014). IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of cyber attack and incident data from IBM's worldwide security operations. IBM Corporation.
IIA (Institute of Internal Auditors). (2004). Practice advisory 2060-2.
IIA (Institute of Internal Auditors). (2011). Introduction des normes. IFACI - Institut Français de l'Audit et du Contrôle Internes, 1-29.
IIA (Institute of Internal Auditors). (2017). Code de déontologie. Cadre de référence internationale des pratiques professionnelles - Edition 2017, 1-4.
IIA (Institute of Internal Auditors). (2017). Insight that internal audit brings to cybersecurity culture. Tone at the top, Issue 82, 1-4.
IIA (Institute of Internal Auditors). (2017). International standards for the professional practice of internal auditing. Maitland Avenue, Altamonte Springs.
IIA (The Institute of Internal Auditors). (2020). Standards and Guidance: Mandatory Guidance, Definition of Internal Auditing. The Institute of Internal Auditors North America.
Ik-Whan, G. K., & Kwon, D. B. (2004). Factors related to the organizational and professional commitment of internal auditors. Managerial Auditing Journal, 19(5), 606-622.
International Monetary Fund. (2023, March 23). Lebanon: Staff concluding statement of the 2023 Article IV mission. Retrieved from https://www.imf.org/en/News/Articles/2023/03/23/lebanon-staff-concluding-statement-of-the-2023-article-iv-mission
Islam, M. S. (2018). Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal, 33(4), 377-409. Retrieved from https://doi.org/10.1108/MAJ-07-2017-1595
ISO/IEC 27002. (2013). Information technology -- Security techniques -- Code of practice for information security controls.
ISO/IEC. (2012). Information technology -- Security techniques -- Guidelines for cybersecurity. International Organization for Standardization.
Ivanova, N. B. (2017). Identity as a factor of conflict behavior in organizations. DIEM: Dubrovnik International Economic Meeting, 3(1), 34-44.
Jaeger, J. (2013). Human error, not hackers, cause most data breaches. Compliance Week, 10(110), 56-57.
James, M. K., & Bailey, T. (2015). Beyond cybersecurity, protecting your digital business. Wiley.
Jamison, J. M. (2018). The future of cybersecurity in internal audit. Internal Audit Foundation and Crowe Horwath, 1-27. Retrieved from https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf
Jérémy, M., & Flores, A.-L. (2011). Mesurer et définir la valeur des marques : Un enjeu dans la concurrence entre groupes professionnels. Finance Contrôle Stratégie, 14(3), 63-90.
Johansson, S. E. (2005). Uppdrag revision – Revisorsprofessionen i takt med förväntningarna. Stockholm: SNS Förlag.
Johnson, M. D. (2006). Multiple professional identities: Examining differences in identification across work-related targets. Journal of Applied Psychology, 91(2), 498-506.

Johnson, R. O. (2004). Mixed methods research: A research paradigm whose time has come. Educational Researcher, 33(7), 14-26.
Jollans, A. (2018). Three ways to collaborate to improve cybersecurity. LinuxOne Solutions.
Jouffroy, M. (2005). Cinq témoignages enthousiastes. Revue Audit, 143, 3-63.
Kagermann, H., & Kunnen, K. (2008). Internal Audit Handbook Management with the SAP®-Audit Roadmap. Springer.
Kahyaoglu, S. C. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal, 33(4), 360-376.
Kaufman, A. S. (1994). Intelligent testing with the WISC-III. John Wiley & Sons.
Kempf, O. (2012). Cyberstratégie à la française. Revue internationale et stratégique, 87(3), 121-129. Retrieved from Senat.
Khoury, G. E. (2011). La résilience des banques libanaises : Analyse de certains aspects de la gestion des risques dans le cadre de l'accord de Bâle. Université de Liège, Liège.
Knapp, K. J. (2006). The top information security issues facing organizations: What can government do to help? Network Security, 1, 327.
Kolkowska, E., & Karlsson, F. (2017). Towards analyzing the rationale of information security noncompliance: Devising a value-based compliance analysis method. Journal of Strategic Information Systems, 26, 39–57.
Kornberger, M. J. (2011). "When you make manager, we put a big mountain in front of you": An ethnography of managers in a Big 4 Accounting Firm. Accounting, Organizations and Society, 36(8), 514-533.
Kosmala, K. H. (2006). The ambivalence of professional identity: On cynicism and jouissance in audit firms. Human Relations, 59, 1396-1428.
KPMG. (2016, September 6). Cyber security is the most prevalent IT risk for banks. Retrieved from https://home.kpmg.com/be/en/home/insights/2016/09/cyber-security-most-prevalent-it-risk-fs.html
Krotov, V. (2015). Bridging the CIO-CEO gap: It takes two to tango. Business Horizons, 58(3), 275-283.
Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Cyberpower and National Security, National Defense University Press.
Kuhlman, R. K. (2015). FINRA publishes its 2015 "Report on Cybersecurity Practices." Journal of Investment Compliance, 16(2), 47-51.
Kulesza, J. (2018). Cybersecurity. Springer, Cham: University of Lodz.
Kunnen, S., & Kunnen, K. (2006). Le développement de l'identité : Un processus relationnel et dynamique. L'orientation scolaire et professionnelle, 35(2), 183-203.
Kwon, J. U. (2012). The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27(1), 219-236.
Lamarque, D. (2016). Contrôle et évaluation de la gestion publique: Enjeux contemporains et comparaisons internationales. Bruylant.
Lambert, J. A. (2016, May). L'identité négative de l'auditeur. Accountability, Responsabilités et Comptabilités, 1-30.
L'assurance en mouvement. (2022, November 10). La cybersécurité, un enjeu majeur pour les RH des banques. Retrieved from https://www.lassuranceenmouvement.com/2021/11/10/la-cybersecurite-un-enjeu-majeur-pour-les-rh-des-banques/

Latour, J. (2018). Cybersecurity Survey, Canadian Report. Cira, Akamai.
Legalais, L. (2014). La construction de l'identité professionnelle des contrôleurs de gestion. Université Paris-Dauphine.
Lehto, M., & Neittaanmäki, P. (2015). Cyber security: Analytics, technology, and automation. Springer International Publishing.
Leong, K. Y. (2017). Cybersecurity: The changing role of audit committee and internal audit. Deloitte, 1-14.
Levitt, A. (2000). Renewing the covenant with investors. New York University Center for Law and Business.
Lévy, P. (1997). L'intelligence collective: Pour une anthropologie du cyberespace. Paris.
Lewis, D. (2010). How IT can help internal audit. THE EDP Audit, Control, and Security Newsletter, 41(3), 1-8.
Loster, P. C. (2005). Managing e-business risk to mitigate loss. Financial Executive, 21(5), 43-45.
Lui, S. S. (2001). Interrole conflict as a predictor of job satisfaction and propensity to leave: A study of professional accountants. Journal of Managerial Psychology, 16(6), 469-484.
Ma, Q. S. (2009). An integrated framework for information security management. Review of Business, 30(1), 58-69.
Mael, F. A. (1992). Alumni and their alma mater: A partial test of the reformulated model of organizational identification. Journal of Organizational Behavior, 13, 103-123.
Mak, P. (2017). The human factors in cybersecurity and preventing errors. Vircom.
Mandzila, E. E. (2011). Chapitre 1 : Organisation et méthodologie de l'audit interne. In E. Bertin, Audit Interne : Enjeux et pratiques à l'international (pp. 18-19). Groupes Eyrolles.
Mann, L. H. (2008). Professional identity: A framework for research in engineering education. Proceedings of the 19th Annual Conference for Australasian Association for Engineering Education. Yeppoon, Australia.
Maranda McBride, L. C. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. Institute for Homeland Security Solutions, 1-36.
Marks, A. B. (2009). Stuck in the middle with who? The class identity of knowledge workers. Work, Employment & Society, 23(1), 49-65.
Marks, A. H. (2010). Employability and the ICT worker: A study of employees in Scottish small businesses. New Technology, Work and Employment, 25(2), 167-181.
Marks, A. S. (2007). Revisiting technical workers: Professional and organizational identities in the software industry. New Technology, Work and Employment, 22(2), 98-117.
Marks, A. S. (2008). Choreographing a system: Skill and employability in software work. Economic and Industrial Democracy, 29(1), 96-124.
Marks, N. T. (2009). The current state of internal auditing: A personal perspective and assessment. EDPACS, 39(4), 1-23.
Marks, N. T., & Norman, J. R. (2009). The current state of internal auditing: A personal perspective and assessment. EDPACS, 39(4), 1-23.
Marshall, R. (2009). The changing landscape for internal auditors in financial institutions. Bank Accounting & Finance, (February-March), 43-46.
Matthews, E. D., & Harris, J. (2016). Cyber situational awareness. The Cyber Defense Review,

1(1), 35-46.
Mayer, C.-H. (2009). Managing conflicts through strength of identity. Management Revue, 20(3), 268-293.
Mayer, M. d. (2013). International politics in the digital age. The XXVIIth SISP Conference, University of Florence, 12-14 September 2013.
McFadzean, E., & Eckhardt, J. (2006). Anchoring information security governance research: Sociological groundings and future directions. Journal of Information System Security, 3-48.
McNeese, M. D. (2011). Situating cyber situation awareness. Cognitive Technology Journal.
McNeese, M. D., Cooke, N. J., & Rogers, M. (2012). Perspectives on the role of cognition in cybersecurity. Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting, 268-271.
Mead, G. (1933). L'esprit, le soi et la société. University of Chicago Press.
Meier, D. (2022). Le Liban, c'était la suisse du Moyen-Orient. In D. Meier, Le Liban: Du mythe phénicien aux périls contemporains (pp. 37-41). Le Cavalier Bleu.
Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340-363.
Mintzberg, H. (1980). Structure in 5's: A synthesis of the research on organization design. Management Science, 26(3), 322-341.
Mohammed, D. (2017). Cybersecurity compliance in the financial sector. Journal of Internet Banking and Commerce.
Morales, J. (2013). Le projet professionnel des contrôleurs de gestion: Analyser les données pour aider les managers à prendre des décisions rationnelles? Comptabilité - Contrôle - Audit, 19(2), 41-70.
Morgan, S. (2016). Cyber crime costs projected to reach $2 trillion by 2019. Forbes.
Morgan, S., & Cawthorne, E. (2017). Cybercrime damages $6 trillion by 2021. Cybersecurity Ventures Official Annual Cybercrime Report. https://cybersecurityventures.com
Munro, L., & Stewart, J. (2010). External auditors' reliance on internal audit: The impact of sourcing arrangements and consulting activities. Accounting and Finance, 50, 371-387.
Musslebrook, K. (2013). Imagining the future: Workforce. Institute for Research and Innovation in Social Services, 14-15.
Neuman, L. (2007). Social research methods (6th ed.). Pearson Education India.
Niemi, A., & Paasivaara, L. (2007). Meaning contents of radiographers' professional identity as illustrated in a professional journal – A discourse analytical approach. Radiography, 13(4), 258-264.
Nizet, J., & Léonard, M. (2014). Interaction, identité et ordre social: Ouvertures critiques. In La sociologie de Erving Goffman (Vol. 2, 93-106). L. Découverte.
Norris, D., & Young, M. (1984). Professionalism, organizational commitment, and job satisfaction in an accounting organization. Accounting, Organizations and Society, 9, 49-58.
Nykodym, N., Taylor, R., & Vilela, R. (2006). Fighting cybercrime. Journal of General Management, 31(4), 63-70.
Nzoho, D. A. (2009). Problématique de l'audit interne dans la gestion des entreprises publiques en République Démocratique du Congo, cas de la SNCC. ISC Kisangani.
O'Shea, K. (2003). Cyber attack investigative tools and technologies. Hanover.
Oandasan, I., & Conn, L. R. (2006). Teamwork in healthcare: Promoting effective teamwork in

healthcare in Canada. Canadian Health Services Research Foundation, 1-23.
OCRCVM. (2014). Guide de pratiques exemplaires en matière de cybersécurité à l'intention des courtiers membres de l'OCRCVM. Canada: Juno Risk Solutions.
Office of the Press Secretary. (2016). Remarks by the President on the Cybersecurity National Action Plan. The White House.
Onwubiko, C. (2009). A security audit framework for security management in the enterprise. Proceedings of 5th International Conference ICGS3, London, 9-17.
Osty, F. (2002). Le désir de métier: Engagement, identité et reconnaissance au travail. Rennes: Presse Universitaire de Rennes.
Oxford University Press. (2014, May 30). Oxford Online Dictionary. Retrieved from Oxford Dictionaries.
Paape, L., & Scheffe, J. (2003). The relationship between the internal audit function and corporate governance in the EU – A survey. International Journal of Auditing, 7(3), 247-262.
Pace, C. (2015). Legacy systems create a cyber-security loophole. Wallix Trace, Audit & Trust.
Paillé, P., & Mucchielli, A. (2012). L'analyse quantitative en sciences humaines et sociales. Armand Colin.
Pavlou, P. A., & Gefen, D. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS Quarterly, 105-136.
Pavlovska, A. (2018). Cyber security in the bank sector: Can IT outsourcing help? Sayenko Kharenko, 1-3.
Payette, J. (2014). Resolving legitimacy deficits in technology startups through professional services practices. The Technology Innovation Management Review.
Penuel, K. B., & Statler, M. (2013). Cyber crime. In Encyclopedia of Crisis Management, 216-217.
Pereira, T. S. M., & Silva, H. S. (2010). A security framework for audit and manage information systems. In Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (pp. 505-508). IEEE.
Perosino, L. (2019, December 12). L'insurrection au Liban: Révolution, unité et crise économique. Le Vent Se Lève. Retrieved from [lvsl](https://lvsl.fr/linsurrection-au-liban
Perrenoud, M., & Cattin, M. (2018). Pour ne pas en finir avec l'identité au travail: Introduction au dossier "Identité au travail, identités professionnelles." Sociologies.
Pettigrew, A. (1985). The awakening giant: Continuity and change in Imperial Chemical Industries. Oxford/New York: Basil Blackwell.
Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. Organization Science, 1(3), 265-292.
Peusquens, R. (2017). CSP, not 007: Integrated cybersecurity skills training. In F. Abolhassan, Cyber security: Simply make it happen (pp. 71-74). Germany: Springer International Publishing AG.
Pezé, S. (2012). La construction identitaire en situation : Le cas de managers à l'épreuve de la détresse de leurs collaborateurs (Doctoral thesis). Paris 9.
Pfeffer, J., & Salancik, G. R. (2003). The external control of organizations: A resource dependence perspective. Stanford, CA: Stanford University Press.
Phillips, B. (2013). Information technology management practice: Impacts upon effectiveness. Journal of Organizational & End User Computing, 25(4), 50-74.

Ponemon Institute. (2012). 2012 Cost of Cyber Crime Study: United States. Ponemon Institute Research Report.
Power, M. (1991). Educating accountants: Towards a critical ethnography. Accounting, Organizations and Society, 16(4), 333-353.
Power, M. (1995). Auditing, expertise, and the sociology of technique. Critical Perspectives on Accounting, 6(4), 317-339.
Pratt, M. G. (2012). Promoting positive change in physician–administrator relationships: The importance of identity security in managing intractable identity conflicts. In Using a Positive Lens to Explore Social Change and Organizations: Building a Theoretical and Research Foundation (pp. 267-284).
Press, N. A. (2013). Cybersecurity, the cybersecurity workforce, and its development and professionalization. In Professionalizing the nation's cybersecurity workforce? Criteria for Decision-Making (pp. 1-13). Washington, D.C.: National Academy of Sciences.
Pribish, M. (2015). Business cybersecurity is a team sport. azcentral.
PricewaterhouseCoopers. (2007). State of the internal audit profession study: Pressures build for continual focus on risk. PwC.
Prot, B. (2022). Le secteur bancaire français : un levier de croissance et d'emplois. Revue d'économie financière, 104, 11-24.
PwC. (2009). State of the internal audit profession study: Internal audit weighs its role amid the recession and evolving enterprise risks. New York: PricewaterhouseCoopers.
Qribi, A. (2010). Socialisation et identité. L'apport de Berger et Luckmann à travers "la construction sociale de la réalité". Bulletin de psychologie, 506(2), 133-139.
Quader, F. (2016). Cybersecurity: It all comes down to the human factor. First Republic Bank.
Rajivan, P. C. (2013). Cyber situation awareness and teamwork. Security and Safety, 1(13).
Rajivan, P. C. (2017). Impact of team collaboration on cybersecurity situational awareness. Computer Science, 10030, 203-226.
Randazzo, M. R. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. Carnegie Mellon Software Engineering Institute, 23-25.
Reding, K. F. (2015). Manuel d'audit interne: Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques. IFACI, Eyrolles, IIA.
Redins, L. (2021, November 19). Cybersecurity: Who is responsible? Récupéré de Cybersecurity Guide: https://cybersecurityguide.org/resources/cybersecurity-responsibility/
Reed, M. I. (1996). Expert power and control in late modernity: An empirical review and theoretical synthesis. Management School, 17(4), 573-597.
Refsdal, A. S. (2015). Cyber-Risk Management. Springer International Publishing.
Renard, J. (2017). Théorie et pratique de l’audit interne (1st ed.). Saint Germain: Groupe Eyrolles.
Réseau Canadien des comités d'audit. (2013). La cybersécurité et le comité d'audit. VantagePoint, 1-15.
Rhee, H. R. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221-232.
Ridley, A. J. (1996). Internal auditing: A profession for the 21st century. IIA.
Robertson, C. (2011). Organizational management of conflicting professional identities. Case Western Reserve University, 603-622.

Robson, K. H. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. Accounting, Organizations and Society, 32, 409–438.
Rogers, M. (2015). Cybercom chief: Cyber threats blur roles, relationships. U.S. Department of Defense. DoD News, Defense Media Activity.
Rok, B. B.-B. (2008). An economic modeling approach to information security risk management. International Journal of Information Management, 28(5), 413-422.
Rosencrance, L. (2021, January 1). Tech Accelerator Guide to Building and Executing an MSP Business Model. TechTarget IT Channel. Récupéré de https://www.techtarget.com/searchitchannel/definition/service-level-agreement
Rubenstein, S., & Altman, R. (2008). Are your medical records at risk? Wall Street Journal, 251(100), D1-D2.
Russell, D. G. (1993). Computer security basics (ISBN: 0-937175-71-4). Sebastopol, CA: O'Reilly & Associates, Inc.
Sachs, J. (2001). Teacher professional identity: Competing discourses, competing outcomes. Journal of Education Policy, 16(2), 149-161.
Sagnol, M. (1987). Le statut de la sociologie chez Simmel et Durkheim. Revue Française de Sociologie, 28(1), 99.
Sainsaulieu, R. (1988). L'identité au travail (3rd ed.). Paris: Presses de la Fondation Nationale des Sciences Politiques.
Sainsaulieu, R. (1994). Sociologie de l'entreprise: Organisation, culture et développement. Presse Sciences Po et Dalloz.
Sanchez, J.-P. (2014). Sécurité informatique : Dis-moi qui tu es, je te dirai comment te protéger. La Tribune.
Sarens, G. (2009). Internal auditing research: Where are we going? International Journal of Auditing, 13, 1-7.
Sarfatti-Larson, M. (1988). À propos des professionnels et des experts. Sociologie et sociétés, 20, 23-40.
Savoie-Zajc, L. (2000). La recherche qualitative/interprétative en éducation. Introduction à la recherche en éducation, 2, 171-198.
Schmidt, L., & Lara, C. O. (2015). IT and InfoSec have different workforce management practices. In Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector? (pp. 11-32). RAND Corporation.
Schneiderman, A. (2017). A.G. Schneiderman announces SHIELD Act to protect New Yorkers from data breaches. New York: Attorney General's Press Office.
Schwartz, S. J. (2011). Handbook of identity theory and research. New York, USA: Springer.
Sebti, H. (2016). L'utilisation des systèmes de contrôle dans la dynamique des groupes professionnels : Le cas des acheteurs dans les partenariats entre clients et fournisseurs. Paris: Dauphine Recherche en Management (DRM).
Secretariat of the Security Committee. (2013). Finland's Cyber Security Strategy - Government Resolution. Helsinki, Finland: Secretariat of the Security Committee.
Selim, G. (2009). Internal auditing and consulting in practice: A comparison between UK/Ireland and Italy. International Journal of Auditing, 13, 9-25.
Shaikh, F. J. (2019). Effects of information security legitimacy on data breach consequences: Moderating effect of impression management. In SIGMIS-CPR '19 (pp. 118-121). Nashville,

TN, USA.
Shils, E. (1965). Charisma, order, and status. American Sociological Review, 30(2), 199-213.
Simmonds, A., Sandilands, P., & van Moorsel, A. (2004). An ontology for network security attacks. In Proceedings of the 18th Annual Computer Security Applications Conference (pp. 317-323).
Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What everyone needs to know. Oxford University Press.
Singh, A. N. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14(4), 225-239.
Skorikov, V. B. (2011). Occupational identity. In S. J. Schwartz, K. Luyckx, & V. L. Vignoles (Eds.), Handbook of identity theory and research (pp. 693-714). Springer.
Smith, S. (2016). An exploration of professional identity in the information technology sector (Doctoral thesis, Edinburgh Napier University). Edinburgh.
Solms, R. v. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.01.007
Soomro, Z., & Nizamani, S. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.10.008
Soussi, R. (2022, March 28). La cybersécurité en manque de jeunes diplômés ! Studyrama. https://www.studyrama.com
Stanganelli, J. (2014). Collaboration is key to cybersecurity. Enterprise Networking Planet. https://www.enterprisenetworkingplanet.com
Steinbart, P. J. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 1-15. https://doi.org/10.1016/j.aos.2018.01.001
Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems, 13, 228-243.
Stewart, A. (2012). Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor. Information Management & Computer Security, 20(4), 312-326. https://doi.org/10.1108/09685221211289639
Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571-610. https://doi.org/10.5465/amr.1995.9508080331
Suddaby, R. B. (2019). Professional judgment and legitimacy work in an organizationally embedded profession. Journal of Professions and Organization, 6, 105-127. https://doi.org/10.1093/jpo/joy019
Sumners, G. S. (2008). Addressing internal audit staffing challenges. EDPACS, 37(3), 1-11. https://doi.org/10.1080/07366981.2008.10766433
Symantec Corporation. (2011). Norton cybercrime report: Cybercrime costs $338bn to global economy; More lucrative than drugs trade. Mountain View, CA.
Tajfel, H. (1978). Differentiation between social groups: Studies in the social psychology of intergroup relations (Vol. 14). Academic Press.
Tajfel, H., & Austin, W. G. (1985). The social identity theory of intergroup behavior. In S.

Worchel & W. G. Austin (Eds.), Psychology on intergroup relations (2nd ed., pp. 7-24). Nelson-Hall.
Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), Psychology of intergroup relations (pp. 7-24). Nelson-Hall.
Tap, P. (1991). Socialisation et construction de l'identité personnelle. In A. Defossez & J. C. Boulanger (Eds.), La socialisation de l'enfance à l'adolescence (pp. 49-74). PUF.
Tap, P. (2005). Identité et exclusion. Connexions, 83(1), 53-78. https://doi.org/10.3917/connex.083.0053
Tap, P. R. (2013). La dynamique personnelle et les identités professionnelles, en situation de changement. Les Cahiers Internationaux de Psychologie Sociale, 99-100(3), 385-407.
Tap, P., & Lecomte, J. (2016). Marquer sa différence. InC: Identité(s), 46-50.
Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 1-11.
The National Cybersecurity Society. (2023, July 16). Service level agreements (SLA). Nationalcybersecuritysociety.org. https://nationalcybersecuritysociety.org/wp-content/uploads/2018/03/FACT-SLAs-FINAL.pdf
The White House, Office of the President. (2015). Fact sheet: White House summit on cybersecurity and consumer protection. Washington, D.C.: The United States Government.
Thornton, P. H. (2002). The rise of the corporation in a craft industry: Conflict and conformity in institutional logics. Academy of Management Journal, 45(1), 81-101. https://doi.org/10.5465/amj.2002.5922397
Tindall, D. (2013). Importance of people, process, and technology to cybersecurity effectiveness. Insecurity, Honeywell Process. https://www.honeywellprocess.com
Tolbert, P. S. (1990). A review of The system of professions: An essay on the division of expert labor by Andrew Abbott. Administrative Science Quarterly, 35, 410-413. https://doi.org/10.2307/2393312
Touhill, G. J. (2014). Cybersecurity for executives: A practical guide. Wiley.
Trcek, D. T. (2007). Information systems security and human behavior. Behaviour & Information Technology, 26(2), 113-118. https://doi.org/10.1080/01449290500524433
Trouchaud, P. (2016). La cybersécurité au-delà de la technologie. Odile Jacob.
Trouchaud, P. (2018). La cybersécurité face au défi de la confiance. Odile Jacob.
UIT. (2009). Recommandation UIT-T X.1205. UIT.
Valparaiso University, U. S. (2017, November 21). Cybersecurity vs. information security – Is there a difference? Valparaiso University. http://onlinecybersecurity.valpo.edu/news/cyber-security-vs-information-security/
Vance, A. L. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263-290. https://doi.org/10.2753/MIS0742-1222290409
Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263–290.
Vaseashta, A. S. (2014). Cybersecurity – Threat scenarios, policy framework and cyber wargames. In Cybersecurity and Resiliency Policy Framework (p. 3). IOS Press.
Venkatraman, S. D. (2008). Biometrics in banking security: A case study. Information

Management & Computer Security, 16(4), 415-430. https://doi.org/10.1108/09685220810905977
Vessié, B. (2014). Cours de contrôle interne et de gestion des risques. UCL-Mons.
Veyne, P. (1971). Comment on écrit l'histoire. Éditions du Seuil.
Visner, S. (2016). Rethinking managed security. Semantic Scholar. https://www.semanticscholar.org
Von Solms, R. V. (2013). From information security to cybersecurity. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.01.007
Vuko, T. S. (2021, September 28). Key drivers of cybersecurity audit effectiveness: The neo-institutional perspective. SSRN. https://ssrn.com/abstract=3932177
Wacheux, F. (1996). Méthodes qualitatives et recherche en gestion. Economica.
Wacheux, F. (1997). La gestion des ressources humaines et l'épistémologie du quotidien (Cahier n° 97/01). Université Paris 1 - Panthéon-Sorbonne.
Wall, D. S. (2005). The Internet as a conduit for criminal activity. In M. D. L. Bell & D. S. Wall (Eds.), Information technology and the criminal justice system (pp. 77-98). Routledge.
Walsh, K., & Quinlan, C. (2008). Creating an individual work identity. Human Resource Management Review, 18(1), 46-61. https://doi.org/10.1016/j.hrmr.2008.04.002
Walters, R. (2016). Cyber attacks on U.S. companies in 2016. The Heritage Foundation. https://www.heritage.org
Wamala, F. (2011). ITU National cybersecurity strategy guide. International Telecommunication Union.
Watson, T. (2008). Managing identity: Identity work, personal predicaments, and structural circumstances. Organization, 15(1), 121-143. https://doi.org/10.1177/1350508407084897
Watson, T. J. (2009). Narrative, life story, and manager identity: A study case in autobiographical identity work. Human Relations, 62, 425-452. https://doi.org/10.1177/0018726708102007
Webb, S. (2015). Professional identity and social work. In 5th International Conference on Sociology and Social Work: New Directions in Critical Sociology and Social Work: Identity, Narratives, and Praxis (pp. 1-22). Glasgow.
Webb, S. (2015). Professional identity and social work. In 5th International Conference on Sociology and Social Work: New Directions in Critical Sociology and Social Work: Identity, Narratives, and Praxis. Chester, England.
Weber, A. (1909). The theory of the location of industries. The University of Chicago Press.
Weiss, J. A. (2010). Changing roles of technology leaders: Strategic partners or high-level mechanics? In HICSS '10 Proceedings of the 2010 43rd Hawaii International Conference on System Sciences. IEEE Computer Society. https://doi.org/10.1109/HICSS.2010.35
Whitman, M. E. (2012). Information security governance for the non-security business executive. Journal of Executive Education, 11(1), 97-111.
Wikipedia. (2020). Audit committee. Wikimedia Foundation, Inc. https://en.wikipedia.org/wiki/Audit_committee
Wilson, A. (2017). Tech can be competitive, but in cybersecurity, collaboration is key. The Guardian Labs, PwC Partner Zone. https://www.theguardian.com
Yang, S. M. (2005). The impacts of establishing enterprise information portals on e-business performance. Industrial Management & Data Systems, 105(3), 349-368.

https://doi.org/10.1108/02635570510585546
Yaping, Y. (2018). Literature review of information security practice survey reports. Service Innovation and Management, Master's Thesis, 5-10.
Yeniman, Y. E. (2011). Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), 360-365. https://doi.org/10.1016/j.ijinfomgt.2010.09.007.

TABLES DES ILLUSTRATIONS ET DES MATIERES

Table des illustrations

Table des figures

Table des matières

ANNEXES
ET RESUMES

Annexes

ANNEXES A : GUIDE D'ENTRETIEN AUPRÈS DE LA BPVF ET DES ÉTABLISSEMENTS BANCAIRES LIBANAIS

A1. Modèle du guide d'entretien

A2. Guide d'entretien auprès de la BPVF

A2.1 Guide d'entretien avec le RSSI

A2.2 Guide d'entretien avec le responsable informatique

A2.3 Guide d'entretien avec le Chef de mission d'audit interne

A2.4 Guide d'entretien avec le superviseur d'audit interne

A2.5 Guide d'entretien avec le directeur des risques conformité et contrôle permanent

A3. Guide d'entretien sur les banques libanaises

A3.1 Guide d'entretien avec un analyste principal informatique chez banque of Beirut (BOB)

A3.2 Guide d'entretien avec un auditeur interne informatique chez Banque

ANNEXES B : MÉTHODOLOGIE DE CODAGE DES GUIDES D'ENTRETIEN

B1. Méthodologie de codage du guide d'entretien du directeur des risques de conformité et contrôle permanent à la BPVF

B2. Méthodologie de codage du guide d'entretien du directeur de l'audit interne à la BPVF

B3. Méthodologie de codage du guide d'entretien du chef de mission de l'audit interne à la BPVF

B4. Méthodologie de codage du guide d'entretien du superviseur de l'audit interne à la BPVF

ANNEXES C : LES SCHÈMES SPÉCIFIQUES

C1. Schème spécifique du RSSI D.G au sein de la BPVF

C2. Schème spécifique du directeur de l'audit interne M.C au sein de la BPVF

C3. Schème spécifique du directeur de la conformité P.G au sein de la BPVF

C4. Schème spécifique du directeur de l'audit interne P.C au sein de l-IBP

C5. Schème spécifique du chef de mission audit interne T.L au sein de la BPVF

ANNEXES D : LISTE D'ACRONYMES

D1. Liste d'acronymes des termes techniques et non techniques

Annexe A : guide d'entretien auprès de la BPVF et des établissements bancaires libanais

A1. Modèle du guide d'entretien

Le Guide d'entretien

Présentation personnelle :

Bonjour,

Je m'appelle « Jean-Jacques Yammine ». J'ai 28 ans et je suis libanais.

Actuellement, je réalise un doctorat à l'IAE de Poitiers en audit interne sous la direction de Monsieur « Jérôme Méric » qui s'effectuera sur une durée minimale de trois ans au sein du laboratoire CEREGE.

Le sujet que je traite est le suivant : « Rôle de l'audit interne dans la cybersécurité d'établissement bancaire : une collaboration inter fonctionnelle au prisme des identités professionnelles ». Alors que le terrain que je favorise est celui des banques.

En effet, la question de la cybersécurité est particulièrement sensible dans le cas de ces établissements. J'ai décidé de choisir votre banque pour étudier ce projet.

Je vous remercie de me recevoir aujourd'hui et de me consacrer du temps.

En quelques mots, l'entretien d'aujourd'hui fait partie de la recherche qualitative dans la partie pratique de ma thèse.

En particulier, cette thèse propose une analyse méthodologique de l'audit interne en vers la cyber sécurité dans les banques, à travers :

- L'étude de l'audit interne et en particulier celui des systèmes d'informations et son positionnement par rapport à la cyber sécurité.
- L'analyse de la cyber sécurité au niveau des banques.
- L'étude des différentes formes d'audit, ainsi que ses référentiels et ses procédures relatifs à la cyber sécurité.
- La mise en œuvre de l'audit interne et son champ d'application sur le terrain.
- La place de l'audit interne face à la fraude et les cybers attaques.
- L'initiation du protocole adopté pour conduire l'audit interne.
- L'analyse de l'impact du système d'information sur l'audit interne et le contrôle de gestion.
- L'évaluation des risques liés à la cyber sécurité par les différentes parties.
- L'impact de la technologie sur le travail de l'auditeur interne, la comptabilité et les documents financiers.
- La gestion de la sécurité du cyber espace.
- La relation de l'auditeur interne avec les différentes parties dans la banque pour maintenir la cyber sécurité.

Les entretiens que je réalise vont être des entretiens non directifs et biographiques.

Bien entendu, tout ce qui sera dit au cours de cet entretien restera absolument confidentiel.

Si je vous propose de l'enregistrer, c'est pour faciliter notre discussion et éviter des erreurs dans ma prise de notes.

Si vous le désirez, je vous remettrai un disque compact une fois que je transcris les informations qui sont nécessaires à notre recherche.

La durée de l'entretien en devrait en principe pas excéder une heure.

Je tiens à dire qu'il n'existe pas de bonne ou mauvaise réponse, ce que je cherche à savoir, c'est bien comment vous définiriez la cyber sécurité, ses enjeux et de savoir vos rôles respectifs et les outils de contrôle mis en œuvre ainsi de mieux comprendre les relations avec les différents acteurs afin de la maintenir.

C’est pourquoi je vous demanderai d’être le plus complet possible dans vos réponses.
Avez-vous des questions ?

I. Questions Propres

1. Qu’est-ce que vous avez faits pendant vos études ?
2. Comment avez-vous trouvez ce travail ?
3. Pouvez-vous nous expliquer votre rôle et vos missions ?
4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?
5. D’après vous, quelles sont les qualités requises d’un superviseur d’audit?
6. Justement, quel est le degré d’interaction que vous avez avec les réseaux métier en termes de SSI ?

II. Lien avec l’entreprise

7. Pourquoi travaillez-vous dans le secteur bancaire ?
8. Pourquoi travaillez-vous dans cette banque ?
9. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?
10. Selon vous, ce qui vous valorise dans votre travail, est ce que c’est votre expérience antérieure ou votre expérience après ?
11. Pourquoi travaillez-vous ?
12. Combien de salariés ? de départements ?

III. Cyber sécurité

13. Que penser vous lors que vous entendez le terme « cyber sécurité » ?
14. Commenter une mission de cyber sécurité.
15. Quelles difficultés y rencontre-t-on ?
16. Qui est cette personne qui est embauché ? Son Poste ?
17. Qui est responsable de maintenir la cyber sécurité dans la banque ?
18. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? Sont-elles été suivies ?
19. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?
20. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?
21. Les employés ont-ils besoin d’une formation régulière sur la sensibilisation à la cybersécurité?
22. Pouvez-vous m’expliquer le travail que vous faites avec les opérateurs informatiques ? Quelle est la relation en matière de cyber sécurité ? c’est-à-dire comment vous travailler ensemble ?
23. Pouvez-vous m’expliquer pourquoi ils ont recours à ce service extérieur ? Quelle est la raison ? Comment s’effectue la démarche ?
24. Certaines disent de confier à l’audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c’est-à-dire s’ils disent c’est le rôle de l’audit interne de maintenir la cyber sécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
25. Selon les entretiens que j’ai réalisés dans votre banque, la plupart ont dit que c’est le rôle de Mr Didier G. de maintenir la cyber sécurité. Commenter.

IV. L’audit interne

1. Votre banque, devrait-elle avoir une fonction d’audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?
2. Décrivez l’auditeur interne dans son travail.
3. Comment la fonction d’audit interne conserve-t-elle son indépendance et son objectivité ?
4. Votre fonction est-elle agile et prête à s’améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?

V. Les autres acteurs

1. Pourriez-vous envisager l’intervention d’autres experts pour maintenir la cyber sécurité ?
2. Comment tenir la direction responsable de la prise en considération des constations d’audit

et de la mise en œuvre des mesures correctives ?
3. Parler de votre mission d'audit sur les responsables de TI.
4. Comment la fonction d'audit interne coordonne-t-elle son travail avec celui des auditeurs externes, de façon à assurer une couverture adéquate des questions à traiter, quelle que soit son approche à l'égard de la dotation en personnel ? Aussi relation avec les responsables de TI ?
5. Décrit l'auditeur interne, lorsqu'il vient faire son travail ?
6. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ? Commenter.
7. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ? avec les employés ?
8. Comment faites-vous pour établir de bonnes relations avec les employés ?
VI. Bref Questionnaire Socio démographique
1. Sexe
2. Année de naissance
3. Etat-Civil
4. Niveau de formation achevée
5. Profession
VII. En fin d'entretien
1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ?
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ?
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective
6. Signature

A2. Guide d'entretien auprès de la BPVF

A2.1 Guide d'entretien avec le RSSI

Le Guide d'entretien avec le RSSI à la BPVF

I. Questions Propres
1. Qu'est-ce que vous avez faits pendant vos études ?
J'ai passé un baccalauréat en France. Et après, j'ai passé des examens bancaires. Le Certificat d'aptitude professionnelle à la profession des banques et un brevet professionnel de banque de trois ans et j'ai fait la première année de l'Institut technique bancaire ITB.
2. Comment avez-vous trouvez ce travail ?
J'ai trouvé ce travail, Euhhhh, en envoyant des CV dans plusieurs banques, et j'ai été retenu dans la banque populaire.
3. Pouvez-vous nous expliquer votre rôle et vos missions ?
Alors je suis responsable des risques opérationnels, Au sein de la direction des risques et du contrôle permanent et de la conformité de la BPVF. J'ai également en charge les plans d'urgence et de poursuite d'activité et la sécurité des systèmes d'information.
4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?
Mon parcours, ça a été un parcours à la profession bancaire pendant une trentaine d'année. Donc, j'étais responsable du traitement des chèques au moyen de paiement. Ensuite, j'étais responsable de la monnaie c'est-à-dire tout ce qui tourne autour des cartes bancaires. Ensuite, j'étais responsable de l'ensemble des moyens de paiement, les chèques, les virements, les traitements, les cartes bancaires, les moyens de paiement internationaux. Et on m'a fait opposition compte tenu de mes connaissances de production bancaire. On m'a fait la proposition de m'occuper de risques

opérationnels. C’est une suite un peu logique.
5. D’après vous, quelles sont les qualités requises d’un RSSI?
Et travailler en mode transversale, travailler en équipe. Et d'avoir une bonne communication. Et de soigner le relationnel, les relations avec des gens, être rigoureux, organiser.
6. Lorsque vous dites les gens ? c’est les clients ? ou les employés ?
En effet, les autres métiers de la banque.
7. Pouvez-vous me citer les postes de ces employés ?
Il y a le responsable des moyens de paiement, les responsables des crédits, les responsables d’épargne, les responsables d’assurance, les responsables ressources humaines, les responsables communication, les responsables immeubles sécurités, ce sont des banques plus que dans le réseau d’agence.
II. Lien avec l’entreprise
8. Pourquoi travaillez-vous dans le secteur bancaire ?
Parce que quand j'étais jeune, la banque avait bonne réputation et c’était un peu la sécurité dans travailler dans une banque.
9. Pourquoi travaillez-vous dans cette banque ?
Parce que c’est une banque à taille humaine. Il y a des valeurs coopératives qui me correspondent bien. En plus, c’est à proximité de mon domicile.
10. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?
Oui, je pense.
11. Selon vous, ce qui vous valorise dans votre travail, est ce que c’est votre expérience antérieure ou votre expérience après ?
Oui, je crois mon expérience d'après, enrichit par la profession bancaire.
12. Pourquoi travaillez-vous ?
Pourquoi je travail ? Je travaille pour gagner ma vie, pour élever ma famille d'une part, et parce que j'ai envie de travailler sur ces domaines-là, parce que ça m'intéresse, d'autre part. Mais bon, je travaille parce que j'ai besoin de travailler pour gagner ma vie comme tout le monde.
13. Combien de salariés ? de départements ?
Justement ? Euhhhh, je n’en sais rien, il pourrait y avoir une dizaine de directions.
III. Cyber sécurité
14. Que penser vous lors que vous entendez le terme « cyber sécurité » ?
Sécurité internet, risque de fraude, risque d’attaques, risque de fuites de données, risque d’arrêt d’activité, risque de cyber malveillant, risque cyber fraude. Je pense au risque, mais je pense aussi à autre mesure pour réduire ce risque.
15. Commenter une mission de cyber sécurité.
Ouais, déjà, je vous rappelle un peu de notre propre organisation dans le groupe BPCE. Oui, oui, il y a un opérateur informatique qui est IBP, Vous avez eu l'occasion de discuter avec le responsable de l'audit IBP, et il y a BPCIT l'opérateur informatique pour la profession informatique, donc les alertes, des cybers attaques viennent d’eux, de ces opérateurs.
Et dans la banque, on se met en cas d'attaque, on se met en mode de gestion de crise avec tous métiers qui sont concernés dans la banque pour faire face à l'attaque et pour appliquer des mesures, des contres mesures qui vont nous être demandées par les opérateurs informatiques d'une part, et dans la pilule de crise, on a aussi le métier de communication qui communiquera si nécessaire aux collaborateurs de la banque et ou aux clients, s’il y a des attaques sur les clients.
16. Comment vous agissez dans votre rôle ? Qu’est-ce que vous faites ?
Moi, personnellement, en tant que responsable de la sécurité des systèmes d'information en cas de crise et moi qui réunirait la cellule de crise avec tous les métiers dont je vous ai parlé tout à l’heure. Et c’est moi qui fais l’interface entre ces métiers et les opérateurs informatiques.
17. Vous me disais que vous allez suivre les instructions de l’opérateur informatique comment agir sur cette incidence spécifique. Commentez.
Oui selon un protocole. Alors, normalement, il y a un protocole de gestion de crise au niveau des

opérateurs informatiques qui lorsqu'ils sont avertis d'une cyber attaque importante. Ils réuniraient les RSSI des établissements rattachés à ces opérateurs. En cellule de crise, charge après au responsable de la sécurité des systèmes d'information d'établissements de réunir sa propre cellule de crise dans l'établissement.

18. Quelles difficultés y rencontre-t-on ?

Les difficultés. La difficulté est bien et de bien analyser les impacts que ce soit pour les collaborateurs ou les clients. De bien analyser les risques, de bien soigner sa communication, la communication, c'est important que ce soit vers les collaborateurs pour qu'ils ne fassent pas des choses qui aggraverait la situation ou vis à vis des clients, surtout si l'indisponibilité du service consécutif à cette cyber attaque.

19. Qui est responsable de maintenir la cyber sécurité dans la banque ?

C'est ce que je vous ai expliqué plutôt le travail des opérateurs informatiques. On confit notre informatique à un opérateur et c'est eux qui sont en charge de mettre en place des contres mesures pour éviter le risque de cyber attaque.

20. Durant mon entretien avec Mr Pascal Gombert, il a commenté en disant que le rôle de maintenir la cyber sécurité dans notre banque est le rôle seulement du RSSI Mr Didier G.. Commenter.

Oui, Pascal Gombert a raison.

Dans chaque établissement, on a nommé un responsable de la sécurité des informations pour la BPVF : c'est moi et c'est à moi de mettre en place, de faire appliquer la politique de sécurité des systèmes d'information par les collaborateurs, car moi de faire la sensibilisation des collaborateurs aux comités des risques qui nous passent sur des liens. Mais quand vous me posez la question qui est responsable de la cyber sécurité sur nos infrastructures informatiques, ce sont les opérateurs informatiques.

21. Operateurs informatiques ? C'est comme technicien informatique ? Comme Manuel Coulon ?

Non, quand je vous parle des opérateurs informatiques, ce sont les collaborateurs du groupe BPCE-IT. C'est une structure à part entière responsable du service informatique de toutes les banques populaires et de toutes les caisses d'épargnes qui font partie du groupe BPCE.

22. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? sont-elles été suivies ?

Oui, on a des modules de formation que les collaborateurs suivent.

23. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?

Oui, on a mis en place un comité interne de sécurité. On prépare les incidents et on intervient sur ce domaine.

24. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?

Surtout par la sensibilisation des collaborateurs à mon niveau, c'est Surtout par la sensibilisation des collaborateurs, pour appliquer des règles de sécurité, et pour ne pas se faire piéger par des attaques de phishing, à vocation…

25. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cybersécurité?

Oui. Il faut répéter, répéter, répéter.

26. La surveillance efficace de la cyber sécurité est-elle assurée ?

Oui. Elle est assurée par BPCE-IT.

Oui. Elle est assurée par BPCE-IT. Oui. Elle est assurée au niveau des opérateurs informatiques.

27. Pouvez-vous m'expliquer le travail que vous faites avec les opérateurs informatiques ? Quelle est la relation en matière de cyber sécurité ? c'est-à-dire comment vous travailler ensemble ?

On travaille ensemble à deux niveaux. Premier niveau, on a le groupe BPCE, admit la filière des RSSI avec des comités de suivi réguliers trimestriels et réellement où les plans d'action des

actualités nous sont donnés. Ça c'est au niveau de l'animation par BPCE de la filière des RSSI.
Et du temps. Et donc, parmi cette animation, il y a tous les RSSI, bien réfléchi les opérateurs, des débiteurs logiciels.
Et en deuxième niveau, au niveau quotidien, nous recevons ces informations, par mail, du groupe BPCE sur ces questions de sécurité, dès lors des alertes, dès lors des clients qui s'ont piégé...
28. Pouvez-vous m'expliquer le travail que vous faites avec les auditeurs internes ? Quelle est la relation en matière de cyber sécurité ?
Les auditeurs peuvent mener des missions d'audit sur la cyber sécurité, et m'interviewé comme ils interviewent les autres départements de banque. Dans un autre sens, moi je n'ai pas de relation avec l'audit.
29. Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cyber sécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
Là ce n'est pas le choix qui a été fait par le groupe BPCE parce que l'audit est un contrôle périodique dans le dispositif de contrôle permanent qui s'applique en France.
L'audit est une structure qui fait du contrôle périodique et non pas du contrôle en permanence. Donc je ne pense pas qu'il doit adapter le fait que l'audit est confié à maintenir la cyber sécurité. L'audit peut faire des missions périodiques sur les apparts de la cyber sécurité mais ne pas la maintenir en totale.
Je pense que le traitement opérationnel de la sécurité des systèmes d'information doit être au plus près des métiers. Il faut que ce soit très opérationnel par des gens qui ont des expertises et une connaissance de la sécurité des systèmes d'information. Le « RSSI », lui il intervient en deuxième niveau sachant que les opérationnels de la sécurité interviennent en premier niveau. Le « RSSI » doit réaliser un certain niveau de contrôle pour s'assurer que le premier niveau est bien réalisé.
L'audit, de mon point de vue, c'est la règlementation des contrôles qui, en France et en Europe, intervient en troisième niveau, et effectue des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. Donc, l'audit n'est pas dans un rôle opérationnel, mais effectue des missions en troisième niveau qui peuvent être beaucoup plus longues et plus approfondies mais ne sont pas dans le traitement opérationnel. Ils vont s'assurer que les dispositifs fonctionnent, qu'il n'y a pas de failles ou s'il y a des failles, ils vont émettre des recommandations. Mais ils ne sont pas dans le quotidien de la cyber sécurité. Ce n'est pas l'organisation du contrôle qui existe chez nous en France, où l'audit est en troisième niveau, il n'est pas en opérationnel sur la sécurité des systèmes d'information.

30. Les cyberattaques représentent aujourd'hui une réelle menace pour les entreprises. Comment appréhendez-vous cette menace ?
On l'appréhende très au sérieux justement par une organisation qu'on espère est efficace, où on a mis en place au niveau « BPCE », encore une fois une politique de sécurité des systèmes d'information, c'est-à-dire une politique à plusieurs niveaux au moins à deux niveaux. Le premier niveau, c'est une charte ou un cadre de fonctionnement de la sécurité des informations qui dit comment on doit être organisé : Quel est le rôle du « BPCE » ? Quel est le rôle des opérateurs informatiques ? Quel est le rôle des établissements bancaires ? A l'intérieur de chacune des ces structures, comment on doit être organisé ? Comment on doit échanger ? Quels outils on doit mettre en place ?
C'est le premier niveau et c'est la charte de fonctionnement, le cadre d'application pour dire que tous les établissements doivent respecter de manière homogène pour lutter contre la cyber sécurité.
Le deuxième niveau de la politique, c'est un référentiel de règles de la sécurité des systèmes d'informations qui s'appliquent à tous les établissements du groupe « BPCE » et un certain nombre de règles que je ne peux pas tous les citer. Évidemment, il y a plusieurs centaines qui vont vous dire par exemple :

• Qu'un mot de passe doit faire tant de caractères pour être suffisamment robuste dans tous les établissements du groupe.
• Que les proxys doivent être installés là où c'est nécessaire.
• Que les messageries doivent être sécurisées.
• Que dans tous les domaines de l'informatique, des règles de sécurité doivent être appliqués, c'est-à-dire c'est le deuxième niveau de la politique de sécurité des systèmes d'information, au-dessous du cadre qui fixe le fonctionnement.

Donc, on appréhende ce risque surtout, par une politique d'une part, on appréhende aussi ce risque par …

31. Pouvez-vous me parler de votre plan actuel d'intervention en cas de cyber incident?

Avec les règles de sécurité qui doivent être appliqués et les normes en place, et justement dans ces règles de fonctionnement, il y a aussi des structures qui s'occupent de lutter au quotidien contre la cyber sécurité, avec ce qu'on appelle des « SOC », centre opérationnel de sécurité qui font de la veille sur tout ce qui est menace, tout ce qui vulnérabilité, et qui mènent des actions de réduction des risques au quotidien.

32. Avez-vous déjà dû faire face à des attaques? Comment avez-vous réagi ? Quels sont les types d'attaques les plus fréquentes ?

En établissement bancaire, « BPVF », non.

Au niveau du groupe au des autres banques, il y a des attaques comme dans toutes les entreprises. On a cité « WannaCry » en 2007 qui a touché toutes les entreprises, mais ces attaques, n'ont pas eu d'impact important, en tout cas, au niveau du groupe « BPCE ». Mais il a fallu bien y répondre, mettre les patches nécessaires, mettre les correctifs de sécurité nécessaires.

Donc, il y a des attaques. Il en y a régulièrement en ransomware.

Mais, il y en n'a pas eu pour le groupe « BPCE » d'impacts importants jusqu'à présent.

IV. L'audit interne

33. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?

Oui, c'est comme la sécurité est un métier d'expert, les auditeurs internes dans une banque sont généralistes dans les effets bancaires.

Dans notre banque, il y a un audit interne à la banque qui intervient pour tous les domaines de la banque. Mais sur ces sujets-là de cyber sécurité, on peut faire appel à des auditeurs externes qui ont une compétence technique particulière qu'on n'aurait pas forcement dans nos établissements sur ces sujets-là. Aujourd'hui, si on veut faire des tests d'intrusion sur des systèmes d'informations, on fait des appels à des auditeurs externes.

34. Si ces auditeurs externes viennent, il ne va pas y avoir une collision avec votre travail ou avec les opérateurs informatiques ? Il ne va pas y avoir un conflit ?

Si on décide, ou lorsque les opérateurs décident de faire des tests d'intrusion sur les systèmes, et qu'ils choisissent un auditeur externe. Ils vont bien sûr travailler avec cet auditeur externe.

Ils vont définir ensemble le périmètre de ce qu'ils souhaitent auditer. Ils vont définir ensemble les modalités, le planning, ce qu'ils attendent.

35. Si les auditeurs sont mandatés par l'administration et non pas par les opérateurs informatiques parce que peut-être l'administration pense qu'ils peuvent mieux maintenir la cyber sécurité. Quel est le cas ? Y a-t-il un conflit ?

A ma connaissance, dans nos établissements, les décisions menées des audits sur les systèmes d'information sont faites par l'audit interne ou l'inspection générale du groupe « BPCE ».

Or au niveau de groupe « BPCE », l'audit interne est appelé l'inspection générale. Elle peut décider de faire appel à des auditeurs externes. Mais en règle générale, la décision de faire un audit sur ces sujets-là, elle est confiée à l'inspection générale qui peut alors faire appel à un auditeur externe ou inspection externe.

En revanche, ce qui peut être demandé par l'administration, mais ce qui sera chez nous, le régulateur, la « BCE » banque centrale européenne, elle pourrait exiger qu'on effectue des tests

d'intrusion par exemple selon certaines conditions. Elle peut fixer les conditions de l'audit ce que doit contenir l'audit, quelle est le résultat attendu de l'audit.
Mais sur le choix de l'auditeur, je ne pense pas.
36. Parler de votre relation de travail avec l'audit interne.
Très peu de relation. Quand il y a des missions d'audit de nos domaines, ils viennent nous interviewés. Mais si non, il y a très peu de relation.
37. Parler de votre relation avec l'auditeur hors du travail ?
Je les vois une fois par an, mais c'est tout à fait ça.
38. Parler de votre relation avec l'auditeur hors du travail en décrivant le comportement de l'auditeur interne dans votre travail.
Pas de relation.
39. Avec les autres employés il y a une relation ?
Oui, sur le domaine de la sécurité des systèmes d'information, on a des interlocuteurs dans les différents métiers de l'informatique plutôt, puisqu'on a des relations régulières avec les gens qui s'occupent des habilitations, les contrôles d'accès par exemple, on a des relations régulières avec les gens qui s'occupent des développements privatifs. On a des accès réguliers avec les gens qui s'occupent de l'informationnel c'est-à-dire les entrepôts de données, tout ce qui peut générer des programmes particuliers.
Enfin, le RSSI que je suis, à des relations avec les différents métiers qui s'occupe de l'informatique dans la banque.
40. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?
Vous devez demander cette question à l'audit. Pas vraiment d'avis sur la question.
41. Votre fonction est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?
Oui, c'est une question de domaine, ou ça évolue assez vite, il faut s'adapter en permanence.
42. Comment s'améliorer continuellement ?
En se formant déjà, en faisant de la veille, savoir ce qui se passe, en identifiant régulièrement les nouveaux risques, avec encore une fois des opérateurs informatiques, bien sûr. Et en sensibilisant en fait sur l'audit.
43. Après l'entretien avec Mr GOMBERT et Mr CEZARD, ils m'ont dit que chaque année, votre banque fait intervenir un service extérieur pour faire des formations en cyber sécurité, pour comment améliorer leur travail en cyber sécurité comme Orange ou Thales. Commenter.
Moi, je n'ai pas connaissance d'expert d'orange cyber défense qui viennent à la banque faire une formation. Mais, peut être chez les opérateurs informatiques et pas à la BPVF.
V. Les autres acteurs
44. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?
Oui, on peut envisager de ce qu'on discute tout à l'heure, de faire intervenir des sociétés spécialisées en sécurité informatique pour faire par exemple des tests d'intrusion, sur notre périmètre relatif. Pas au niveau de la banque populaire « Val de France », mais au niveau encore une fois du groupe « BPCE », ils font intervenir des experts puisqu'on travaille avec des prestataires de services qui sont experts en sécurité informatique. Les entreprises, pas seulement les banques, s'entourent des prestataires de services, spécialisés dans la cybersécurité, pour travailler justement à réduire ces risques.
45. Décrit l'auditeur interne, lorsqu'il vient faire son travail ? et lors d'une mission d'audit ?
En règle générale, c'est quelqu'un sérieux qui vient et qui a bien préparer son entretien. C'est-à-dire il arrive avec un certain nombre de questions, ils viennent toujours par deux, une équipe de deux auditeurs. Mais, les relations avec les auditeurs sont bonnes en général, je crois qu'il n'y a pas de pièges.
Sur une mission d'audit, soit sur une cyber sécurité ou pas, il y a deux auditeurs qui demandent un certain nombre de questions et qui suivent un guide d'audit et qui viennent nous interviewés en nous posant un certain nombre de questions, pour écrire après les réponses, pour se faire une

idée des risques et des éventuelles recommandations à formuler. Ensuite, on se met d'accord avec les auditeurs sur les recommandations, qui nous sont affecter et après on met en œuvre les recommandations, il y a un suivi de recommandation qui est fait par les auditeurs.

46. Si vous voulez décrire le comportement de l'auditeur subjectivement le profil de l'auditeur.

Ce sont des gens avec de général connaissances des processus à faire, ce ne sont pas des spécialistes, une bonne connaissance des métiers bancaires, et ils ont des attitudes à bien communiquer, ils ont des attitudes à bien analyser, à bien identifier les risques.

47. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ?

Alors ils ne sont pas forcément peur ou intimidés, mais en règle générale, les collaborateurs ont crainte d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre, et ces recommandations à mettre en œuvre sont des moyens à engager qu'on n'a pas forcement tout le temps.

48. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ?

Il faut avoir un bon relationnel, se respecter.

49. Comment faites-vous pour établir de bonnes relations avec les autres employés ?

Pour les autres les métiers, on a mis en place des lieux d'échange trimestrielle, qu'on appelle des comités de sécurité des systèmes d'information, où on échange sur les différents sujets d'actualités, sur les différentes actions à mener. Donc, on a des lieux d'échange avec les différents métiers.

50. Quelles initiatives mettre en place pour que les dirigeants s'approprient effectivement les enjeux de la cybersécurité ?

Pour qu'ils s'approprient des enjeux, il faut qu'ils soient sensibilisés bien sûr, il faut les éclairer sur les risques, sur ce qui pourrait arriver si jamais on ne mettait pas en œuvre les politiques et les moyens pour réduire les risques de cyber sécurité. Donc, il faut éclairer les dirigeants pour qu'ils dégagent les moyens nécessaires.

51. Comment savez-vous que vos équipes sont compétentes pour une réponse à incident ?

Il y a des contrôles qui sont faits, il y a des formations qui sont réalisés. Or les contrôles sont faits par des équipes de contrôle permanent de deuxième niveau.

En France, comme je vous l'ai dit, il y a trois niveaux :

Il y a les métiers qui réalisent des contrôles de premier niveau.

Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits.

Et puis, il y a l'audit en troisième niveau, comme on disait tout à l'heure, qui effectue des missions ponctuelles, périodiques.

VI. Bref Questionnaire Socio démographique

1. Sexe Male
2. Année de naissance 1961
3. Etat-Civil Célibataire
4. Niveau de formation achevée Bac et Examen Bancaire
5. Profession RSSI

VII. En fin d'entretien

1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ? Non
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ? Assez pertinent, les questions socio démographiques sont agréables.
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective 1 heure et 31 min
6. Signature.

A2.2 Guide d'entretien avec le responsable informatique

Le Guide d'entretien avec le responsable informatique à la BPVF

I. Questions Propres

1. Qu'est-ce que vous avez faits pendant vos études ?

J'ai achevé un master Méthodes Informatiques Appliquées à la Gestion des Entreprises (MIAGE) à l'université d'Orsay à Paris. Le but de ce master était de me permettre à réaliser des projets dans les organisations et d'acquérir une bonne compréhension des systèmes d'information. Il m'a donné aussi des connaissances informatiques en analyse, conception et développement ainsi qu'une première approche des structures organisationnelles et des outils du management.

2. Pouvez-vous nous expliquer votre rôle et vos missions ?

Dans mes équipes, enfaite, Euuuuuuuuuhhh, on va gérer tout ce qui permet la production bancaire, c'est-à-dire tout ce qui est parc informatique et téléphonique donc poste de travail. On va gérer ce parc, la mise à disposition des collaborateurs, la mise à disposition après des applications bancaires nécessaires aux collaborateurs pour effectuer leurs métiers. Il faut de l'habilitation. J'ai un service habilitation enfaite qui est rattaché à mes équipes. Bien aussi tout ce qui dit application. Forcement il y a des données, des produits bancaires, des bases informations qui sont renseignées. De ce fait, j'ai sous ma responsabilité l'équipe administration informationnelle c'est-à-dire ils vont gérer, enfin garantir la qualité des donnés du système d'information pour pouvoir après mettre à disposition du contrôle de gestion des données fiables, pour le pilotage des tableaux de bord et donc de pilotage de la banque.

Ensuite, j'ai un autre pôle qui est donc plutôt orienter vers l'assistance des utilisateurs quand ils ne savent pas utiliser ou ils sont perdus sur leurs postes. Ils ont un message d'erreur, ils ne savent pas trop ou pour faire le lien entre la centrale informatique et la banque sous la déclaration des incidences par rapport soit à des fonctionnalités soit par rapport à de la technique. Puisque nous, on a dû vous l'expliquer que le groupe de banque populaire est gérer par une centrale informatique l'i-BP.

3. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?

Donc moi j'ai fait une maitrise en gestion informatique (MIAGE). J'ai commencé par travailler dans une société de service, euh, j'écrivais des programmes pour les banques voilà. Et ensuite, j'ai postulé dans une banque et en occurrence à la banque populaire et voilà c'est comment je suis arrivée. Donc, je suis arrivée dans le département informatique mais qui est dirait effectivement récent par rapport à ce que je connaissais dans la société de service puisque on dépend d'une centrale informatique. Et donc on fait quelques petits développements à la banque puisqu'il faut des petites applications privatives mais le rôle des développements on dépend de la centrale informatique.

4. D'après vous, quelles sont les qualités requises d'un responsable informatique ?

Je pense beaucoup d'écoute. Il faut aussi avoir un service client qui soit au cœur de l'activité. Cela parfaitement on fait de l'assistance, bien c'est mieux. Il faut avoir justement quelques notions des travaux des utilisateurs en langage commun. Donc ça je pense que c'est important. C'est l'une des principales qualités qui sont requises pour le poste de responsable informatique. Et puis être à l'aise aussi des outils parce que ça bouge tout le temps avec l'innovation. Là, on voit on a des collaborateurs c'est un peu compliqué, l'arrivée des tablettes, la signature électronique. Ils ont eu quand même besoin d'accompagnement.

5. Justement, quel est le degré d'interaction que vous avez avec les réseaux métier en termes de SSI ?

Donc, nous on travaille beaucoup avec le RSSI qui est Didier G.. On communiquait s'il y a des incidents ou des attaques qu'on était perçu par la centrale informatique. Il va nous sensibiliser et donc nous on va faire la communication auprès des collaborateurs. On a mis aussi en place au niveau de la banque en alterne un comité enfaite trimestrielle, un comité de sécurité du système

d'information dans lequel on a un SIRH, on a nous en informatique l'assistance production informatique, il y a donc Didier G. et il y a notre RSSI. Et on met en place, on décide au vus de l'actualité soit si on veut que ça soit assez récurent, on met en place des campagnes de sensibilisation des collaborateurs. Par rapport au mail, on reçoit en pièces jointes : attention aussi. Est-ce nous remonte les collaborateurs en agence ? Parce qu'on a eu un cas en ailière ou un collaborateur d'agence nous a remonté à l'assistance un mail qui a reçu un client et qui a priori était un mail frauduleux par rapport à des virements. Donc là, qu'est-ce qu'on fait ? Nous on reçoit on le remonte à la centrale informatique pour après eux ils investiguent et s'ils peuvent remonter la filière donc voilà. On fait à la fois aide aux collaborateurs et ensuite on est ici là en réaction je dirai par rapport à ce qui pourrai nous être remonter du groupe, du BPCE, de la centrale informatique IPB et bien notre RSSI.

II. Lien avec l'entreprise

6. Pourquoi travaillez-vous dans le secteur bancaire ?

Le secteur bancaire, pour moi est en transformations majeures qui s'opèrent dès aujourd'hui sur tous ses métiers informatiques incitant les collaborateurs à devenir acteur de leur carrière. C'est pourquoi j'ai choisi ce secteur en pleine mutation et évolution informatique et c'est cela qui me plait et qui m'a attiré.

7. Pourquoi travaillez-vous dans cette banque ?

C'est une banque avec un bon esprit d'équipe, avec un esprit humain. C'est un des domaines bancaires où l'humain est présent de façon considérable.

8. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?

Oui.

9. Selon vous, ce qui vous valorise dans votre travail, est ce que c'est votre expérience antérieure ou votre expérience après ?

Ce qui me valorise. C'est les deux. Je pense que c'est mon expérience passée en informatique et mon parcours professionnelle ainsi que ma continuité à apprendre tous les aspects nouveaux et les défis en informatique.

10. Pourquoi travaillez-vous ? Pour vivre, pour gagner de l'argent.

11. Combien de salariés ? de départements ?

Je ne sais pas le nombre exact de salariés. Peut-être c'est, je crois 7 ou 8 départements. Je ne sais pas.

III. Cyber sécurité

12. Que penser vous lors que vous entendez le terme « cyber sécurité » ?

Je pense veille attention et s'armer bien.

Je pense qu'effectivement l'organisme central c'est-à-dire le central informatique qui peut avoir des sondes et des outils pour pouvoir détecter les choses et les anomalies. Bien je pense donc que ces eux qui sont les mieux placés. Après, il faut qu'il y ait des rôles en banque justement les RSSI, c'est très important, qui sont en banque et qui ont des rôles bien spécifiés pour pouvoir centraliser et prendre connaissances des problématiques qu'on pouvait rencontrer. Donc, s'il y un RSSI au niveau des banques, je pense que c'est primordial.

13. Commenter la relation du RSSI avec les responsables informatiques si elle existe en termes de cybersécurité.

Le problème c'est moi que le seul rôle que je peux avoir parce que tout ce qui est outils informatiques et réseaux c'est piloter par la centrale informatique. J'ai aucun moyen. Mais la détection à notre niveau, elle est toujours après quoi. On ne peut rien anticiper, on ne peut rien mesurer. Donc pour moi, à mon niveau, ça va être la sensibilisation, la communication ou bien la gestion de la crise quand il y a une attaque et du coup donc j'ai vraiment besoin du RSSI et de la sécurité groupe parce que c'est eux qui vont nous alimenter en informations pour pouvoir faire le relai auprès des utilisateurs. Bien pour nous, c'est la collaboration, il y a beaucoup d'échanges aussi qu'on a mis en place ce comité trimestriel, on communique tous les deux. Bien c'est ça.

14. Peut-être vous collaborer bien avec le RSSI ayant la même qualification et compétence

informatique ?
Didier G. notre RSSI a une bonne connaissance en informatique et donc ça nous permet d'être complémentaires et même avec le responsable de sécurité informatique au niveau de la banque qui est bien même expert avec l'architecture. Donc, il dirait qu'on forme un trio qui permet de pouvoir de se comprendre de s'expliquer et du coup pouvoir communiquer et sensibiliser les utilisateurs. Et j'ai effectivement ce comité qui est trimestriel, mais ça nous n'empêche pas enfaite de communiquer au fils de l'eau. Même je dirai qu'on va jusqu'à, nous chez nous, les utilisateurs n'ont pas le droit d'installer n'importe quel logiciel à partir duquel peut être ça va faire entrer quelconque virus. Tout passe ils doivent faire une demande. Ça arrive à parc informatique et téléphonique et chez moi. Mais avant toute chose, on demande toujours l'avis du RSSI et RSI avant d'installer un nouveau logiciel tout le temps. Car s'il y a un moindre doute, ils vont demander à la centrale informatique et eux ils ont déjà les informations et voilà. C'est pour cela, je dirai qu'il y a vraiment une étroite collaboration mais je pense qu'elle est importante.
15. Les cyberattaques représentent aujourd'hui une réelle menace pour les entreprises. Comment appréhendez-vous cette menace ?
Je dirai. On sait qu'elle est là. Il y a déjà eu des cellules de crises d'organiser et parfois ces cellules de crises organisées avec la centrale informatique et le RSSI. Et puis nous, on avait dû bloquer tout ce qui était création de bénéficie pour les virements à la main des clients de la banque pour les bloquer pour que ça passe par l'agence parce qu'on savait qu'on avait une attaque à ce moment-là. Mais, je dirai le fait qu'on est même des collaborateurs du groupe qui connaissent bien.
Moi je le vis donc sereinement même si je sais qu'il faut être très vigilent. Mais je le vis sereinement dans le sens où je suis entouré de personnes compétentes et que le système, ils savent mettre les verrouilles au moment où il faut. Après, bien sûr qu'il y a des petits malins qui trouvent toujours des failles et voilà ce sont des gens qui sont très intelligents. Mais je dirai que ce n'est pas une chose qui me panique au quotidien même si je sais que ça pourra arriver mais je pense qu'on a les structures qui va bien pour essayer de réagir au plus vite.
16. Avez-vous déjà dû faire face à des attaques ? Comment avez-vous réagi ?
On en a eu effectivement au niveau du groupe. Justement, on a monté très rapidement. Il y a une cellule de crise avec la centrale informatique et le RSSI et nous à l'informatique, nous avons des points de synchro plusieurs fois par jour. Une disait ou est-ce qu'on était, une donnait les actions, c'est quand on avait vu qu'il y avait des clients qui avaient cliqué sur des liens et qui effectivement avait été attaqué. Donc, on avait une faille de route, la centrale nous avait dit qu'il faut communiquer aux clients… aux clients qui avaient cliqué sur le lien. Effectivement c'est dans la réaction, mais là il faut être présent et il faut avoir la disponibilité c'est-à-dire être forcément disponible pour ce genre de choses. Moi je l'ai.
17. Quels sont les types d'attaques les plus fréquentes ?
Si ça se trouve généralement par email où on vous demande les identifiants et je dirai en fait c'est de plus en plus difficile à détecter dans le sens qu'il y a des fautes d'orthographe, c'était mal libellé, ou même dans les signatures … Aujourd'hui parfois ils prennent les logos c'est parfois dans un parfait français. Donc c'est parfois difficile de ne pas tomber dans le piège je dirai.
18. Qu'est-ce que vous avez appris de votre dernier cyber incident ?
Ce que j'ai pu apprendre. C'est justement rester sur aine, à bien écouter les consignes et surtout à communiquer vraiment au fils de l'eau toutes les informations pour que les collaborateurs soient à la fois rassurés car ils sentent qu'il y a un monde autour pour eux qu'ils puissent aussi rassurer les clients et il y a en même temps pour pouvoir apprendre et je voudrai dire en sensibilisation, il faut qu'on s'approfondisse. Voilà, on a mis des petits vidéos dernièrement aussi en lignes sur les différentes formes d'attaques. Et sincèrement, je pense qu'il faut les passer ces campagnes-là auprès des utilisateurs et enfaite ce qu'on fait c'est qu'on les met en obligatoire dans les parcours de formation. Donc, ils sont obligés à les voir et à les regarder.
19. Pouvez-vous me parler de votre plan actuel d'intervention en cas de cyber incident ?
Alors là c'est plus en prévention. Ça c'est de la prévention de la sensibilisation.

Après en réaction de crise, c'est vraiment comme je vous le dis, on fait cellule de crise et RSSI et centrale informatique et moi donc ma principale mission c'est de faire le relai entre les utilisateurs et les clients.

20. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cybersécurité ? Que pensez-vous des formations en cybersécurité ?

Nous, on a justement pris le pas pour faire quelque chose de récurent. On a justement appris du passé. On s'améliorait là-dessus. Alors, maintenant de dire qu'on est au top, c'est certainement qu'il y a toujours des actes d'amélioration mais dès que je vois, dès qu'on voit qu'on peut les remonter au près des collaborateurs pour l'assistance. Ils nous remontent régulièrement même ils sont vigilants, ils sont sensibilisés. Donc, je pense que tout est fait.

21. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?

Oui, elle est informée. De toute façon, dès qu'il y a une cellule de crise ils sont informés.

22. Qui est responsable de maintenir la cyber sécurité dans la banque ?

Nous en tant que service informatique est très piloté par le groupe et puis par les préconisations du RSSI dans le groupe.

Donc moi je n'ai aucun lien avec toute la partie de sécurité du groupe. C'est le RSSI qu'il là. C'est lui qui est responsable de maintenir la cybersécurité en première partie.

23. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?

Nous, c'est principalement la sensibilisation des utilisateurs. Et donc mon niveau est celui de la sensibilisation des utilisateurs. Donc, je ne peux pas mettre aucune sonde et je ne peux pas lire aucun résultat de sonde. Je ne peux pas faire aucune recherche informatique. Je n'ai pas grande chose à ma disposition.

24. La surveillance efficace de la cybersécurité est-elle assurée ?

Donc pour moi, la cybersécurité est assurée par le groupe.

25. Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cyber sécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.

Moi je crois que la sensibilisation c'est le rôle de tous. Si par exemple, l'informatique va mettre à disposition les vidéos de sensibilisation auprès des utilisateurs. Le rôle des collaborateurs est de sensibiliser les clients par des formations. Donc, c'est une chaine. C'est pourquoi je crois que c'est le rôle de tous. Après, je pense que c'était une bonne chose que le groupe c'est une chose règlementaire qu'il y ait un responsable de la sécurité des systèmes d'information dans les établissements pour porter ce rôle-là et le centraliser et l'animer parce que c'est le rôle de tous et tout le monde ne peut pas l'animer. Il faut qu'il y ait un garde-fou je pense. Et pour moi, ce n'est pas le rôle de l'auditeur qu'il soit auditer pour vérifier que c'est bien effectuer, que le rôle est bien mené en banque, que la mission est bien effectuée, oui.

Donc pour moi, ce n'est pas à l'audit de porter la mission de cybersécurité.

Ils peuvent collaborer. Mais enfaite c'est plus. L'auditeur fait son travail. Quand tu audites le RSSI. Il s'assure que sa mission est bien portée. Et après un auditeur pour moi, ce n'est pas un auditeur qui doit porter la sensibilisation des collaborateurs. Ce n'est pas l'auditeur qui doit gérer les cellules de crise. Pour moi, l'auditeur est là pour contrôler que les missions sont bien accomplies.

IV. L'audit interne

1. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe en cybersécurité ?

Dans notre banque, on a un service d'audit interne. Et pour moi, comme ils auditent toutes les services. Ils auditent aussi le RSSI et toutes les fonctions de RSSI. Donc, c'est n'est pas ma partie, je ne peux pas aller contrôler ce que fait l'auditeur interne. Mais, je pense c'est en tout cas en partie le RSSI. Pour l'Audit externe ?

L'auditeur interne, c'est ce que je vous disais. Ils auditent tous les services. Nous, à l'informatique,

on a été auditer il n'y a pas longtemps. Mais, par contre, pas sur la cybercriminalité, parce ce n'est pas mon champ d'expertise. Moi je suis là dans la sensibilisation des utilisateurs en informatique.
2. Parler de votre relation de travail avec l'audit interne. Une coopération ? ou travail individuel pour chaque fonction ?
Nous travaillons avec les auditeurs lorsqu'ils mènent des audits informatiques. Nous mettons en place les recommandations identifiées par les auditeurs et suivons l'évolution de ces mises en place via un outil en complétant nos déclarations de dossiers de preuves. Nous travaillons aussi avec les auditeurs lorsqu'ils ont besoin de connaitre les habilitations informatiques des services qu'ils auditent.
3. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?
Mais justement, en étant détaché, en étant pas jugé partie, c'est comme ça que l'auditeur peut garder sa crédibilité et donner des recommandations pour l'amélioration continu.
4. Votre fonction informatique est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?
Je dirai aujourd'hui quand je vois le feu d'attaques qui va au bout, je dirai qu'on n'est pas mal. Je pense maintenant qu'il faut être toujours en veille parce que ça va tellement vite. Il ne faut pas s'arrêter à s'améliorer et que s'il y a des améliorations qui sont identifiés et peuvent être apporter. Et je crois que le groupe travail en continu ci-dessus et il le faut. C'est nécessaire.
V. Les autres acteurs
1. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?
Moi, je ne pense pas. C'est après Didier qui peut vous aider en tant que RSSI. Moi je ne sais pas.
2. Comment la fonction d'audit interne coordonne-t-elle son travail avec celui des auditeurs externes, de façon à assurer une couverture adéquate des questions à traiter en cybersécurité ?
L'auditeur interne il n'audite pas sur ce sujet. L'auditeur interne effectivement audite tous les services. Il audite tous les sièges et toutes les agences mais ce n'est pas le sujet. Et moi j'ai eu un audit il n'y a pas très longtemps, mais l'audit rapportait sur mes activités principales et je dirai la cybercriminalité n'a pas été dans ce champ d'audit. Comme elle est portée par le RSSI moi je ne suis pas audité pour cette partie-là.
3. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ?
Moi je ne ressens pas. Ils viennent avec des contraintes. Ils viennent
4. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ? avec les employés ?
Il n'y a pas de spécificité avec l'audit par rapport aux autres services de la banque. Moi je suis à l'écoute. Je fais des échanges et je partage.
VI. Bref Questionnaire Socio démographique
1. Sexe Féminin
2. Année de naissance 1971
3. Etat-Civil Mme COULON Manuelle
4. Niveau de formation achevée MIAGE
5. Profession Responsable informatique
6. Rang dans la profession Cadre
VII. En fin d'entretien
1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ?
Non, l'entretien a touché tous les aspects de mon travail.
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ?
Bon.
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective 1h 5min

6. Signature.

A2.3 Guide d'entretien avec le Chef de mission d'audit interne

Le Guide d'entretien avec le chef de mission d'audit interne à la BPVF

I. Questions Propres

1. Qu'est-ce que vous avez faits pendant vos études ?

J'ai fait une école de commerce à paris dans un institut supérieur du commerce. Ensuite, j'ai fait un DECF un diplôme de comptabilité. J'ai commencé à faire ma carrière dans l'audit comptable dans cabinet d'expertise comptable en audit externe et en suite j'ai rejoint la Banque populaire de Bourgain France compte en audit interne. Et j'ai fait une mobilité group pour venir à la Banque populaire val de France toujours en audit interne

2. Comment avez-vous trouvez ce travail ?

Chercher par internet pour la Banque populaire Bourgain France compte et après c'est une mobilité. Si ton cv est organisé en Banque populaire régional et on peut changer de région donc j'ai changé de région donc j'ai fait une mobilité.

3. Pouvez-vous nous expliquer votre rôle et vos missions ?

Mes missions sont variées, d'audit, ça peut être d'audit sur les fraudes, sur les check, sur la sécurité du système d'endogène, j'été intervenue également, et également des audit sur le réseau multi marche donc audit d'agence, voilà, j'interviens en tant que chef des mission et du coup on doit élaborer un programme de travail pour identifier des risques préalable à mettre en place du contrôle pour valider le programme du travail des test voilà et mettre en rapport avec des recommandation sur les point risques qu'on a identifié mais des coûts intérieurs sur des missions travaillées.

4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?

J'ai fait une école de commerce de comptabilité sur l'entre an audit externe, c'est dans les cabinets d'expertise comptable donc j'ai fait l'audit et je vais voir les entreprises, mais j'été externe du l'entreprise et du coup j'ai voulez faire de l'audit interne un audit à l'intérieur de l'entreprise, mais c'été la suite logique de l'audit externe

5. D'après vous, quelles sont les qualités requises d'un chef de mission ?

La rigueur, organisation, parce que il fait qualifié.

Empathie parce que il faut être d'ambiance comme même avec les auditée.

Capacité d'analyser des synthèses parce qu'il faut synthétiser tous les travaux qui sont fait par les auditeurs donc il faut avoir une capacité pour synthétiser tous les problématiques relevés.

Prise de hauteur pour arriver avoir prendre de la hauteur, prendre du reçus en fait on n'étudie point de taille mais avec ces points de taille il faut arrive à prendre de la hauteur pour synthétiser en fait pour voir les problèmes.

L'auditeur de plus y détail tous c'est travaux, etc.

Le chef des missions il faut prendre de hauteur pour synthétiser les problématiques relevées par l'auditeur.

6. Justement, quel est le degré d'interaction que vous avez avec les réseaux métier en termes de SSI ?

Nous on n'intervient pas sur la sécurité de système d'information ce que je peux vous dire c'est qu'on a eu mission l'année dernier mais comme on est des auditeurs généralistes on a dû faire appel à des cabinets externes donc nous avons travaillé avec des cabinets externes qui ont auditée le système d'information de nos banques. Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT en fait on est des auditeurs généralistes de banque mais pas des auditeurs spécialisés des systèmes information il ya des cabinets. L'a c'est le cabinet « ITEKIA » spécialisé en système d'information qui est venu chez nous, travailler en relation avec nous. Mais nous on faisait plus des relations avec les auditée on fait un peu la bottelette mais c'est

eux qui faisait l'investigation.

7. Pourquoi vous aller recourir à un service extérieur ? pourquoi maintenant ?

En interne chez nous on n'a pas d'auditeur spécialisé en sécurité du système d'information on n'a pas d'auditeur qui sont spécialisé en informatique et pour voir si le système d'informatique est bien verrouillé il faut une certaine compétence d'informatique on a pas en interne donc on a fait appeler à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission.

II. Lien avec l'entreprise

8. Pourquoi travaillez-vous dans le secteur bancaire ?

On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était une diversité de métier intéressant et une diversité d'opportunité également de carrière on peut travailler dans le commercial, dans développement, dans l'inter donc une diversité de métier qui est proposé c'est ce qui m'a attiré dans le secteur bancaire.

9. Pourquoi travaillez-vous dans banque populaire val de France ?

Là c'est un choix familial en fait de rejoindre ma famille qui est cité dans une région dans l'appartement des avelines donc la Banque populaire parce que c'est une Banque mutualise qui value l'humain comme un demi collaborateur ce n'est pas une immense machine c'est une Banque qui value l'humain voilà pour la valeur, pour l'être humain et pour le rapprochement géographique familial.

10. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?

Oui je pense après j'aurai la barrière de l'anglais on a beaucoup des banques nationales qui demande qu'on soi bi-langues et qu'on écrit et on parle l'anglais donc je pense que ça va commencer à se constituer en France. Si non, je pense qu'on est capable de travailler dans n'importe quelle banque. À mon avis c'est le même mais il y a changement de système d'information mais si non c'est le même technique d'audit. Donc je pense oui je peux travailler dans un autre établissement. Sauf la problématique de l'anglais.

11. Selon vous, ce qui vous valorise dans votre travail, est ce que c'est votre expérience antérieure ou votre expérience après ?

Moi c'est plutôt actuellement le fait de présenter nos travons à des directions et de les faire réfléchir sur des améliorations sur le contrôle interne donc c'est pouvoir proposer des rapports avec des recommandations avec la valeur ajoutée pour la banque, c'est ce qui me valorise en gros.

12. Pourquoi travaillez-vous ?

Alors, ça c'est une bonne question, pour gainer ma vie, pour avoir un salaire à la fin du mois et également pour m'épanouir parce que je pense que le travail ça permis l'accompli de ma personnalité et puis également une problématique matérielle pours gainer sa vie.

13. Combien de salariés ? de départements ?

Dans la Banque populaire val de France le salarié total c'est 2200.

Il y a le réseau commercial, la direction des risques, je ne sais pas exactement mais 6 ou 7 départements j'imagine des départements fractionnels ou des départements commerciaux. sIl y a le développement, finance, il y a le réseau multi marché donc tout ce qui est les agences, tous les fonctions risque et contrôle, audit etc. qui sont attaché directement à la direction générale il y a tous ce qui est les gestions privée et entreprise, les marchées de l'entreprise donc 5 ou 6 départements.

III. Cyber sécurité

14. Que penser vous lors que vous entendez le terme « cyber sécurité » ?

Protection, contre des attaques externes sur le système d'information protection des données également parce qu'on a les données des clients qui sont confidentielles il faut qu'elles soient protégées et également protection contre les attaques malveillantes et l'espionnage voilà ce genre des choses c'est vraiment la protection du système d'information pour éviter qu'il y a des intrusions.

15. Vous m'avais dit avant que l'année passée on faisait un audit sur le système d'informatique

pouvez-vous commenter cette mission en terme de cyber sécurité ? commentez cette mission en général, que ce qui c'est passer ?
Je ne sais pas le rapport sur les yeux ce que je sais que aves contrôle les habilitations, vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, il avait regardé tous les dispositifs de contre de tests, d'intrusion pour voir si notre banque réalise bien des tests d'intrusion. Ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y a un système qui est développer par I-BP et cela qu'on avait tendance à passer comme c'est I-BP qui protège tous or il y a des applications développées chez nous en interne donc ils ont recensé cette application privative dans tous les services et ils ont fait des tests pour voir s'ils étaient bien verrouillés. Ils ont même réalisé des tests d'intrusion. Ils ont réalisé eu même des tests d'intrusion donc vous imaginer pour faire ça il faut comme même certaine compétence informatique ce qui explique que nous ne prouver pas le faire.
16. C'est pourquoi vous aller recourir à un service externe qui est spécialisé en sécurité d'information ?
Justement, pour par exemple ces types de deux choses : ils ont comme ça put faire des tests d'intrusion pour voir s'ils ont été bien verrouillé parce que nous on n'a pas pu faire en interne.
17. Vous avez fait c'est-à-dire l'audit interne ici a un rôle de vérifier les procédures et les protocoles des tests mais la vérification des tests, comment ils vont faire ? c'est par un service externe !
Sur cette mission-là, la directrice de l'audit, l'ancienne directrice de l'audit qui est partie maintenant elle avait choisi qu'on fait appel à un cabinet extérieur parce qu'elle considère qu'on avait pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives et je pense qu'elle avait raison parce qu'on n'avait pas tous les compétences requise pour par exemple faire des tests d'intrusion.
Donc nous sur les audits banquer on se débrouille c'est à dire on a des compétences en interne pour faire nos audits surtout sur le domaine bancaire protection clientèle, les contrats crédits, tous se sont risqué bancaire on a les compétences en interne, au niveau de la sécurité de système d'information qui est nouveau comme même un problématique intéressant on n'a pas d'auditeur spécialisé en ce système d'information. C'est pour cela on a fait appeler à ce cabinet.
18. Avant dans l'entretien précédent, on m'a dit que vous avez embauché une nouvelle personne dans un nouveau post. Mais elle a oublié le poste. C'est en termes de sécurité. Vous avez une idée qui est ce poste ?
Mais pas dans notre service d'audit interne, Je ne sais pas son poste mais ça peut être RSSI responsable sécurité du système d'information.
Tu c'est son nom ? Non
Car il y a G. en RSSI
Oui effectivement il y a une deuxième personne et ça été une suite à notre mission qu'on a fait l'année dernière. Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. En fait c'est le résultat de l'audit qui a dit attention un demi collaborateur et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'il ont relevé c'est que justement le RSSI n'est pas suffisamment pro actif, ça serait près des services que tout est bien fait quand tu avais un développement d'implication privative parce que quand tu développes une implication privative il fait prendre en compte la sécurité de système d'information et ça le cabinet externe a trouvé que justement on ne prenais pas suffisamment compte la sécurité du système d'information pour développer des application privatives.
C'est pourquoi la solution a été d'embaucher un autre RSSI pour couvrir à temps complet ?
C'est ça exactement mais je ne connais pas le nom de l'employée.
19. Qui est responsable de maintenir la cybersécurité dans la banque ?
C'est le RSSI justement, et tous les services également en fait. Tous ce qui développe des applications privatives doit prendre en compte cette impérative de sécurité quand il développe des

applications privatives et faire une coordination avec le RSSI justement.
20. Certains disent que c'est le rôle de tous les employés. Commenter.
Oui alors, oui mais en particulier quand même oui mais ils ne sont pas tôt parce que nous également on doit faire attention à bien verrouiller nos ordinateurs à pas donner des informations confidentielles etc. d'une certaine manière ils ont raisons mais il y a également tous ce qui développe des applications privatives doit venir compte et ça n'est pas fait jusqu'à présent et le RSSI doit être impliqué dans tous les développements d'application privative dans la banque.
21. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? sont-elles été suivies ?
On n'a pas eu temps de ça, en fait pour vous dire après la mission qu'on a fait avec le cabinet « ITEKIA ». Ils ont fait une formation avec les autres banques populaires pour justement réaliser la même mission que nous mais dans les autres banques en fait on était un peu la banque pilote. On a fait mission avec ce cabinet externe et après ça ils ont fait une formation pour les autres auditeurs internes des autres banques suit à ça. Une formation pour la cybersécurité.
22. Après le résultat que vous avez fait d'embaucher un nouveau RSSI. Quelle autre action corrective a été prise ? ou seulement cette action ?
Il y en a d'autre mais je n'ai pas le rapport sous la main.
23. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?
Oui, oui, ouii c'est même le directeur général qu'à demander.
24. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?
Réaliser des missions là-dessus puis comme je vous les a dit tout à l'heure dans la vie tous les jours comme je vous l'ai dit tout est concerner donc il faut voilà être vigilant sur nos codes, ne pas laisser trainer le mot de passe puis si non dans nos cadres de missions, les missions d'audit comme même nature comme on a fait l'année dernière même si c'est avec un cabinet on a intervenu pour rédiger le rapport etc.
25. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cyber sécurité ?
Oui je pense oui
26. La surveillance efficace de la cybersécurité est-elle assurée ?
Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en terme de dispositif du contrôle de recrutement de RSSI. C'est en cours d'amélioration. Et l'année prochaine on a fait des missions d'audit groupe donc qui vont être pilotée par des DTCE des missions justement de l'informatique locale donc on va continuer à investiguer et faire des missions sur cette thématique pour renforcer parce que c'est nouveau en fait la problématique de RSSI ce n'est pas tellement pris en compte jusqu'à présent mais il faut aller de plus en plus.
27. Certaines disent de confier à l'audit interne le rôle de maintenir la cybersécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cybersécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
Non moi je n'ai pas tout à fait d'accord. Nous on n'est en 3ième niveau. Nous on vient vérifier que c'est bien fait mais nous on intervient en 3ième rideau donc pour moi ce n'est pas nous de maintenir tous seul la cybersécurité c'est avec la direction des risques, c'est avec les autres services avec les services qui développent des applications, des services informatiques mais il y a pas que l'audit nous on vient en derrière c'est ce que je puisse dire donc on n'est pas, ce n'est pas que à nous de les faire.
IV. L'audit interne
1. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?
Ça ne serait pas suffisant d'avoir que des auditeurs externes presque nous on est en plein temps dans la banque pour auditer en permanence il y a tellement des trucs pour auditer, un audit externe

il faudra qu'il soit là tout le temps ça serait pas possible pour moi c'est obligatoire d'avoir un audit interne.

2. Parler de votre relation avec l'auditeur hors du travail en décrivant le comportement de l'auditeur interne dans votre travail.

Il doit avoir un principe d'indépendance c'est-à-dire nous on est là pour vérifier donc on doit être indépendant des personnes comme audit parce qu'on doit surveiller si les normes sont bien appliqués donc il ne faut pas de collision entre guillemet il faut qu'on soient disponible, professionnelle, à l'écoute il faut qu'on vaille pas trop parce qu'on vient déranger les gens dans le travail donc il faut prendre en compte les impératives des autres employées donc il y a tout un aspe de professionnalisme mais à la fois d'empathie et d'indépendance c'est tout ça pour moi l'auditeur.

3. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?

La justement il faut que l'auditeur adopte le comportement d'indépendance pour moi c'est comme ça qu'on peut, il faut qu'on n'entre pas en conflit interne. Exemple : il ne faut pas avoir un poste d'envie quand on va auditer une direction parce qu'on ne va pas être indépendant par rapport à ce qu'on va dire, on va être trop gentille pour avoir le poste.

4. Votre fonction …Est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?

Oui nous il nous manque les compétences internes parce que pour moi il faut des auditeurs spécialisés en système d'information. Un auditeur généraliste aura du mal à évaluer la force, qualité de contrôle interne d'informatique s'il ne connait rien dans l'informatique donc il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT.

5. Si comme vous le dite des auditeurs IT sont dans la banque embauché, vous n'auriez plus besoin de demander à des services extérieurs de venir auditer ? ils vont jouer le rôle que joue le service extérieur.

Oui c'est ça, après il faut avoir des moyennes et puis il faut avoir l'envie de suffisamment une mission à mener là-dessus vous savez c'est toujours l'histoire entre le besoin et le coût etc.

V. Les autres acteurs

1. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cybersécurité ?

Je pense que ça peut être de refaire ce qu'on a fait l'année dernier c'est-à-dire de recourir un cabinet externe.

2. Pourquoi ne pas donner une recommandation ? comme vous avez donnez d'embaucher le RSSI ? d'embaucher des auditeurs spécialisés en informatique ?

Le besoin n'est pas, disons qu'on a eu une mission peut-être dans l'année chaque année on va avoir une mission amener sur le système d'information je pense que ce n'est pas suffisant pour nécessiter.

Aujourd'hui en tous cas, ça ne semble pas suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission

3. Après tous les entretiens que j'ai réalisés, mes recherches, le problème de cyber sécurité est en croissance c'est un problème urgent dans tous les organisations il faut qu'il y a des mesures, prendre des décisions car la cybersécurité c'est un problème en croissance.

Je comprends il est en croissance mais le nécessaire chez nous est d'avoir un auditeur en temps plein. C'est pour l'instant. Mais je suis d'Accord avec vous c'est ce que la banque est entrainé de faire de renforcer ses systèmes parce que il n'y a pas que des niveaux humains également les contre à la place il faut que tous les services soient impliqués. Les services informatiques aussi donc voilà on peut déjà renforcer ce qu'on a fait et ensuite voir ce qu'il faut recruter d'autres mais déjà si en interne on arrive à des failles il faut les résoudre déjà avec les gens qu'on a remplacé il n'a pas qu'avec les recrutements externes pour réguler les problèmes.

4. Les budgets qui sont mis en terme de cybersécurité dans tout le monde, j'ai des statistiques qui montre que tous les entreprises ils payent, ils augmentent leur budget en terme de

cybersécurité, dans votre banque est ce que l'audit interne joue un rôle de réducteur du coup c'est à dire dans ses budgets ou il n'a pas un rôle ?
Là justement On a demandé, il y a le rapport qu'on a fait l'année dernier avec les cabinets externes qu'il y a recrutement plus au niveau de RSSI donc on est plutôt dans le sens il faut qu'on renforce, les moyens des sécurités à situer ont été plutôt dans l'aspect-là mais pas dans l'aspect des coûts.
5. Comment tenir la direction responsable de la prise en considération des constations d'audit et de la mise en œuvre des mesures correctives ?
Là c'est la direction des risques, elle est en charge de prendre compte de la recommandation sur le fait d'augmenter, les rejoint des moyennes allouer à la sécurité des systèmes d'info. Donc c'est ce qui affecte la direction des risques. C'est à eux de mettre en œuvre les mesures, le plan d'action avec une date de séance donc ils n'ont pas de liberté de prendre en compte la recommandation.
6. Comment la fonction d'audit interne coordonne-t-elle son travail avec celui des auditeurs externes, de façon à assurer une couverture adéquate des questions à traiter, Quelle que soit son approche à l'égard de la dotation en personnel ? Aussi relation avec les responsables de TI ?
On avait un programme de travail qui a été établie avec l'inspection générale de BPCE et programme de travail a été mené par le cabinet extérieur mais il passe par nous pour tout ce qui a été documenter à demander au collègue interne et on les a renvoyés les documents sur un message ré-sécurisé crypté. Nous on coordonne comme ça.
7. Décrit l'auditeur interne, lorsqu'il vient faire son travail ?
Il doit organiser sa journée, planifier ses rendez-vous, mener des entretient, réaliser des tests pour vérifier tous ce qu'on lui a dit est correcte, synthétiser tous ce qu'on a dit pour rédiger un rapport.
8. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ?
Oui, il pense que l'audit est un rôle de gendarme mais on n'est pas là que pour ça. C'est-à-dire quand on fait partie de l'entreprise puis quand on veut faire avancer une entreprise en proposant des actes d'amélioration mais pas que des gendarmes mais ça dépend des audités. Il y a des audités qui ont compris qu'on est là pour valeur ajoutée et autre qui nous voient uniquement comme des gendarmes et qui ont peur. Et ça c'est un travail de pédagogie à faire quand on fait la mission. C'est pour expliquer qu'on est là pour travailler avec eux mais pas de faire des gendarmes.
9. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ? avec les employés ?
Il faut communiquer, pédagogie puis voilà professionnelle
10. Bref Questionnaire Socio démographique
1. Sexe male
2. Année de naissance1982
3. Etat-Civil
4. Niveau de formation achevée plus 5
5. Profession audit interne
6. En fin d'entretien Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ?
Non, je vous envois quelques points d'amélioration qu'on a relevé suite à notre mission l'année dernière, je vous liste quelques points donc les pistes d'amélioration qu'on a envisagée suite à notre auditée. Je pense que ça vous intéresse.
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ?
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective 48 minutes 26 second
6. Signature.
Pour comprendre une chose dans la hiérarchie du groupe dans la banque.
Vous êtes un chef de mission et dans votre équipe il y a un superviseur et sous eux, il y a des auditeurs réguliers

Oui en fait y il a mais ça dépend.

A2.4 Guide d'entretien avec le superviseur d'audit interne

Le Guide d'entretien avec le superviseur d'audit interne à la BPVF

I. Questions Propres

1. Qu'est-ce que vous avez faits pendant vos études ?

Moi, j'ai fait des études, j'ai passé comptable, donc j'ai une formation comptable, je suis expertise comptable en fait. Avant d'être expertise comptable, j'ai réalisé un Bac+4 en comptabilité.

2. Comment avez-vous trouvez ce travail ?

Le travail actuel ? Je suis sortie de mes études, j'ai fait une mission d'intérim où je suis arrivé par hasard au milieu bancaire, ce n'étais pas un choix de ma part, donc j'ai tombe dans une première banque mais pas la banque populaire. Quand même pour vous préciser, j'ai 49 ans, ça fait 26 ans je travaille dans les banques. C'est plusieurs banques dans mon passée, et donc la première banque je suis arrivée par hasard. Et, donc, je suis arrivé dans une première banque qui s'appelait Fortis Banque, que vous ne connaissez peut-être pas, je suis resté une dizaine d'année, je suis arrivé dans le groupe BPCE en 2001, et après, à force de contacte et de réseau, j'ai commencé par un contrat BPCE S1, et je suis arrivé actuellement dans la BPVF, je suis arrivé, sans dire de bêtise, attendez, en 2003. Excusez-moi, en mai 2009.

3. Pouvez-vous nous expliquer votre rôle et vos missions ?

Actuellement, je travaille à l'audit. Je suis superviseur à l'audit. Donc, vous avez eu faire ça avant avec mon directeur d'audit Monsieur « Manuel Couillet ». Et donc, mon rôle en tant que superviseur, c'est de coordonner les équipes, donc, d'animer les missions d'audits que nous réalisons, de coordonner les équipes, de les animer, de les amener au niveau attendu. C'est-à-dire, à l'audit, nous avons une méthodologie qui est très évidente, et des profondes d'habilitations qui sont déjà définis à l'avance, et qui nous demande, nous avons un minimum de cas inspecté. Donc, mon rôle c'est d'animer cette équipe pour que les travaux soient accomplis avec la qualité attendue en quantité et en qualité je voudrai dire. En fait, sur l'assurance que les missions sont bien prémunis dans la banque dans leur contenu et réaliser dans les délais qui nous sont donné. Parce que nous avons à faire l'audit en 4 ans à réaliser et il faut que toutes les missions soient renouvelées. C'est pour dire que cette mission qui était prévus en début d'année nous ne la faisons pas. Et donc, mon rôle est de saturer que tout est fait en temps parfait.

4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?

Alors j'ai bien commencé comme je vous l'ai dit en milieu comptable. Donc, j'ai fait 25 ans tous les métiers comptables, possible imaginable au sein de la finance, et je suis arrivé à la banque populaire Val de France en tant que responsable de la révision comptable, et au bout de 5 an, j'ai évolué vers un poste de superviseur par hasard, on va dire c'est pareil, j'ai vu l'annonce proposé, et je me suis dit naturellement ce sont des métiers de contrôle, thématique indifférente, mais ce sont des métiers un peu près similaire, donc je me suis dit c'est le moment de changer, et puis élargir sa vision dans le sens de sortir de la comptabilité pour savoir tous les aspects de la banque. Puisque dans l'audit, nos audits ils n'ont pas la comptabilité, mais nous auditons de toute façon toutes les services de la banque. Je suis arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé.

5. D'après vous, quelles sont les qualités requises d'un superviseur d'audit?

Rigueur, agilité, beaucoup d'ouverture d'esprit. Si on a un problème, on trouve une solution rapidement. Et jamais ne se perdre non plus, il faut toujours garder l'esprit qu'on est là pour préserver les intérêts de la banque puisque nous nous sommes amenées à mettre à jour les risques et de découvrir les risques, et de détecter les risques pour le directeur général qui est notre principal client. Il faut arriver à conserver l'esprit d'équipe parce qu'on est une équipe de plusieurs auditeurs. Et il faut arriver à satisfaire tout le monde.

Il faut arriver à préserver les intérêts des auditeurs, et préserver les services que nous auditons.

C’est un rôle un peu diplomate entre guillemets. En France, il faut arriver à contenter les intérêts de tout le monde.

6. Justement, quel est le degré d’interaction que vous avez avec les réseaux métier en termes de SSI ?

En termes de SSI, ce n’est pas notre confort, c’est vraiment un métier très spécifique, ce sont des expertises que nous n’avons pas forcement, donc, il y a rien à réaliser des missions sur les SSI. Nous avons fait appel à un cabinet extérieur pour connaitre ses limites. Nous, nous sommes des gens qui sont généralistes et la plupart des temps, on est curieux, on a des méthodes pour apprendre des sujets qu’on ne connaît pas, les SSI par exemple, c’est un vrai métier. Par contre, moi, j’ai une sensibilité sur tout ce qui est environnement informatique. Donc, c’est en cas d’application que moi je n’ai pas mal de connaissances, sur toutes les applications, des différents métiers de la banque, j’ai quand même cette sensibilité contre les sujets qui ne sont pas connus. Je connais seulement l’importance de ces sujets, et je rappelle régulièrement tout le monde. Et après, je suis moins expert en ce métier. Je sais vous avez interviewé Didier G., ils ont embauché un expert là-dessus. En tout cas, ce sont des problématiques que nous avons en tête, dont nous connaissons l’importance.

II. Lien avec l’entreprise

7. Pourquoi travaillez-vous dans le secteur bancaire ?

Par hasard au départ, c’est le hasard, l’opportunité. Et, je vais dire que maintenant j’y reste parce que je trouve que c’est un milieu en mouvement, c’est un milieu qui évolue, qui va changer, donc il y a plein de métiers intéressants qui n’existent pas forcement encore, ça laisse beaucoup d’opportunités de carrière. C’est un milieu que j’aime bien, je ne vois pas changer de milieu de travail. Je resterai dans la banque le plus long possible.

8. Pourquoi travaillez-vous dans cette banque ?

Banque populaire Val de France. Moi, je suis attaché au milieu mutualiste. Donc, c’est une banque qui me plait. Ce sont les valeurs mutualistes qui me plaisent, et donc, je me n’en verrai pas allez dans une autre banque, société générale ou … C’est à cause du côté mutualiste que je suis là, je reste attachée à la banque, je suis fidèle. Donc, je suis une collaboratrice fidèle aux valeurs de la banque, et à la banque elle-même, je suis fidèle à mon employeur. Donc, je ne me vois pas allez ailleurs dans une autre banque.

9. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?

Oui, une banque, c’est-à-dire un client. Toutes les banques ont des clients. On a le même régulateur au-dessus qui gèrent les banques auxquels nous devront rendez compte. Oui, ce que soit cette banque ou une autre, ce n’est pas par parce j’aime les valeurs mutualistes dans une banque que je ne vais pas allez dans une autre banque. Ça sera juste un choix de ma part de rester dans cette banque. Ce qui pourra par ailleurs me bloquer, c’est que je ne pars pas assez couramment et qui pourrai me bloquer des perspectives en d’autres comptes qui seraient relation avec les banques. Mais, sinon, le métier est le même d’une banque à l’autre.

10. Selon vous, ce qui vous valorise dans votre travail, est ce que c’est votre expérience antérieure ou votre expérience après ?

Les deux. C’est l’ensemble des choses. On va dire le passée c’est plutôt la rigueur, c’est dans ce cas où je me dis que mon passée me sert beaucoup. Par contre il faut savoir inventer tous les jours, c’est plutôt le présent qui fait que je me contrôle moi-même chaque jour au quotidien. Donc, il faut être curieux. A l’audit, nous avons la chance de découvrir plein de sujets que nous ne sommes pas experts en au départ. Ça nous donne l’occasion d’appréhender de nouveaux sujets.

11. Pourquoi travaillez-vous ?

Ahhhhh ! C’est une bonne question. Pourquoi je travaille ! Parce que j’aime bien travailler déjà, et j’aime bien découvrir de nouveaux choses, de nouveau challenges, apprendre à assez évoluer avec mon environnement. Et, c’est déjà aussi avoir des relations humaines tous les jours. Moi, j’ai une équipe à gérer. C’est-à-dire avoir des relations avec mon équipe, avec les équipes extérieures auxquelles nous avons audités.

C’est recouru à l’argumentation, ça nous mettent en contact avec le monde extérieur.
Moi je suis active, et j’aime mon travail et je veux continuer à travailler, à progresser.
12. Combien de salariés ? de départements ?
Oui, oui, on a plus de 2000 salariés. 2050 l’année dernière, oui. Je ne sais pas combien il y a de services exactement, je peux vous dire qu’il y a un peu plus que 200 agences, mais au nombre de services, je ne peux pas vous dire exactement combien, mais je connais assez bien l’environnement de notre banque, en tout cas, ça nous fait exactement beaucoup de contacts avec énormément de mondes. Ce qui importe c’est un sous-jacent qu’on connait bien la banque. Nous sommes pas dans une tour d’histoire, on est en contact avec tout le monde, on est énormément de relation qui ne se passe pas forcement dans toutes les banques. Dans ce cas, l’audit chez nous est en relation, on très bien enserré dans le dispositif de la banque. Nous sommes au contacte, moi je communique énormément avec tout le monde, je normalement de relations avec tout le monde, j’écoute les problématiques des uns les autres, ce qui peut nous aider aussi dans notre métier.
III. Cyber sécurité
13. Que penser vous lors que vous entendez le terme « cyber sécurité » ?
C’est le danger numéro 1 on va dire. Pour moi, c’est le danger numéro 1 dans les entreprises actuellement. Et puis, c’est un risque qui s’est largement sous-estimé parce que ça coûte cher. Et que déjà, c’est un nouveau risque, et ça va mettre du temps à appréhender, et pour moi c’est un danger, un vrai danger, un danger qui doit être une préoccupation pour toutes les entreprises au-delà les banques.
14. Commenter une mission de cyber sécurité.
Non, je n’ai pas les compétences. C’est par contre en employant un cabinet, je pourrai faire des liens entre un cabinet, et lui apporté le lien entre les connaissances métier et les problématiques de cyber sécurité. Mais, en tout cas, moi je n’ai pas les compétences à mon niveau.
15. Quelles difficultés y rencontre-t-on ?
Au sein de la banque, j’ai l’effet d’avoir des gens qui ont des connaissances et des préoccupations en informatique mais je dirai au sens large. Et de mettre à jour le problème, ça veut dire qu’à l’instant, c’est un sujet, jusqu’à un an, qu’on ne se préoccupait pas du tout au sein de la banque. Maintenant, depuis un an, les choses ont changé, ils ont embauché quelqu’un qui devra arriver. Cette problématique qui affecte ce sujet est qu’il coûte cher. Je pense qu’ils vont être amenés de plus en plus à contrecarrer, on va subir des attaques comme beaucoup d’établissements a d’autre. Pour moi, c’est un nouveau sujet. C’est un nouveau sujet pour nous, il faut savoir à mettre en compétences. Il y a très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n’avons pas pour l’instant chez nous. Ce qui sensibilise l’informatique, ce sont des profils très rares. Et dans les banques, ce ne sont pas les profils majoritaires pour l’instant. Il y a très peu de gens qui connaissent ce sujet.
16. Qui est cette personne qui est embauché ? Son Poste ?
Je ne sais pas. J’ai juste entendu qu’on allait renforcer le sujet. Voilà, après son poste, je ne pourrai pas vous le dire. La nouvelle personne va arriver chez Didier G. pour collaborer avec lui. Car ce qui manquait Didier G. en expertise technique, la clairement c’est pour renforcer ce sujet-là. C’est un côté positive qu’on a clairement conscience qu’on a besoin d’une autre personne. On ne peut pas être généraliste sur un sujet pareil.
17. Qui est responsable de maintenir la cyber sécurité dans la banque ?
Il faut qu’il y ait l’expert. Mais, c’est l’affaire de tous, il faut que ce soit une préoccupation de tous. Il faut changer la mentalité, il faut éviter les comportements à risque. Pour moi, c’est une préoccupation de tous, parce qu’on peut tous se faire attaquer si on prend des risques. On peut prendre des risques, et on peut laisser les portes ouvertes, pour s’attaquer. Clairement, mais pour ça il faut animer le sujet, il faut que les gens prennent conscience que c’est un danger. Et le danger peut venir de partout. On est 2000 collaborateurs au sein de la banque, c’est facile d’y trouver une faille pour entrer dans la banque. Voilà, pour moi, c’est l’affaire de tous. Il faut du travail.
18. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? sont-elles été

suivies ?
Oui, on a des formations, ce n'est pas en cyber sécurité exactement, c'est plus. On sait que ça existe, on dit qu'il y a des risques, on a des animations, ce n'est pas au sens propre. Ce ne sont pas des formations en cyber sécurité à mon sens. Voilà, ça commence à monter que c'est un sujet qui porte des risques. On part de loin. On commence à faire prendre conscience aux gens que c'est un sujet qui a des risques informatiques, qu'il faut faire attention à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. Pour moi, c'est bien ce qu'on fait. Et que tout le monde soit expert sur le sujet. On a la formation, on a forme, puisqu'on nous forme sur le sujet. C'est de la formation, une prise de connaissances, on fait progresser les gens sur ce sujet. La cyber sécurité, c'est un vaste sujet, que personne, à l'instant, il y a peu de gens qui savent ce qui montre ce sujet.
19. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?
Ahhhhh ! Oui. Oui. Ça c'est une vraie préoccupation maintenant. Ils ont pris conscience. Au niveau de la direction générale, il y a aucun sujet. Moi, je crois qu'ils ont pris conscience du danger. Après entre prendre conscience et trouver les bons moyens, trouver vite les moyens, ça va être plus compliqué de mettre en œuvre les moyens. Ça coûte cher et ça prend du temps. Mais, nous prenons conscience, ça fait sûre.
20. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?
Dans nos audits, au quotidien, je veux dire en termes d'application interne, parce que le développement nous avons beaucoup d'assez questions informatiques. Ils sont développés par notre prestataire informatique, et donc I-BP. Et nous avons aussi beaucoup d'application informatique privative. C'est comme ça. Ces applications là nous donnent nos audits que nous allons auditer un procès ou un service, nous faisons la revue de toutes les applications. Donc, quelque part, si on voit des failles en termes d'habilitation ou d'application qui sera un peu à la dérive ou isolé dans son coin. Nous avons moyen d'attirer l'attention sur ces applications-là. Il faut dire attention. Il faut appeler un expert sur le sujet pour savoir s'il y a une faille ou pas. En tout cas, une faille la répertorier rendent en procès quelle type d'application. On peut avoir notre rôle à jouer en termes de détection d'application un peu orpheline dans certains services.
21. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cybersécurité?
Oui. Pour moi, oui. De toute façon, nous embauchons dans le monde de banque, il y a beaucoup de jeunes qui sont embauché, beaucoup de personnes qui partent en retraite. Et de toute façon, il y a beaucoup de jeunes qui arrivent chaque année. Pour tous ces nouveaux, il faut bien les former. Et même, pour les anciens, il ne faut pas relâcher là caution. Je pense qu'il faut y avoir… C'est de tous les moments, il faut rappeler que c'est important, d'appréhender le risque. Si on ne rappelle pas régulièrement, les hackers sont de plus en plus imaginatifs, pour faire du phishing et c'est la première faille. Pour moi, les hackers sont toujours en avance de tout le monde. Donc, il ne faut pas sous-estimer leurs forces. Il faut y avoir une prise de conscience de ça. Et plus on les informe rapidement, voilà, pour moi, il faut communiquer et être former.
22. Pouvez-vous m'expliquer le travail que vous faites avec les opérateurs informatiques ? Quelle est la relation en matière de cyber sécurité ? c'est-à-dire comment vous travailler ensemble ?
Le seul fait était lorsqu'on fait la mission l'année dernière. On a envisagé un expert métier, un cabinet spécialisé. Donc, on les a assistés, on a participé avec eux dans leurs missions. Après notre rôle était de coordonner, de sert en sorte d'interlocuteurs, pour faciliter leurs missions. Après, en termes d'expertises, on n'a pas l'expertise, on les a laissés à leurs métiers et on a fait en sorte que les gens se comprennent. La cyber sécurité, c'est un métier, une façon de se parler, de s'exprimer. Mais l'informatique, nous avons essayé de mettre en correspondance les demandes des un avec les réponses des autres, et de faire en sorte, que tout le monde se comprenne.
23. Pouvez-vous m'expliquer pourquoi ils ont recours à ce service extérieur ? Quelle est la

raison ? Comment s'effectue la démarche ?
La démarche, c'est que nous avons un plan d'audit, sur 4 ans, ça fait partie des risques qu'on n'avait pas encore audité. Et on sentait que c'était un risque majeur pour les banques. Et donc, on a amené ce cabinet. Je pense, je ne peux pas vous dire, je n'ai pas participé au choix du cabinet, ma direction je pense qu'ils ont dû avoir un choix de plusieurs personnes, de plusieurs cabinets. Et voilà, donc, s'il demande de la banque, et aussi par rapport au groupe, c'est-à-dire que ce cabinet-là, nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP. Les prestataires informatiques, on sentait qu'on avait besoin, on les a fait venir. Ils ont travaillé. Et le but était que les failles qui étaient identifiées puissent être corrigées. Et pour le compte de la communauté de la banque populaire, c'est-à-dire nous avons mis à jour des constats. I-BP les a corrigés mais ne les a pas corrigés que dans notre établissement. Il ne les a corrigés pour les autres banques populaires, c'est aussi la démarche. Voilà, on a fait participer un cabinet au bénéfice du groupe. Et c'était à notre demande en tout cas.
24. Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cyber sécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
Non, pour moi non. Parce que l'audit n'a pas de compétence métier. On n'est pas expert. Je disais tout à l'heure que les auditeurs sont généralistes et on n'a pas de compétence, il faut vraiment… La cyber sécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue. Comme je vous le dit pour moi, les hackers entre guillemets, sont très inventifs, très rapides, très compétents. C'est un métier qu'on ne peut pas suivre. Il faut quelqu'un qui soit dédié à ça. Nous, on en peut pas suivre, on n'a pas les compétences en tout cas. Par contre, on peut participer au processus d'alerte et de maintien. Pour moi, le risque de cyber sécurité, c'est un risque qui est important. Par contre il y a plein de risques dans la banque dont nous devons être prémunis aussi. C'est un risque très technique, compliquer à cerner.
25. Selon les entretiens que j'ai réalisés dans votre banque, la plupart ont dit que c'est le rôle de Mr Didier G. de maintenir la cyber sécurité. Commenter.
Oui. Oui. Selon moi, le RSSI c'est son travail. Il est bien l'expert. Comme je vous l'ai dit, il y a une nouvelle personne qui est venu qui a des compétences techniques en plus. Donc, c'est clairement la position de la banque de ne pas laisser la faille arriver. Moi, je pense que l'expertise doit rester là où elle est actuellement, il renforce le travail informatique. C'est le meilleur endroit où ça peut être. Et en plus dans la banque, il est au sein du service, il est en contact avec tout le monde. Donc, il garde sa position pour animer le sujet, il faut qu'il puisse être en contact avec tout le monde. Je pense que c'est la meilleure position, à mon sens, c'est très bien qu'il soit là-bas.
IV. L'audit interne
1. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?
Pour moi de toute façon, au sens large, l'audit interne est réglementaire. Donc, toutes les banques ont forcément…Le régulateur c'est la BCE… vous aurez de l'audit interne dans toutes les banques. Ça ce n'est pas négociable.
Par contre, pour la cyber sécurité, toutes ces thématiques, nous avons au niveau de l'audit interne, un budget chaque année, que nous pouvons utiliser pour faire appel à des prestataires externes sur des spécificités ou expertises techniques que nous n'aurions pas dans notre collaborateur. Voilà, typiquement, la cyber sécurité en fait partie. Si nous n'avions pas de comptable, peut être que nous aurions faire appel à des prestataires pour nous faire des missions comptabilité. Ça va dépendre des profils des collaborateurs de notre équipe d'audit. Or je vais vous dire que si ça se trouve, certains établissements qui ont des compétences techniques informatiques dans la sécurité, ne font pas forcement appel à un prestataire externe, peut-être qu'ils ont des compétences. Après c'est compliqué…Nous avons des budgets pour recourir à des prestataires externes. Si on peut faire des missions en internes, on les fait. Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes.

2. Décrivez l'auditeur interne dans son travail.

L'auditeur interne a toujours le même processus. Avant d'entrer sur un sujet, je vous rappelle qu'il est généraliste. Donc, c'est un sujet qu'il ne connait pas forcement. Donc, on commence par faire un programme de travail, définissions toutes les thématiques que nous allons traiter. Ça c'est l'auditeur qui va traiter. Moi, en tant que superviseur, je valide avec lui, et nous faisons valider avec notre directeur d'audit. Et après, nous définissons les questions et les thématiques, un peu comme vous. Vous avez une prise de questions. Donc, après, une fois qu'on a défini les questions et les thématiques que nous voulons avoir traité, nous allons faire des entretiens avec les audités. Donc, évidement, ils ont plein de questions, et ils vont commencer à appréhender les autres risques. Charge à nous après, de récupérer les documents pour valider et pour projet ce que les audites nous ont annoncé mais de façon orale. Donc, on a toujours cette démarche d'aller vérifier et de garder preuve de ce qu'on nous dit. Et donc, avec tout ça, avec ces documents, entre les questions, nous apportons des réponses à nos questions, et nous identifions les risques. Donc, il est censé de ne pas avoir a priori l'auditeur. L'auditeur est ponctuel. Les constats que nous mettons à jour, on ne peut pas les opposés. Ce sont des constats avec des preuves. Ils ne sont pas opposables. Et donc, nous allons en fin de mission, de toute façon, allez expliquer nos constats aux audités. Nous allons leur faire adhérer à nos constats puisque c'est toujours la démarche de l'audit de faire adhérer les constats. S'ils ne sont pas d'accord, ils ont le droit de le reprendre. On trouve toujours un accord en fin. Et après, si nous identifions un risque, nous émettons des recommandations et donc cette recommandation permet de couvrir le risque. Donc, le service qui récupère une recommandation, est chargé de trouver une solution pour couvrir les risques identifiés sur le sujet. Donc, enfin, l'auditeur, nous suivons ces recommandations qui sont suivies toute l'année pour qu'elles soient mise en œuvre.

3. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?

Objectivité parce que nous sommes attachés au DG. Nous sommes indépendants vis-à-vis de tous les autres services du groupe. Nous avons tout pouvoir entre guillemets, nous avons accès à tous les éléments, les informations. On ne peut pas nous faire de rétention d'informations, et d'autre façon, notre premier client est notre directeur général. Évidemment, nous sommes au service de nos clients. Nous sommes là pour protéger la banque et protéger aussi nos clients. Néanmoins, nous n'avons pas de pressions. Si nous avons quelques choses à dire, nous le disons. Et comme nous avons de toute façon toujours des constats, qui ne peuvent pas être mise en cause, nous avons pouvoir de le dire. Après l'établissement choisit de couvrir ou pas les risques, ce n'est pas notre problème. Si le directeur général ne souhaite pas recouvrir un risque, ce de sa responsabilité. Notre travail est de mettre à jour les risques, de les identifier. Et donc s'il vient à arriver qu'il n'accepte pas à couvrir un risque majeur ou grave. Donc, on est indépendant, clairement indépendant.

4. Votre fonction est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?

Alors oui. Agile ça c'est le propos de la banque populaire

Notre service aussi. Il est agile. Puisque je vous disais, on peut avoir accès à toutes les informations. Mais, il y a beaucoup d'informations qui ne sont pas disponibles. Il y a un manque d'information. Donc, on n'a pas toujours tout ce qu'on veut. Donc, on est toujours très agile. On essaye de trouver toujours des solutions. Ça demande beaucoup d'énergie, mais ça on sait faire.

En termes de cyber sécurité, je vais vous dire que ce n'est pas le sujet à l'audit actuel. A l'audit actuellement, ce n'est pas le sujet principal la cyber sécurité. C'est un sujet niveau banque. A l'audit, c'est un sujet parmi tant d'autres. Notre rôle au quotidien est la protection de la clientèle. En termes de régulateur, ce n'est pas la cyber sécurité. Nous, on rendait compte, il faut que nos clients soient bien traités, qu'ils aient toutes les informations nécessaires utiles contre leurs ennemies. Ça c'est notre occupation comme régulateurs. En termes de sécurité, on se protège. Mais nous, notre ennemie est notre problème si on ne se protège pas. Le régulateur ne demande pas de se protéger. Donc, ce n'est pas notre mission principale au niveau de l'audit.

V. Les autres acteurs

1. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?
Oui, si on a besoin, bien sûr. Si ça va servir la mission et pour réduire les attaques, et pour des risques qu'on ne peut pas identifier, on fera bien intervenir des prestataires. Je pense là que le directeur général devrait être conscient du sujet.
2. Comment tenir la direction responsable de la prise en considération des constations d'audit et de la mise en œuvre des mesures correctives ?
Pour les constats, tous les constats qui sortent de nos missions, moi personnellement je les verrouille, entre guillemets au sens interne. Je les verrouille c'est-à-dire que je vérifie effectivement les constats, les constats remis en cause. Donc, je vérifie d'ailleurs, ce qu'on appelle la piste d'audit. Donc, dès que nous avons un constat, nous avons la preuve de ce que nous avançons et nous n'allons pas les présenter à la direction générale et aux audités quand nous ne sommes pas sûr de nos constats.
Tous les constats que nous présentons ont été vérifiés, ils sont verrouillés, il n'y a aucun souci.
Après donc les fautes que nous avons émis les recommandations, pour qu'on puisse les identifier. Moi, à mon niveau, je suis tous les trimestres. On a ce qu'on appelle un suivi de recommandations. Et donc, je suis dans l'avancement des recommandations que les services ont souffrance pour y trouver des solutions. Je peux les accompagner à trouver des solutions malgré tout avec les connaissances que j'ai. Et de toute façon, pour les recommandations, chaque recommandation a une durée de mise en œuvre, c'est-à-dire si vous avez identifié un problème sur un sujet dans un service, on va lui donner un an pour trouver une solution pour couvrir le service. Pendant cette année, tous les trimestres, je relance ce service pour dire est ce que cette recommandation est en avance. Est-ce que vous êtes bloqué ? Est-ce que vous avez un souci ? Mon rôle est de faire un reporting auprès du directeur général, pour faire attention dans ce service-là, c'est que ce sujet, ils ont un peu mal à le gérer, il faut le faire avancer. En toute façon, moi j'alerte. J'alerte la direction générale. Et je reste en fonction d'accompagnement au niveau du service. En toute façon derrière, nous avons un vrai suivi des constats que nous avons, que nous avons vu. Nous avons mis là-dessus, et une fois que le conseil mis en œuvre, je vérifie parce qu'il m'apporte la preuve, que la recommandation était mise en œuvre, moi je vérifie que la preuve, ils ont toujours un support écrit qui atteste que la recommandation est traitée.
3. Parler de votre mission d'audit sur les responsables de TI.
En général, je ne sais pas répondre à seuil du coup. Ma mission, est que je coordonne beaucoup, j'essaye de voir toutes les problématiques de la banque, de faire le lien entre toutes les sujets de la banque. Au-delà de ça, on a tous les intérêts de se préserver aux intérêts de la banque. Si je peux avoir une information d'un côté, puis transmettre une fois à l'autre. Voilà, mon rôle je suis à l'écoute. Après, je n'ai pas un rôle non plus. Moi, je suis à l'écoute.
4. Comment la fonction d'audit interne coordonne-t-elle son travail avec celui des auditeurs externes, de façon à assurer une couverture adéquate des questions à traiter, quelle que soit son approche à l'égard de la dotation en personnel ? Aussi relation avec les responsables de TI ?
5. Décrit l'auditeur interne, lorsqu'il vient faire son travail ?
Euhhhh ! Là comment dire. Lorsqu'il vient faire son travail ! Le matin, il avance tous les jours sur ces questions, il a des questions à qui il faut répondre. Tous les matins, il est ouvert, il fait plutôt des propositions, il est à l'écoute de ses audités quand il pose des questions s'il n'a pas la réponse. C'est des gens contentieux, des gens contentieux, qui cherchent à savoir la part des choses lorsqu'ils mettent des constats. Après au quotidien, il arrive le matin à son poste, il fait ses contrôles, il a éventuellement des entretiens à réaliser avec les audités. Au quotidien, moi, je ne suis pas régulièrement avec eux. On reste au quotidien à l'écoute. S'ils ont des problèmes, moi, je suis là pour les écouter, pour trouver des solutions. Donc, c'est un auditeur, qui va communiquer dans la banque, avec son directeur, ou avec moi-même. Ils communiquent énormément avec les audités, avec ses co-équipiers aussi. Et c'est quelqu'un qui ne reste pas tout seul. S'il a un problème, il va en parler tout de suite. En tout cas, c'est quelqu'un qui est agile, autant que moi. Une personne qui n'a pas de luxe d'avoir du temps à perdre. On a plein d'audits. On a une liste

de mission à réaliser pendant l'année. Ainsi, il faut allez vite. Il faut allez vite. L'agilité donc est au quotidien. Il faut être inventif. Et puis, il faut avoir de l'énergie en revanche, beaucoup d'énergie et trouver des solutions rapidement à ces problèmes. Il faut que les auditeurs soient bien faits et comprendre les sujets rapidement.

6. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ? Commenter.

Oui, c'est sûr. Pour le passée, l'audit était plutôt. En fait, le positionnement de l'audit et ses missions ont changé depuis quelques années. Avant, c'était sanctions, il y avait des procédures qu'on ne respecte pas, ce n'est pas bien. Depuis quelques années, peut-être 4 ou 5 ans, l'audit est plus dans un rôle d'audit conseil. Donc, on va leur rapporter des solutions, on voit des problèmes et on les aide à trouver des solutions, on est plus dans le conseil. Maintenant les gens ont peur, ils ont peur de ce qu'ils ne connaissent pas. Donc, ils pensent qu'on va les…On va mettre en cause leur travail au quotidien. Non, évidement, lorsqu'on trouve une faille, forcément, il faut directement là conserver. On va les identifier la cause, des défaillances que nous trouvons. C'est-à-dire c'est un problème, si dans un service, ils nous ont dit que personnes de mes collègues font ça, forcément, le travail serait moins bien fait. Donc, nous, nous allons mettre en cause de dire : Bien non, vous avez un problème, ce n'est pas que le travail est mal fait, ce qui vous demande c'est l'effectif. Enfin, ils ont peur de l'inconnu, ils ont peur de se sanctionner, de mettre en cause leur travail. Alors qu'en fait, ce que nous regardons ce n'est pas leur travail mais le processus. Ça va du mal à leur faire comprendre, que ce ne sont pas les personnes que nous auditons mais les processus au sens large.

7. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ? avec les employés ?

Dans l'équipe d'audit, moi, dans mon quotidien, c'est de l'écoute. C'est de l'écoute au quotidien. C'est beaucoup de ressenti. Il y en a un qui n'est pas bien, qui est fatigué, qui est énervé. Voilà, c'est bien une motivation, trouver de l'intérêt, trouver des solutions lorsqu'ils ont des problèmes. C'est de l'écoute, de l'accompagnement, de l'accompagnement au quotidien. Donc, au sein de l'équipe, effectivement, mon rôle est assez central pour animer, pour réduire les détentions entre les équipes ça arrive. C'est un risque comme un autre. Donc, moi je suis à l'écoute et la surveillance, comme je l'ai dit, même si je suis là pour que le travail soit fait. Et mon rôle est que le travail soit fini en fin d'année. Et cette double casquette, où il fait qu'ils s'apprennent non plus, que la situation est variante et qu'il faut trouver la solution par n'importe quelle manière possible.

8. Comment faites-vous pour établir de bonnes relations avec les employés ?

Dans les autres services, on va dire en externe, c'est pareil. Je suis en audit pour rappeler les tensions si les services sont en souffrance, même quand nous les auditons de toute façon. Je suis là quand il y a moins de compréhension, ou un manque de disponibilité, je suis là pour trouver des solutions. Pour moi mon rôle, c'est vraiment, de plaisir tout le monde, et de leur prouver que l'audit peut trouver des solutions, et qu'on n'est pas là juste pour travailler. Notre rôle est d'identifier un problème et d'y trouver des solutions qui pourront les aider de toute façon. Donc, voilà, je n'ai pas trop de souci au sein de la banque, j'ai de bonnes relations avec tout le monde, je n'ai pas de problèmes et au sein de l'équipe, c'est pareil. Et voilà, c'est aussi, de faire que tout ça passe bien, et faire attention aux tensions au sein des équipes, de phase de transparence, être à l'écoute de tous, et donner des informations aux autres quand ils le veulent, et d'être à l'écoute de prendre les informations qui sont à prendre à l'extérieur du service.

VI. Bref Questionnaire Socio démographique

1. Sexe Féminin
2. Année de naissance 1970
3. Etat-Civil Célibataire
4. Niveau de formation achevée Bac+4
5. Profession Superviseur d'audit

VII. En fin d'entretien

1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ? Non
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ? Non, nous avons abordé beaucoup de questions
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective 80 min
6. Signature.

A2.5 Guide d'entretien avec le directeur des risques conformité et contrôle permanent

Le Guide d'entretien du directeur des risques conformité et contrôle permanent à la BPVF

I. Questions Propres

1. Qu'est-ce que vous avez faits pendant vos études ?

J'ai commencé par une formation bancaire dans le CFPB qui est le centre de formation de la profession bancaire. Puis, j'ai achevé un master M2 en management général à l'ESSEC Business School.

2. Comment avez-vous trouvez ce travail ?

J'ai trouvé mon travail grâce à une annonce d'emploi.

3. Pouvez-vous nous expliquer votre rôle et vos missions ?

Je suis directeur des risques conformité et contrôle permanent. Donc, j'ai en charge un ensemble des risques, pas tout à fait ensemble, parce que je n'ai pas dans mon périmètre la sécurité des biens et des personnes. Et puis immobilier, je n'ai pas les locaux, sinon j'ai tous les risques opérationnels, risque de crédit, de conformité, risques financiers… en effet tous les risques de non-conformité.

4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?

J'ai passé les tests.

5. Vous êtes directement arrivé à ce poste? Ou vous avez avancé d'un poste à un autre dans cette banque ?

Non, moi j'ai commencé actuellement dans une agence. Puis, j'ai fait tous les postes : clientèle, gérant, sous-directeur, directeur, directeur du groupe.

6. C'est-a-dire vous connaissez le fonctionnement ? le processus dans la banque ? puisque vous avez passé dans tous les postes ?

Oui, du côté commercial, tous les postes.

7. D'après vous, quelles sont les qualités requises d'un directeur des risques conformité et contrôle permanent?

Les qualités. Euhhhh. Il faut être pragmatique, et la vision est d'être le plus opérationnel. Comme j'ai travaillé dans le réseau, ça me permet de comprendre les risques auxquels nous sommes exposés et donc du coup, de prévenir les risques de non-conformité comme il le faut. Gérer donc et tenter de prévenir et relater ces risques ou tous ce j'ai pu détecter comme anomalie auprès de la direction générale. Mon objectif est de rapporter les risques à la direction générale, de prévenir les risques.

8. Justement, quel est le degré d'interaction que vous avez avec les réseaux métier en termes de SSI ?

Ma réponse est que la sécurité des informations concerne tout le monde.

II. Lien avec l'entreprise

9. Pourquoi travaillez-vous dans le secteur bancaire ?

Euhhhh, pour gagner de l'argent, pour vivre.
10. Pourquoi travaillez-vous dans cette banque ?
Euhhhh, parce que c'est une banque régionale, et donc le mode de fonctionnement qui me convient. C'est-à-dire c'est une banque humaine qui me convient.
11. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?
Euhhhh, Oui.
12. Selon vous, ce qui vous valorise dans votre travail, est ce que c'est votre expérience antérieure ou votre expérience après ?
Euhhhh, dans mon poste, ce qui me valorise c'est mon expérience d'après.
13. Pourquoi travaillez-vous ?
Pour gagner ma vie.
14. Combien de salariés ? de départements ?
Euh, pour être exacte, il y a des directions, je ne sais pas exactement le nombre de département.
III. Cyber sécurité
15. Que penser vous lors que vous entendez le terme « cyber sécurité » ?
Ce qu'on entend par cyber sécurité, c'est tout ce qui est lié à la sécurité de nos données, donc de la data. Et Cyber donc, parce qu'on se pose sur internet, et aussi la cyber criminalité où il faut se protéger soit au vol, au phishing, par rapport à la data et les entrées numériques.
16. Commenter une mission de cyber sécurité.
Pardon. Je ne comprends pas. C'est un travail effectué par un service extérieur je crois à la banque.
17. Quelles difficultés y rencontre-t-on ?
Les difficultés, c'est bien de circonscrire en temps d'une peine, de bien savoir les cybers attaques, pour qu'on fasse des protections pour éviter de se faire attaquer.
18. Qui est responsable de maintenir la cyber sécurité dans la banque ?
Le RSSI. C'est le responsable de sécurité et système informatique qui est responsable de maintenir la cybersécurité dans notre banque.
19. C'est seulement selon vous, lui qui est responsable maintenir la cyber sécurité dans la banque ?
Oui, c'est seulement son rôle la sécurité de l'information.
20. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? sont-elles été suivies ?
Je ne sais pas Nous devons être technique effectivement, on devrait être attentif, prudents dans ce domaine car on peut laquer en compétence.
21. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?
Oui, tout à fait.
22. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?
Mon rôle c'est de prendre les bonnes décisions, de faire le bon budget, un équilibre entre humain et technique et financier. Parce que technique, il faut avoir de l'argent pour faire des quêtes, il faut avoir de l'argent pour mettre les machines en travail, il faut avoir de l'argent pour faire des tests d'intrusion et de communication.
23. C'est-à-dire, selon vous, il ne faut pas y avoir une sensibilisation, par exemple, lorsque vous utilisez votre ordinateur, de ne pas le laisser connecter sur internet, peut être votre courrier ouvre un fichier de phishing et va créer un problème de cyber sécurité ?
Pour les utilisateurs, c'est déjà fait, pas d'amélioration, c'est déjà fait.
24. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cybersécurité?
Oui, ils ont besoin des formations je crois chaque deux an.
25. Sont-ils suffisant ? ces formations chaque deux an ?
Je ne sais pas. Chacun a son propre rôle.
Il faut le faire, sensibiliser et ré-sensibiliser c'est tout pareil. Ce n'est pas seulement le sujet car il

y a d'autres risques que le cyber. Il y a plein de risque. Il faut sensibiliser les gens, donc il faut avoir le bon canal, le bon message, il faut qu'il soit retenu. Ré-sensibiliser une entreprise c'est renvoyer une information, l'information la plus efficace.
26. La surveillance efficace de la cyber sécurité est-elle assurée ?
Oui, c'est une obligation.
27. Pouvez-vous m'expliquer le travail que vous faites avec les opérateurs informatiques ? responsables informatiques ? en matière de cyber sécurité ?
Ils sont forcément associés à mon travail. On est toujours lié, parce que moi j'ai un responsable informatique sous ma responsabilité. Bien sûr, les personnes qui sont en informatique sont bien impliquées dans leurs travaux et participent aussi à nos travaux.
28. Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cybersécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
A l'audit interne, non, surtout non. L'audit interne c'est du niveau 3. Le niveau 3 est opérationnel. Moi je suis en niveau 2, moi je ne peux pas être opérationnel.
C'est au niveau 1 de l'être. Moi, je ne suis pas uniquement pour concerter, pour orienter, pour sensibiliser. Mais je n'ai pas un rôle opérationnel. Donc, je ne suis pas au niveau 3. Ce n'est pas à l'audit interne de le faire.
L'audit interne fait des audits. Autrement, on peut faire des audits, ce n'est pas elle qui doit assurer sur la sécurité.
29. Quelle est le rôle de l'audit interne en matière de cyber sécurité? selon vous? ou elle n'a pas un rôle?
Si, elle a un rôle, de contrôle périodique. En France, vous avez le contrôle permanent de niveau 3, le contrôle permanent de niveau 2 c'est moi, et le contrôle de niveau 3 c'est l'audit. Le niveau 3 il fait des missions ponctuelles, des missions qui peuvent être sur la cyber criminalité. Mais un rôle d'audit ni un rôle de contrôle ni un rôle de gérer l'opérationnel.
IV. L'audit interne
1. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?
Là c'est une obligation règlementaire. Nous sommes obligés d'avoir une fonction d'audit interne dans toutes les banques.
2. Parler de votre relation de travail avec l'audit interne.
L'audit interne. Avec l'audit interne, on est en relation très proche, dès lors qu'il fait des missions d'audit sur n'importe quel sujet ou autre, il peut émettre des recommandations aussi bien à l'exploitant de niveau 1, qu'au niveau de moi en termes de contrôle, il peut aussi exercer des contrôles, des contrôles d'habilitation par exemple.
3. Parler de votre relation avec l'auditeur hors du travail en décrivant le comportement de l'auditeur interne dans votre travail.
Moi je ne le vois pas à titre personnel. Je ne le vois seulement que dans le monde du travail.
4. Décrit l'audit interne comme personne dans son travail.
Ils sont des gens sérieux, qui sont très perfectif de leur rôle, justement de bien maintenir, de bien saturer, que le travail effectué par le niveau 1 et le niveau 2 correspondent à la règlementation. Comme j'irai tenter de faire, des missions de façon périodiques. Donc, voilà, je n'ai pas de problème particulier avec l'audit interne.
5. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?
Comme moi, ils sont rattachés directement au directeur générale, et forcement ils sont indépendants. Ils ont rôle, un lien hiérarchique avec le directeur général, et il a un lien fonctionnel avec l'inspection générale du groupe BPCE. Comme moi, je peux avoir un lien hiérarchique avec le directeur général, et j'ai un lien fonctionnel avec les directeurs du groupe BPCE de la direction du risque.
6. Pouvez-vous me réexpliquer la partie où vous m'avez dit que vous êtes rattachés à l'audit

?
Je ne suis pas rattaché à l'audit. Dans sa mission, s'il détecte des anomalies, il émet des recommandations. Les recommandations me sont adressées parce que, il y aurait peut-être un contrôle que je n'aurai pas fait, ou mal fait. D'après ces recommandations, que j'ai plusieurs mois pour mettre en place ce qu'il me demande de faire.
7. Quel est votre comportement lorsque vous avez eu de l'auditeur interne un rapport où il y a un dysfonctionnement ou une anomalie en termes de sécurité des informations ?
On essaye de voir si cette anomalie constatée à notre niveau est effectivement réelle, et l'anomalie est bien présente, si l'anomalie est présente, et qu'on doit répondre à la règlementation. On exécute comme nous dit la recommandation.
8. Votre fonction est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?
Donc, je suis prêt à évoluer dans tous les domaines forcement dans le domaine de la cyber sécurité dont nous sommes faibles. Donc, il faut se prémunir.

V. Les autres acteurs
1. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?
Oui, on l'a déjà fait l'année passée.et par contre l'année prochaine, on va la refaire.
On n'a pas les gens compétents, et quand on ne les a pas, on fait appel à un cabinet.
2. Pouvez expliquer ce point en détail.
On n'avait pas la compétence pour faire ce que l'audit nous demande de faire. Donc, on a fait appel à un cabinet pour nous alerter sur le fait des tests d'intrusion, qui sont sur la partie technique, et c'est un constat mais sur la partie technique, pas sur la partie organisation. Et donc, pour faire ce qu'on devait faire, les tests d'intrusion, au niveau de prévention cyber, de faire un scan des données qui étaient sur le serveur, donc un certain nombre de missions, d'actions de mesure d'effectuer en interne.
3. Ce cabinet est-il spécialisé en informatique ?
Oui, tout à fait, c'est ça.
4. Vous voyez que cette procédure va se répéter chaque année ?
Oui, tous les ans, tous les ans il faut le faire.
5. Vous voyez que cette procédure passe dans toutes les banques ? ou seulement dans la banque populaire ?
Je ne sais pas. De toute façon, c'est une obligation. Le régulateur nous met en garde de plus en plus sur ce risque de vol de donnée qui peut être sanctionné. Donc, c'est une chose qui est assez grave sans compter le risque de faille. Donc, c'est une chose sur lesquelles banques sont sensibles, le groupe BPCE l'ait, maintenant les autres banques je ne sais pas, mais je crois qu'ils le sont même que nous.
6. Comment tenir la direction responsable de la prise en considération des constations d'audit et de la mise en œuvre des mesures correctives ?
C'est ce que nous avons fait suite à une recommandation, la recommandation est donnée suite à une anomalie, il suffit de porter la preuve qui répond exactement, au attente pour qu'on puisse lever. C'est-à-dire que la recommandation a été réalisée.
Il faut apporter les preuves que les recommandations ont été mené ou réalisée.
7. Décrit l'auditeur interne, lorsqu'il vient faire son travail ?
Ils sont plusieurs, chacun a son type et sa personnalité différente. En générale, ils sont plutôt dans l'attente, ils viennent écouter, ils y écoutent, ils demandent en avance des preuves sur les informations que nous avons présentée. C'est-à-dire qu'on fait des contrôles mais ils veulent des preuves qu'on a bien réalisé les contrôles. Ils sont alors attentifs, mais vigilants, à bien s'assurer que tous ce qui a été dit, a été fait.
8. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ?
Non, mais, ça s'est fini ça. Ça a été vingt temps et ça a changée. Ils ne sont pas inquiétés du tout.

Parce qu'avant, il n'y avait pas ce niveau 1, niveau 2, niveau 3, les rôles, les contrôles, les audits, les audits contrôles. Un audit c'est un contrôle, donc quand ils faisaient un contrôle, les gens se sentaient inquiets avant l'heure. Donc, maintenant, c'est fini. Les rôles sont clairement définis, et le niveau 3 n'a pas de pouvoir de sanction non plus.
9. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ?
Parler, c'est avec la communication.
10. Avec les employés ?
On échange sur la pertinence des questions qu'ils ont posées et de l'orientation de leurs missions. Des fois, on est plus ou moins d'accord, on leur dit. Mais je discute tout avec l'équipe. C'est un échange, si je ne suis pas d'accord avec les conclusions, ils doivent tenir compte de mes remarques.
VI. Bref Questionnaire Socio démographique
1. Sexe
Male
2. Année de naissance
1969
3. Etat-Civil
Monsieur GROMBERT
4. Niveau de formation achevée
BAC+5
VII. En fin d'entretien
1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ? NON
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ? NON
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu
5. Durée effective 1 heure 4 minutes
6. Signature.

A3. Guide d'entretien auprès des établissements bancaires libanais

A3.1 Guide d'entretien avec l'analyste principale de sécurité informatique chez banque of Beirut (BOB)

Le Guide d'entretien avec un analyste principal de sécurité informatique chez BOB

I. Questions Propres
1. Qu'est-ce que vous avez faits pendant vos études ?
Mes études. J'ai achevé une licence pour trois ans en informatique à Université Saint-Esprit de Kaslik. Puis, j'ai achevé un master en génie informatique et communication dans la même université.
2. Comment avez-vous trouvez ce travail ?
Après avoir pris quelques mois de congé et quelques emplois secondaires, j'ai commencé ma recherche d'emploi. Mon objectif était d'en trouver un où je pourrais avoir un meilleur travail, une vie meilleure.
En 2009, j'ai commencé comme stagiaire à « Global Technology Solutions » S.A.R.L pour trois mois. Puis, en 2012, j'ai trouvé un travail comme ingénieur technique chez « SAMA » S.A.L.
J'ai commencé à travailler sur mon profil LinkedIn en ajoutant une photo de profil, en mettant à jour mon résumé, mon expérience de travail et en remplissant le reste de mon profil.

En 2014, J'ai été contacté via LinkedIn pour une entrevue pour un poste à la banque BOB. J'ai reçu une offre d'emploi pour analyste principale de sécurité informatique – chef d'équipe que j'ai fini par accepter.

3. Pouvez-vous nous expliquer votre rôle et vos missions ?

Mon travail en tant que chef d'équipe d'analystes responsable de la sécurité consiste à assurer la sécurité de la banque en appliquant les meilleures pratiques et en analysant les événements pour protéger ses données, son réseau et tous ses systèmes. Donc, je suis responsable des équipes d'analystes en sécurité informatique. Je coordonne les équipes, donc, j'animer les missions que nous réalisons, pour que les travaux soient bien accomplis.

Nous planifions et prenons des mesures de sécurité pour protéger les réseaux et systèmes informatiques de la banque. Nos responsabilités s'élargissent continuellement à mesure que le nombre de cyber attaques augmente. Nous devons continuellement nous adapter pour garder une longueur d'avance sur les cybers attaquants. Nous devons rester à jour sur les dernières méthodes utilisées par les attaquants pour infiltrer les systèmes informatiques et sur la sécurité informatique. Nous devons rechercher de nouvelles technologies de sécurité pour décider de ce qui protégera le plus efficacement leur organisation. Cela peut impliquer parfois que nous assistons à des conférences sur la cybersécurité pour entendre les témoignages d'autres professionnels qui ont connu de nouveaux types d'attaques.

4. Par quels chemins êtes-vous arrivé à ce poste ? Quel est ton parcours, ta formation ?

J'ai postulé pour ce poste en sachant que j'avais 2 ans d'expérience en tant qu'ingénieur technique de la sécurité informatique. En plus, j'ai obtenu plusieurs certificats de sécurité :

- je suis devenu professionnel certifié en sécurité des systèmes d'information « CISSP »
- Certificat « Cyber threat intelligence » issu de l'association des banques au Liban.

Donc, c'était pour moi, comme un sur classement de poste d'accepter ce poste comme analyste principal de sécurité de l'informatique et chef de l'équipe.

5. D'après vous, quelles sont les qualités requises d'un analyste de sécurité informatique?

Bonne formation technique en informatique, expérience en sécurité, bonnes compétences analytiques. Il faut aussi savoir gérer l'équipe et résoudre les problèmes.

6. Justement, quel est le degré d'interaction que vous avez avec les réseaux métier en termes de SSI ?

Mon rôle est de paramétrer les systèmes de supervision de la sécurité. Comme je vous l'ai dit, je supervise le travail de l'équipe qui catégorise, analyse et traite les alertes de sécurité de façon régulière pour en améliorer l'efficacité.

Dans le domaine de la cybersécurité, nous analysons et nous interprétons les alertes, les événements corrélés et nous recherchons les vulnérabilités. Nous devons collaborer pour identifier les lacunes d'accès et de collecte qui peuvent être comblées par des activités de cyber collecte et / ou de préparation, et exploiter toutes les ressources et techniques d'analyse autorisées pour pénétrer les réseaux ciblés.

II. Lien avec l'entreprise

7. Pourquoi travaillez-vous dans le secteur bancaire ?

Le secteur bancaire libanais : c'est un secteur solide, sûr et important qui offre différentes opportunités.

8. Pourquoi travaillez-vous dans cette banque ?

Je connais tous les produits bancaires et aussi les avantages qu'ils offrent aux clients lorsque nous les comparons aux produits offerts par d'autres banques. Je préfère travailler ici, car je crois honnêtement que c'est la banque des gens. Et c'est une des meilleures banques libanaises selon mon avis.

9. Etes-vous capable de travailler dans une autre banque ? un autre établissement ?

Oui.

10. Selon vous, ce qui vous valorise dans votre travail, est ce que c'est votre expérience antérieure ou votre expérience après ?

Mon expérience d'après.

11. Pourquoi travaillez-vous ?

Je travaille pour acquérir de l'expérience et être un individu efficace dans la société en s'assurant que la confidentialité, l'intégrité et la disponibilité sont préservées.

12. Combien de salariés ? de départements ?

Je ne sais pas exactement combien il y a de salariés, de départements.

III. Cyber sécurité

13. Que penser vous lors que vous entendez le terme « cyber sécurité » ?

Confidentialité, piratage, risque, attaques. Je pense à la menace qui signifie tout danger potentiel pour notre entreprise, ses biens ou ses employés. La cybersécurité permet de garantir que les données de notre organisation sont à l'abri des attaques. Si d'autres personnes accèdent à ces informations sensibles, notre banque pourrait voir sa carte bancaire ou de crédit volée ou compromise.

14. Commenter une mission de cyber sécurité.

Dans notre banque, on n'a jamais eu une attaque en cybersécurité.

Notre gestion de crise en cas de cyber attaques est relative à un protocole que le directeur de notre département est en charge d'appliquer. Normalement, le protocole de gestion de crise est au niveau du directeur de département, qui lorsqu'il est avertis d'une cyber attaque importante, il va réunir les chefs d'équipes des établissements rattachés à cette attaque. Aussi, il va réunir la cellule de crise. Elle comporte : moi, tous les chefs des équipes, les opérateurs informatiques rattachés spécialement à la cellule, le chef de département.

15. Quelles difficultés y rencontre-t-on ?

La difficulté est bien d'analyser les risques, de bien soigner la situation de façon à ne pas aggraver la situation ou vis à vis des clients.

16. Qui est responsable de maintenir la cyber sécurité dans la banque ?

Pour moi, pas seulement notre département. Mais tous les employés sont responsables de maintenir la cybersécurité dans la banque. Une bonne sécurité ne concerne pas les meilleurs outils. Celles-ci changent beaucoup trop souvent. Cela commence par la culture et les gens. Nous devons les évaluer et notre programme de sécurité suivra. Nous ne devons pas supposer que nos employés savent tout ce qu'ils doivent savoir sur la sécurité informatique. Nous devons faire une formation continue à tous les employés sur les risques technologiques et la cybersécurité ... Ce processus comprend l'établissement et le maintien des rôles de sécurité informatique.

17. Que penser vous des formations en matière de sécurité ? de cyber sécurité ? sont-elles été suivies ?

Oui. Ils sont très importants. Nous faisons ces formations deux fois par an.

18. Est-ce que la haute direction est informée des impacts de la cybercriminalité dans votre banque ?

Oui, la haute direction est directement informée des impacts de la cybercriminalité. Si notre département de sécurité informatique détecte une anomalie, un cyber attaque, là haute direction est directement informée de cette attaque. Je transmets l'analyse faite par mes équipes des dysfonctionnements en sécurité informatique au directeur du département de sécurité informatique, qui à son tour, va alerter la haute direction.

19. Quel rôle pouvez-vous jouer pour renforcer la cybersécurité dans votre travail ?

Je dois être toujours à jour avec ce qui se passe dans le cyber monde afin de mettre toutes les mesures. Je dois sensibiliser et être toujours prêt à réagir aux incidents en termes de cybersécurité. Je dois donner une grande importance au détail et à l'analyse de chaque incident dans mon travail.

20. Les employés ont-ils besoin d'une formation régulière sur la sensibilisation à la cybersécurité?

Oui. Il faut qu'ils soient toujours à jour spécialement dans le domaine de cybersécurité.

21. La surveillance efficace de la cyber sécurité est-elle assurée ?

Oui.

22. Certaines disent de confier à l'audit interne le rôle de maintenir la cyber sécurité dans une banque ? Que pensez-vous ? c'est-à-dire s'ils disent c'est le rôle de l'audit interne de maintenir la cyber sécurité ? Et pas le rôle ni des opérationnelles ni des responsables de la sécurité.
Ce n'est pas vrai, les agents de sécurité jouent un rôle obligatoire dans le maintien de la sécurité. L'équipe d'audit interne doit faire son travail qui est « l'audit ».
Le service d'audit interne s'assure qu'il n'y a pas de lacunes et que le travail de cybersécurité est en cours mais ce n'est pas lui qui effectue et analyse les tâches et événements de cybersécurité. C'est le rôle de notre département de sécurité informatique.

IV. L'audit interne

1. Votre banque, devrait-elle avoir une fonction d'audit interne ? Pourquoi ne pas recourir seulement à un auditeur externe ?
Oui, il doit avoir une fonction d'audit interne afin d'auditer et de vérifier régulièrement les pratiques des différents services. Mais, il vaut peut-être mieux avoir également un audit externe, car nous aurons une double vérification en cours.
2. Parler de votre relation de travail avec l'audit interne.
Je ne les vois que lorsqu'ils viennent auditer notre service de sécurité informatique. Au moment où l'audit choisit de faire un examen à la limite de la sécurité des cadres de données, ils dirigent un nombre spécifique de réunions, et donc ils viennent à nous pour poser un nombre spécifique de questions selon un guide d'audit. Ils viennent après revoir et suivre que ce qui est dit est complet. Ils feront également des vérifications narratives. À ce stade, il y a deux cas:
Il est possible qu'ils distinguent un danger qui n'est pas sécurisé, ils donneront une suggestion pour faire un plan d'activité qui pourrait être l'exécution d'un autre contrôle. Il est possible qu'ils ne reconnaissent aucune particularité et par conséquent, il ne donne pas de propositions.
3. Parler de votre relation avec l'auditeur hors du travail en décrivant le comportement de l'auditeur interne dans votre travail.
Je les vois ou j'interagis rarement avec eux. Je ne les vois que lorsqu'ils viennent auditer notre service de sécurité informatique. À part cela, il n'y a aucune relation avec l'auditeur interne dans notre travail quotidien.
4. Avec les autres employés il y a une relation ?
Non, je n'ai pas de relations avec autres employés. Sauf, dans le domaine de la sécurité des systèmes d'information, dans les différents métiers de l'informatique plutôt, j'ai des relations régulières avec les autres collaborateurs de mon équipe.
5. Comment la fonction d'audit interne conserve-t-elle son indépendance et son objectivité ?
Je crois que les auditeurs internes conservent leur indépendance et objectivité en gardant une distance sociale avec les autres employés.
6. Votre fonction est-elle agile et prête à s'améliorer continuellement selon le besoin ? spécialement en cyber sécurité ?
Oui, nous avons besoin toujours d'être à jour dans tous les domaines de sécurité, pas seulement la cyber sécurité.
7. Quelles qualités le chef d'audit devrait-il posséder ?
Je ne sais pas. Peut-être il faut demander cette question à l'audit lui-même.
8. L'audit interne doit-il s'appuyer sur d'autres fonctions ?
De même, pas de réponse.
V. Les autres acteurs
1. Pourriez-vous envisager l'intervention d'autres experts pour maintenir la cyber sécurité ?
Oui, pourquoi pas peut être un service extérieur, des testeurs externes.
2. Décrit l'auditeur interne, lorsqu'il vient faire son travail ?
Ils sont des gens très sérieux, qui viennent seulement faire leur travail. Ils sont complexes et exigeants.

3. Est-ce que les employés ont peur lorsqu'il y a un audit ? Sont-ils inquiets ? intimidés ?
Certains d'entre eux oui. Parce que c'est comme avoir un test, bien sûr, l'employé est un peu inquiet, a souligné. Mais pour nous, nous ne sommes pas intimidés par les missions d'audit car nous nous appuyons sur notre expertise et notre expérience en sécurité informatique.
4. Comment faites-vous pour établir de bonnes relations avec l'équipe d'audit interne ? avec les employés ?
Non, il n'y a pas d'action particulière vis-à-vis des auditeurs, parce que c'est ce que je vous disais tout à l'heure. Il y a seulement interaction lors des missions d'audit. Par contre, pour les autres employés, j'ai des relations avec eux spécialement dans mon équipe et mon département mais avec des limites.
VI. Bref Questionnaire Socio démographique
1. Prénom, Nom C. Kh.
2. Sexe Féminin
3. Année de naissance 07/05/1987
4. Etat-Civil Célibataire
5. Niveau de formation achevée Master en génie informatique et communication
6. Profession Analyste principal de la sécurité de l'information
VII. En fin d'entretien
1. Avez-vous quelque chose à ajouter, d'autres renseignements à transmettre que vous avez peut-être oubliez de dire ou que l'entretien n'a pas permis de toucher ? Non, je crois que l'entretien a abordé toutes les questions relatives à l'audit et à la cybersécurité.
2. Comment vous avez trouvé ce questionnement ? Si vous aurez ajouté ou supprimez des questions ? Non, c'était un bon entretien.
3. Je vous remercie pour votre temps et votre participation.
4. Date et Lieu Beirut,
5. Durée effective 58 min

A3.2 Guide d'entretien avec l'auditeur interne informatique chez Banque AUDI

Le Guide d'entretien avec un auditeur interne informatique chez Banque AUDI en Anglais

I. Socio Demographic Questions
1. Name : Jad
2. Gender: Male
3. Birth Date: 02/02/1989
4. Civil Status: Single
5. Profession: IT Auditor
II. Personal Questions
1. What did you do during your studies?
a. Systems and Network Engineering
2. How did you find this job?
a. Referenced by a friend
3. Can you explain your role and your missions?
a. Perform Information Systems Audit reviews
4. How did you get to this job? What is your background, your training?
a. I applied, I got interviewed three times and I got an offer
b. My background comes from IT system and network administration (Previous experience)
5. In your opinion, what are the qualities required of an IT internal Auditor?

a. Motivation, Hard Work, Integrity, Fluent English, patience…
III. Link with the company
1. Why do you work in the banking sector?
a. Because it is one of the most stable sectors in Lebanon
2. Why do you work in this specific bank?
a. Because it is a Alpha bank
3. Are you able to work in another bank? Another establishment?
a. Yes, sure thing
4. In your opinion, what values you in your work, is it your previous experience or your experience after?
a. Both, my previous experience was pure IT and my current experience is a mix between IT skills previously acquired and current experience in Auditing…
5. Why do you work ?
a. To stay updated with the newest trends, technologies…
b. To earn money
6. How many departments ? Employees ?
a. Audit department is around 28 employees.
III. Cybersecurity
1. What do you think when you hear the term "cyber security"?
a. Security of the whole system and network environment
2. Who is responsible for maintaining cyber security in the bank?
a. A specific department named ISBC (Information Security and Business Continuity)
3. What do you think of security training? Cyber security? Have they been followed?
a. Security training is essential since this is a field that constantly changes, hence the importance of training. Yes, the bank usually sends us to follow trainings
4. Is senior management informed of the impact of cybercrime on your bank?
a. Yes
5. What role can you play to strengthen cyber security in your work?
a. Due to the nature of our work (Issuing audit reports), management, IT Operations and IT Security take action based on the contents of the reports.
6. Do employees need regular cyber security awareness training?
a. Of course
7. Can you explain to me the work you do with the Information operators? Is there a relation regarding cyber security?
a. Yes of course, the IS Audit work is mostly related to cyber security.
8. Some say to entrust internal audit with the role of maintaining cyber security in a bank? What do you think? It is the role of internal audit to maintain cyber security? And not the role of operational staff or security officials (IT)
a. Incorrect, IS Audit by itself cannot handle the Cyber security role. They are actually the third line of defense. It is a group work that includes Information Security department, IT Operations and Audit. And even the employees themselves.
IV. Internal Audit
1. Should your bank have an internal audit function? Why not just use an external auditor?
a. By regulations, all banks operating in Lebanon must have an Internal Audit function
2. Talk about your working relationship with internal audit.
a. N/A
3. Talk about your relationship with the auditor outside of work by describing the behavior of the internal auditor in your work.
a. There is not direct relationship between myself and the external auditors, we usually share our reports by Email.

4. Is there a relationship with the other employees?
a. Our relations usually involve IT and IS Staff at the Bank.
5. How does the internal audit function maintain its Independence and objectivity?
a. IA employees are carefully chosen, they cannot audit areas that they previously worked on…
6. How internal audit function can conserve her independence and objectivity ?
a. Same as above
V. Other Actors
1. Could you consider the intervention of other experts to maintain cyber security?
a. Of course, external auditors, penetration testers…
2. Describes the internal auditor, when he comes to do his work?
a. Initiation meeting, Field work, report creation…
3. Are employees afraid when there is an audit? Are they worried? Intimidated?
a. Sometimes, it depends on the person…
4. How do you go about building good relationships with the internal audit team? With employees?
a. It all depends on the method of performing of the Audit, we usually focus that the goal of our Audit is not finding mistakes and blaming employees, however it is to lower the risk…
5. Comment your audit mission on the IT department.
a. Audit missions usually go smooth, especially since the staff does not change must often…
b. It all starts with an initiation meeting, including why will we perform the Audit, and what is the goal, then we ask for few documents, we analyze those documents, we obtain results, share those results with the auditees, and finally we issue the report that goes the the management…
6. Did you have any incident while auditing the IT department with the IT staff?
a. Not really, everything is normally smooth.

Annexe B : Méthodologie de codage des guides d'entretiens

B1. Méthodologie de codage du guide d'entretien du directeur de la conformité à la BPVF

Codage du Guide d'entretien du directeur de la conformité

Nous commencerons l'analyse par un repérage des niveaux du discours considéré comme un récit. Selon Roland Barthes, tout récit peut être analysé selon trois niveaux correspondant à trois lectures différentes mais nécessairement articulées :

- Le niveau des fonctions est celui auquel se déploient les épisodes du récit que nous appellerons des séquences. Nous les numéroterons par (S). Ces séquences racontent le parcours de Pascal Gombert dans la banque.
- Le niveau des actions concerne les éléments du récit qui mettent en scène des « actants », c'est-à-dire des personnages qui agissent, interviennent, jouent un rôle dans le récit. Nous numéroterons tous les éléments de l'entretien comprenant de tels indices d'actant par (A).
- Le niveau de la narration se repère par la présence de thèses, d'arguments, de propositions destinées à nous convaincre, à défendre son point de vue. Nous noterons ces parties de l'entretien par (P).

Premier codage de l'entretien

47 questions = 47 séquences

Codage du Segment 1 (§1) :

« J'ai commencé par une formation bancaire dans le CFPB qui est le centre de formation de la profession bancaire. » (S1.1)

« Puis, j'ai achevé un master M2 en management général à l'ESSEC Business School. » (S1.2)

Codage du Segment 2 (§2) :

« J'ai trouvé mon travail grâce à une annonce d'emploi. » (S2.1)

Codage du Segment 3 (§3) :

« Je suis directeur des risques conformité et contrôle permanent. » (S3.1)

« Donc, j'ai en charge un ensemble des risques, pas tout à fait ensemble, parce que je n'ai pas dans mon périmètre la sécurité des biens et des personnes. » (P3.1)

« Et puis immobilier, je n'ai pas les locaux, sinon j'ai tous les risques opérationnels, risque de crédit, de conformité, risques financiers… en effet tous les risques de non-conformité. » (P3.2)

Codage du Segment 4 (§4) :

« J'ai passé les tests. » (S4.1)

Codage du Segment 5 (§5) :

« Non, moi j'ai commencé actuellement dans une agence. » (S5.1)

« Puis, j'ai fait tous les postes : clientèle, gérant, sous-directeur, directeur, directeur du groupe. » (S.5.2)

Codage du Segment 6 (§6) :

« Oui, du côté commercial, tous les postes. » (S6.1)

Codage du Segment 7 (§7) :

« Les qualités. Euhhhh. » (P7.1)

« Il faut être pragmatique, et la vision est d'être le plus opérationnel. » (P7.2)

« Comme j'ai travaillé dans le réseau, ça me permet de comprendre les risques auxquels nous sommes exposés et donc du coup, de prévenir les risques de non-conformité comme il le faut. » (P7.3 et S7.1)

« Gérer donc et tenter de prévenir et relater ces risques ou tous ce que j'ai pu détecter comme anomalie auprès de la direction générale. » (P7.4)

« Mon objectif est de rapporter les risques à la direction générale, de prévenir les risques. » (A7.1 et S7.2)

Codage du Segment 8 (§8) :

« Ma réponse est que la sécurité des informations concerne tout le monde. » (P8.1)

Codage du Segment 9 (§9) :

« Euhhhh, pour gagner de l'argent, pour vivre. » (P9.1)

Codage du Segment 10 (§10) :

« Euhhhh, parce que c'est une banque régionale, et donc le mode de fonctionnement qui me convient. » (P10.1)

« C'est-à-dire c'est une banque humaine qui me convient. » (P10.2)

Codage du Segment 11 (§11) :

« Euhhhh, Oui. » (P11.1)

Codage du Segment 12 (§12) :

« Euhhhh, dans mon poste, ce qui me valorise c'est mon expérience d'après. » (P12.1)

Codage du Segment 13 (§13) :

« Pour gagner ma vie. » (P13.1)

Codage du Segment 14 (§14) :

« Euh, pour être exacte, il y a des directions, je ne sais pas exactement le nombre de département. » (P14.1)

Codage du Segment 15 (§15) :

« Ce qu'on entend par cyber sécurité, c'est tout ce qui est lié à la sécurité de nos données, donc de la data. » (P15.1)

« Et Cyber donc, parce qu'on se pose sur internet, et aussi la cyber criminalité où il faut se protéger soit au vol, au phishing, par rapport à la data et les entrées numériques. » (P15.2)

Codage du Segment 16 (§16) :

« Pardon. Je ne comprends pas. » (P16.1)

« C'est un travail effectué par un service extérieur je crois à la banque. » (P16.2)

Codage du Segment 17 (§17) :

« Les difficultés, c'est bien de circonscrire en temps d'une peine, de bien savoir les cybers attaques, pour qu'on fasse des protections pour éviter de se faire attaquer. » (P17.1)

Codage du Segment 18 (§18) :

« Le RSSI. C'est le responsable de sécurité et système informatique qui est responsable de maintenir la cybersécurité dans notre banque. » (A18.1)

Codage du Segment 19 (§19) :

« Oui, c'est seulement son rôle la sécurité de l'information. » (A19.1)

Codage du Segment 20 (§20) :

« Je ne sais pas. » (P20.1)

« Nous devons être technique effectivement, on devrait être attentif, prudents dans ce domaine car on peut laquer en compétence. » (P20.2)

Codage du Segment 21 (§21) :

« Oui, tout à fait. » (P21.1)

Codage du Segment 22 (§22) :

« Mon rôle c'est de prendre les bonnes décisions, de faire le bon budget, un équilibre entre humain et technique et financier. » (S22.1)

« Parce que technique, il faut avoir de l'argent pour faire des quêtes, il faut avoir de l'argent pour mettre les machines en travail, il faut avoir de l'argent pour faire des tests d'intrusion et de communication. » (S22.2 et P22.1)

Codage du Segment 23 (§23) :

« Pour les utilisateurs, c'est déjà fait, pas d'amélioration, c'est déjà fait. » (S23.1)

Codage du Segment 24 (§24) :

« Oui, ils ont besoin des formations je crois chaque deux ans. » (P24.1)

Codage du Segment 25 (§25) :

« Je ne sais pas. » (P25.1)

« Chacun a son propre rôle. » (P25.2)

« Il faut le faire, sensibiliser et ré-sensibiliser c'est tous pareil. » (P25.3)

« Ce n'est pas seulement le sujet car il y a d'autres risques que le cyber. » (S25.1)

« Il y a plein de risques. » (S25.2)

« Il faut sensibiliser les gens, donc il faut avoir le bon canal, le bon message, il faut qu'il soit retenu. » (P25.4)

« Ré-sensibiliser une entreprise c'est renvoyer une information, l'information la plus efficace. » (P25.5)

Codage du Segment 26 (§26) :

« Oui, c'est une obligation. » (P26.1)

Codage du Segment 27 (§27) :

« Ils sont forcément associé à mon travail. » (S27.1)

« On est toujours lié, parce que moi j'ai un responsable informatique sous ma responsabilité. » (S27.2 et P27.1)

« Bien sûr, les personnes qui sont en informatique sont bien impliquées dans leurs travaux et participent aussi à nos travaux. » (S27.3)

Codage du Segment 28 (§28) :

« A l'audit interne, non, surtout non. » (P28.1)

« L'audit interne c'est du niveau 3. » (S28.1)

« Le niveau 3 est opérationnel. » (S28.2)

« Moi je suis en niveau 2, moi je ne peux pas être opérationnel. » (P28.2)

« C'est au niveau 1 de l'être. » (S28.3)

« Moi, je ne suis pas uniquement pour concerter, pour orienter, pour sensibiliser. » (P28.3)

« Mais je n'ai pas un rôle opérationnel. » (P28.4)

« Donc, je ne suis pas au niveau 3. » (S28.4)

« Ce n'est pas à l'audit interne de le faire. » (S28.5)

« L'audit interne fait des audits. » (S28.6)

« Autrement, on peut faire des audits, ce n'est pas elle qui doit assurer sur la sécurité. » (P28.5)

Codage du Segment 29 (§29) :

« Si, elle a un rôle, de contrôle périodique. » (S29.1)

« En France, vous avez le contrôle permanent de niveau 3, le contrôle permanent de niveau 2 c'est moi, et le contrôle de niveau 3 c'est l'audit. » (S29.2)

« Le niveau 3 il fait des missions ponctuelles, des missions qui peuvent être sur le cyber criminalité. » (S29.3)

« Mais un rôle d'audit ni un rôle de contrôle ni un rôle de gérer l'opérationnel. » (S29.4)

Codage du Segment 30 (§30) :

« Là c'est une obligation règlementaire. » (S30.1)

« Nous sommes obligés d'avoir une fonction d'audit interne dans toutes les banques. » (S30.2)

Codage du Segment 31 (§31) :

« L'audit interne. » (A31.1)

« Avec l'audit interne, on est en relation très proche, dès lors qu'il fait des missions d'audit sur n'importe quel sujet ou autre, il peut émettre des recommandations aussi bien à l'exploitant de niveau 1, qu'au niveau de moi en termes de contrôle, il peut aussi exercer des contrôles, des contrôles d'habilitation par exemple. » (S31.1 et A31.2)

Codage du Segment 32 (§32) :

« Moi je ne le vois pas à titre personnel. » (A32.1)

« Je ne le vois seulement que dans le monde du travail. » (A32.2)

Codage du Segment 33 (§33) :

« Ils sont des gens sérieux, qui sont très perfectif de leur rôle, justement de bien maintenir, de bien saturer, que le travail effectué par le niveau 1 et le niveau 2 correspondent à la règlementation. » (A33.1)

« Comme j'irai tenter de faire, des missions de façon périodiques. » (P33.1)

« Donc, voilà, je n'ai pas de problème particulier avec l'audit interne. » (P33.2)

Codage du Segment 34 (§34) :

« Comme moi, ils sont rattachés directement au directeur général, et forcement ils sont indépendants. » (A34.1)

« Ils ont rôle, un lien hiérarchique avec le directeur général, et il a un lien fonctionnel avec l'inspection générale du groupe BPCE. » (A34.2)

« Comme moi, je peux avoir un lien hiérarchique avec le directeur général, et j'ai un lien fonctionnel avec les directeurs du groupe BPCE de la direction du risque. » (S34.1 et A34.3)

Codage du Segment 36 (§36) :

« Je ne suis pas rattaché à l'audit. » (P36.1)

« Dans sa mission, s'il détecte des anomalies, il émet des recommandations. » (A36.1)

« Les recommandations me sont adressées parce que, il y aurait peut-être un contrôle que je n'aurai pas fait, ou mal fait. » (S36.1)

« D'après ces recommandations, que j'ai plusieurs mois pour mettre en place ce qu'il me demande de faire. » (S36.2)

Codage du Segment 37 (§37) :

« On essaye de voir si cette anomalie constatée à notre niveau est effectivement réelle, et l'anomalie est bien présente. » (S37.1)

« Si l'anomalie est présente, et qu'on doit répondre à la règlementation, on exécute comme nous dit la recommandation. » (S37.2)

Codage du Segment 38 (§38) :

« Donc, je suis prêt à évoluer dans tous les domaines forcement dans le domaine de la cyber sécurité dont nous sommes faibles. » (P38.1)

« Donc, il faut se prémunir. » (P38.2)

Codage du Segment 39 (§39) :

« Oui, on l'a déjà fait l'année passée, et par contre l'année prochaine, on va la refaire. » (S39.1)

« On n'a pas les gens compétents, et quand on ne les a pas, on fait appel à un cabinet. » (A39.1)

Codage du Segment 40 (§40) :

« On n'avait pas la compétence pour faire ce que l'audit nous demande de faire. » (P40.1)

« Donc, on a fait appel à un cabinet pour nous alerter sur le fait des tests d'intrusion, qui sont sur la partie technique, et c'est un constat mais sur la partie technique, pas sur la partie organisation. » (A40.1)

« Et donc, pour faire ce qu'on devait faire, les tests d'intrusion, au niveau de prévention cyber, de faire un scan des données qui étaient sur le serveur, donc un certain nombre de missions, d'actions de mesure d'effectuer en interne. » (S40.1 et P40.2)

Codage du Segment 41 (§41) :

« Oui, tout à fait, c'est ça. » (P41.1)

Codage du Segment 42 (§42) :

« Oui, tous les ans, tous les ans il faut le faire. » (P42.1)

Codage du Segment 43 (§43) :

« Je ne sais pas. » (P43.1)

« De toute façon, c'est une obligation. » (P43.2)

« Le régulateur nous met en garde de plus en plus sur ce risque de vol de donnée qui peut être sanctionné. » (A43.1)

« Donc, c'est une chose qui est assez grave sans compter le risque de faille. » (P43.3)

« Donc, c'est une chose sur lesquelles banques sont sensibles, le groupe BPCE l'ait, maintenant les autres banques je ne sais pas, mais je crois qu'ils le sont même que nous. » (A43.2 et P43.4)

Codage du Segment 44 (§44) :

« C'est ce que nous avons fait suite à une recommandation, la recommandation est donnée suite à une anomalie, il suffit de porter la preuve qui répond exactement, à l'attente pour qu'on puisse lever. » (S44.1)

« C'est-à-dire que la recommandation a été réalisée. » (S44.2)

« Il faut apporter les preuves que les recommandations ont été mené ou réalisée. » (S44.3)

Codage du Segment 45 (§45) :

« Ils sont plusieurs, chacun a son type et sa personnalité différente. » (A45.1)

« En générale, ils sont plutôt dans l'attente, ils viennent écouter, ils y écoutent, ils demandent en avance des preuves sur les informations que nous avons présentée. » (A45.2)

« C'est-à-dire qu'on fait des contrôles mais ils veulent des preuves qu'on a bien réalisé les contrôles. » (A45.3 et S45.1)

« Ils sont alors attentifs, mais vigilants, à bien s'assurer que tous ce qui a été dit, a été fait. » (A45.4)

Codage du Segment 46 (§46) :

« Non, mais, ça s'est fini ça. » (P46.1)

« Ça a été vingt temps et ça a changée. » (P46.2)

« Ils ne sont pas inquiétés du tout. » (P46.3)

« Parce qu'avant, il n'y avait pas ce niveau 1, niveau 2, niveau 3, les rôles, les contrôles, les audits, les audits contrôles. » (S46.1)

« Un audit c'est un contrôle, donc quand ils faisaient un contrôle, les gens se sentaient inquiets avant l'heure. » (P46.4)

« Donc, maintenant, c'est fini. » (P46.5)

« Les rôles sont clairement définis, et le niveau 3 n'a pas de pouvoir de sanction non plus. » (S46.2 et P46.6)

Codage du Segment 47 (§47) :

« Parler, c'est avec la communication. » (P47.1)

Codage du Segment 48 (§48) :

« On échange sur la pertinence des questions qu'ils ont posées et de l'orientation de leurs missions. » (P48.1)

« Des fois, on est plus ou moins d'accord, on leur dit. » (A48.1)

« Mais je discute tout avec l'équipe. » (P48.2)

« C'est un échange, si je ne suis pas d'accord avec les conclusions, ils doivent tenir compte de mes remarques. » (P48.3 et A48.2)

1. Classement des unités codées : Recodage

A. Les séquences-types de l'entretien de Pascal Gombert

Nous allons maintenant regrouper et ordonner les séquences dans l'ordre chronologique depuis le départ (S0) jusqu'à la fin de l'entretien (S+). Nous allons joindre toutes les unités concernées (tous les S) en leur donnant un titre résumant leur contenu.

Nous avons divisé l'entretien de Pascal Gombert en quatre séquences respectives selon l'ordre chronologique.

1. Niveau de formation et progression de la carrière

S0=S1.1+S1.2+S2.1+S4.1+S5.1+S5.2+S6.1+S7.1

2. Fonction de directeur des risques conformité et contrôle permanent : Rôle et missions

Sa=S3.1+S7.2+S22.1+S22.2+S23.1+S25.1+S25.2+S27.1+...+S27.3+S31.1+S34.1

3. Audit interne : Rôle et mission par rapport à la cybersécurité

Sb=S28.1+...+S28.6+S29.1+...+S29.4+S30.1+S30.2+S31.1+S34.1

4. Conséquence d'une faille ou anomalie sur le travail de Pascal

Sc=S36.1+S36.2+S37.1+S37.2+S39.1+S40.1+S44.1+S44.2+S44.3+S45.1+S46.1+S46.2

Nous allons maintenant proposer un premier résumé des séquences-types de l'entretien de Pascal Gombert après avoir effectué le regroupement selon un ordre chronologique.

Résumé des séquences-types de l'entretien de Pascal Gombert

Au début de l'entretien, Pascal Gombert nous explique son parcours professionnel puis son insertion professionnelle dans la BPVF. Il commence par une formation bancaire dans le CFPB en achevant après un master M2 en management général à l'ESSEC Business School. Puis, il a fait tous les postes de la banque et ça lui a donné une vision particulière et un riche contexte pour comprendre les risques auxquels la banque est exposée et donc de prévenir les risques de non-conformité comme il le faut.

Il résume son rôle de directeur des risques conformité et contrôle permanent à rapporter les risques à la direction générale et de prévenir les risques. Son rôle est de prendre les bonnes décisions, de faire le bon budget, un équilibre entre humain et technique et financier. Il clarifie que les problèmes techniques sont différents à gérer par contrainte de coût et d'argent même s'il a un responsable informatique sous sa direction.

Pascal justifie que l'audit interne est en niveau 3 de surveillance. L'audit n'a aucun rôle d'assurer la cybersécurité mais seulement un rôle de mener des missions ponctuelles sur la cybercriminalité c'est-à-dire un rôle opérationnel.

Pascal énonce qu'il reçoit les recommandations sur un contrôle qu'il a mal fait ou pas exécuter. Il est assujetti après de se méfier de la présence des anomalies de suivre les recommandations associées à ces anomalies. En cas de cybersécurité, Pascal obtient les recommandations sur ce qu'il devait faire au niveau des tests d'intrusion, au niveau de prévention cyber, et de faire un scan des données qui étaient sur le serveur, donc un certain nombre de missions, d'actions de mesure d'effectuer en interne. Il termine en affirmant que les rôles des différents acteurs dans la banque sont clairement définis, et l'audit interne n'a pas de pouvoir de sanction non plus.

B. Les actants du récit de Pascal Gombert

Nous allons ici identifies les personnages dans le récit de Pascal Gombert. Nous allons inclure Pascal lui-même lorsqu'il se dédouble (« moi, je…).

Nous notons respectivement les acteurs de A1 jusqu'à An.

Le premier actant du récit est Pascal lui-même puisqu'il a utilisé le « moi » 10 fois.

Le second actant est le responsable de sécurité et de système informatique (RSSI) « Didier G. ».

A2= A18.1+A19.1

Le troisième actant est l'audit interne.

A3=A31.1+A31.2+A32.1+A32.2+A33.1+A34.1+A34.2+A34.3+A36.1+A45.1+...+A45.4+A48.1+A48.2

Le quatrième actant est le cabinet extérieur embauché par la banque.

A4=A39.1+A40.1

Le cinquième actant est le régulateur.

A5=A43.1

Le sixième actant est la BPCE.

A6=A43.2

Les actants du récit de Pascal GOMBERT

Le premier actant est Pascal Gombert lui-même. Nous remarquons qu'il a fréquemment utilisé le « moi » dans son récit pour donner son avis ou son opinion.

Le deuxième actant est le RSSI « Didier G. ». Pascal confirme que c'est lui qui est responsable d'assurer la cybersécurité dans la banque.

Le troisième actant est l'audit interne. Pascal est en relation directe avec les auditeurs internes grâce aux missions d'audit et des exercices de contrôle. Il les décrit comme des gens sérieux, qui sont très perfectif de leur rôle, justement de bien maintenir, de bien saturer, que le travail effectué par le niveau 1 et le niveau 2 correspondent à la règlementation. Ils sont indépendants ayant un lien hiérarchique avec le directeur général et il a un lien fonctionnel avec l'inspection générale du groupe BPCE. Pascale ajoute qu'ils sont alors attentifs, mais vigilants, à bien s'assurer que tous ce qui a été dit, a été fait.

Le quatrième actant est le cabinet externe embauché par la direction générale. Pascal justifie le recours à un cabinet externe par manque de compétence technique informatique en cas de cybersécurité. Pascal appuie sur le rôle du cabinet embauché en cybersécurité qui consiste à alerter les employés sur le fait des tests d'intrusion, qui sont sur la partie technique. Pascal explique qu'il faut agir sur l'aspect technique et non pas l'aspect organisationnelle.

Le cinquième actant est le régulateur de la BPVF. Selon Pascal, le régulateur rappelle que le vol de donnée a pour pénalité d'être sanctionné.

Le sixième actant est la BPCE. Ce groupe sensible contre la cybersécurité fait appel à un cabinet externe spécialisé en sécurité informatique pour l'assurer.

C. Les classes d'arguments

Ce niveau d'analyse concerne l'ensemble des arguments, démonstrations et propositions de Pascal Gombert destinés à nous convaincre. Nous allons regroupés l'ensemble des unités codées en P selon des « classes d'arguments » dont chacune représente une étape logique dans un raisonnement. Nous allons classer les arguments le type de raisonnement que Pascal présente dans ces réponses. Nous en avons repéré six qui font l'objet d'arguments explicites qui sont à la base de ce classement.

Nous avons noté (P1) les propositions de Pascal Gombert associé à son travail dans la banque. Elle a expliqué plusieurs fois que c'est le hasard et l'opportunité qui l'ont amené dans la BPVF et son présent poste.

Nous résumons cet ensemble ainsi : *« Le travail par hasard et par opportunité dans le secteur bancaire ».*

Nous avons noté (P2) les expressions de Pascal associés aux exigences de l'auditeur interne dans la banque. Elle a les mêmes exigences que ceux des auditeurs internes :

Cet ensemble se résume ainsi : *« Travail semblable, profil très proche que celui des auditeurs internes ».*

Nous avons noté (P3) toutes les formules associées à la zone de confort de Pascal dans son travail et ses avantages positifs.

Cet ensemble se résume ainsi : *« Impliquée dans sa banque : Bonne connaissance, rattachée et fidèle. »*

Nous avons noté (P4) les faiblesses et désavantages du métier de Pascal en cybersécurité :

« En termes de SSI, **ce n'est pas notre confort**, c'est vraiment un métier très spécifique. » (P5.1)

- « **Ce sont <u>des expertises</u> que nous n'avons pas forcement**, donc, il y a rien à réaliser des missions sur les SSI. » (P5.2)
- « Par contre, moi, j'ai **une sensibilité sur tout ce qui est environnement informatique.** » (P5.5)
- « Et après, je suis **<u>moins expert</u>** en ce métier. » (P5.8)
- « « Non, je **<u>n'ai pas les compétences</u>**. » (P13.1)
- « Mais, en tout cas, **<u>moi je n'ai pas les compétences à mon niveau</u>**. » (P13.3)
- « Pour moi, c'est **un nouveau sujet.** » (P14.5)
- « C'est **un nouveau sujet pour nous**, il faut savoir à mettre en compétences. » (P14.6)
- « Il y a très peu de gens qui sont sensibles à ce sujet et ce sont **des vraies compétences que nous n'avons pas pour l'instant chez nous.** » (P14.7)
- « **Je ne sais pas**. » (P15.1)
- « On ne peut pas **être généraliste sur un sujet pareil**. » (P15.4)
- « Il faut appeler **<u>un expert</u>** sur le sujet pour savoir s'il y a une faille ou pas. » (P19.4)

Nous résumons cet ensemble : *« L'audit interne est faible en compétence technique, il n'a pas les expertises spécifiques dans ce domaine de cybersécurité. »*

Nous avons noté (P5) les expressions et les formules relatives à la cybersécurité :

- « C'est le **danger numéro 1** on va dire. » (P12.1)
- « Pour moi, c'est **le danger numéro 1** dans les entreprises actuellement. » (P12.2)
- « Et puis, c'est **un risque qui s'est largement sous-estimé** parce que **ça coûte cher.** » (P12.3)
- « Et que déjà, c'est un **nouveau risque**, et ça va mettre du temps à appréhender. » (P12.4)
- « Et pour moi c'est **un danger, un vrai danger, un danger** qui doit être une préoccupation pour toutes les entreprises au-delà les banques. » (P12.5)

- « Pour moi, c'est une préoccupation de tous, parce qu'on peut tous se faire attaquer si on prend des risques. » (P16.3)
- « Mais, c'est l'affaire de tous, il faut que ce soit une préoccupation de tous. » (P16.1)
- « Clairement, mais pour ça il faut animer le sujet, il faut que les gens **prennent conscience** que **c'est un danger**. » (P16.5 et S16.1)
- « Et le danger peut venir de partout. » (P16.6)
- « Voilà, pour moi, c'est l'affaire de tous. » (P16.7)
- « On commence à faire **prendre conscience aux gens** que c'est un sujet qui a des risques informatiques, qu'il **faut faire attention** à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. » (S17.5)
- « Pour moi, **c'est bien ce qu'on fait.** » (P17.3)
- « Et que tout le monde soit expert sur le sujet. » (P17.4)
- « Moi, je crois qu'ils ont pris conscience du danger. » (P18.2)
- « Ça coûte cher et ça prend du temps. » (P18.3)
- « Il faut dire attention. » (P19.3)
- « C'est **un risque très très technique**, compliquer à cerner. » (P23.12)

Nous résumons cet ensemble par le raisonnement de Pascal. *Elle explique que la cybersécurité doit être un problème de tous les employés dans la banque car c'est le danger numéro 1. Il faut sensibiliser tous les employés et prendre conscience du danger de ce risque. C'est un danger qui coûte cher et qui va prendre du temps à appréhender. Elle argumente qu'elle fait jusqu'à maintenant un bon travail de formation et de sensibilisation à ce risque, mais ce n'est pas suffisent, il faut plus de travail.*

Nous avons noté (P6) les expressions et les formules associés à qui est responsable d'assurer la cybersécurité :

- « La cyber sécurité**, c'est un métier**, une façon de se parler, de s'exprimer. » (P21.3)
- « La cybersécurité, **c'est un vaste sujet**, que personne, à l'instant, il y a peu de gens qui savent ce qui montre ce sujet. » (P17.7)
- « On peut avoir notre rôle à jouer en termes de détection d'application un **peu orpheline** dans certains services. » (P19.6)
- « La cybersécurité, pour moi, **c'est un métier**, aussi vrai, **le responsable de cyber sécurité est un métier qui évolue**. » (P23.5)
- « Selon moi, **le RSSI** c'est son travail. » (P24.2 et A24.1)
- « Il **est bien l'expert.** (RSSI) » (A24.2)
- « Comme je vous l'ai dit, il y a **une nouvelle personne** qui est venu qui a **des compétences techniques en plus.** » (P24.3)
- « Moi, je pense que **l'expertise** doit rester là où elle est actuellement, il renforce le travail informatique. » (P24.4)
- « C'est le **meilleur endroit** où ça peut être. » (P24.5)

Pascal a expliqué que c'est le rôle d'une part de tous d'assurer la cybersécurité. L'audit interne est faible en compétence et expertise technique dans ce domaine. Elle admet que la cybersécurité est un métier qui doit être indépendant. Le RSSI et la nouvelle personne embauchée qui vient l'assister ont les expertises et compétences spécifiques pour appréhender les risques de la cybersécurité.

D. Le schème provisoire de l'entretien

Nous allons tout d'abord restituer le schème en situant les arguments dans leur ordre d'intervention dans le récit et en les mettant en relation « spatiale » avec les deux autres classes d'unités précédemment recodées : les séquences et les actants. Nous allons les présenter dans ce tableau qui constituera un schème provisoire de l'entretien.

	Séquences (Sn)	Arguments (Pn)	Actant (An)
Niveau de formation et progression de la carrière (S_0)	• Je suis expertise comptable en fait. (S1.1) • J'ai réalisé un Bac+4 en comptabilité. (S1.2) • Je suis arrivé par hasard au milieu bancaire. (S1.3) • Je suis arrivée par hasard. (S1.6) • Actuellement, je travaille à l'audit. Je suis superviseur à l'audit. (S2.1) • Et au bout de 5 an, j'ai évolué vers un poste de superviseur par hasard, • Arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé. (S3.4)	• Je suis arrivé par hasard au milieu bancaire. (P1.1) • Ce n'était pas un choix de ma part (P1.2) • Je suis arrivée par hasard. (P1.3) • Un poste de superviseur par hasard, (P3.1) • C'est le moment de changer, (P3.2) • Je suis arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé. (P3.4) • J'aime bien travailler déjà, et j'aime bien découvrir de nouvelles choses (P10.2) • J'aime mon travail et je veux continuer à travailler, à progresser. (P10.4) • Je ne vois pas changer de milieu de travail. (P6.2) • Je resterai dans la banque le plus long possible. (P6.3) • C'est une banque qui me plait. (P7.1) • C'est à cause du côté mutualiste que je suis là, je reste attachée à la banque, je suis fidèle. (P7.3) • Collaboratrice fidèle aux valeurs de la banque, et à la banque elle-même, je suis fidèle à mon employeur. (P7.4)	• Le Moi.(répété plusieurs fois).
Fonction de superviseur en Audit : Rôle et missions (Sa)	• Je suis superviseur à l'audit. (S2.1) • Mon rôle c'est de coordonner les équipes, de les animer, de les amener au niveau attendu. » (S2.2) • Et donc, mon rôle est de saturer que tout est fait en temps parfait. (S2.6) • Je rappelle régulièrement tout le monde sur la cybersécurité. (S5.1) • Moi, j'ai une équipe à gérer. (S10.1) • Moi je communique énormément avec tout le monde. (S11.2)	• Rigueur, agilité, beaucoup d'ouverture d'esprit. (P4.1) • Si on a un problème, on trouve une solution rapidement. (P4.2) • Conserver l'esprit d'équipe parce qu'on est une équipe de plusieurs auditeurs. (P4.4) • Satisfaire tout le monde. (P4.5) • Préserver les intérêts des auditeurs, et préserver les services que nous auditons. (P4.6) • Diplomate (P4.7) • Généralistes, curieux. (P5.3) • Être curieux. (P9.4) • L'agilité donc est au quotidien. (P32.7) • Il faut être inventif. (P32.8) • C'est de l'écoute au quotidien. (P34.2) • C'est beaucoup de ressenti. (P34.3)	• Moi, en tant que superviseur, je valide avec lui, et nous faisons valider avec notre directeur d'audit. (A26.5) • Préserver les intérêts de la banque, découvrir les risques, et de détecter les risques pour le directeur général qui est notre principal client. (A4.1) • Notre premier client est notre directeur général. (A27.2) • Si le directeur général ne souhaite pas recouvrir un risque, ce de sa responsabilité. (A27.4) • Le directeur général devrait être conscient du sujet. (A29.2) • Reporting auprès du directeur général, pour faire attention dans ce

				service-là, c'est que ce sujet, ils ont un peu mal à le gérer, il faut le faire avancer. (A30.1) • J'alerte la direction générale. (A30.2)
Cybersécurité : Contrainte et implication (Sb)	• C'est un sujet, jusqu'à un an, qu'on ne se préoccupait pas du tout au sein de la banque. (S14.2) • Les choses ont changé, ils ont embauché quelqu'un qui devra arriver. (S14.3) • J'ai juste entendu qu'on allait renforcer le sujet. (S15.1) • C'est un côté positive qu'on a clairement conscience qu'on a besoin d'une autre personne. (S15.2) • Clairement, mais pour ça il faut animer le sujet, il faut que les gens prennent conscience que c'est un danger. (S16.1) • On est 2000 collaborateurs au sein de la banque, c'est facile d'y trouver une faille pour entrer dans la banque. (S16.2) • Oui, on a des formations, c'est pas en cyber sécurité exactement, c'est plus. (S17.1) • On commence à faire prendre conscience au gens que c'est un sujet qui a des risques informatiques, qu'il faut faire attention à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. (S17.5)	• En termes de SSI, ce n'est pas notre confort, c'est vraiment un métier très spécifique. (P5.1) • Ce sont des expertises que nous n'avons pas forcement, donc, il y a rien à réaliser des missions sur les SSI. (P5.2) • j'ai une sensibilité sur tout ce qui est environnement informatique. (P5.5) • je suis moins expert en ce métier. (P5.8) • je n'ai pas les compétences. (P13.1) • je n'est pas les compétences à mon niveau. (P13.3) • Nouveau sujet. (P14.5) • Nouveau sujet pour nous, il faut savoir à mettre en compétences. (P14.6) • On ne peut pas être généraliste sur un sujet pareil. (P15.4)		• Il est généraliste. (A26.2) • Un sujet qu'il ne connait pas forcement. (A26.3) • C'est l'auditeur qui va traiter. (A26.4) • L'auditeur est ponctuel. » (A26.9) • Il faut que les auditeurs soient bien faits et comprendre les sujets rapidement. » (A32.11) • C'est un problème, si dans un service, ils nous ont dit que personnes de mes collègues font ça, forcément, le travail serait moins bien fait. » (A33.1)
Conséquence de la cybersécurité sur la banque (Sc)	• Donc, quelque part, si on voit des failles en termes d'habilitation ou d'application qui sera un peu à la dérive ou isolé dans son coin. (S19.4) • De toute façon, nous embauchons dans le monde de banque, il y a beaucoup de jeunes qui sont embauché, beaucoup de personnes qui partent en retraite. (S20.1) • Et plus on les informe rapidement, voila, pour moi, il faut communiquer et être former. (S20.3 et P20.10) • Donc, on les a assistés, on a participé avec eux dans leurs missions. (A21.3 et S21.2) • Après notre rôle était de coordonner, de sert en sorte d'interlocuteurs, pour faciliter leurs missions. (S21.5) • Et donc, on a amené ce cabinet. (S22.3) • Je pense, je ne peux pas vous dire, je n'est pas participer au choix du cabinet (S22.4) • ce cabinet là, nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP. (S22.5) • Et le but était que les failles qui étaient identifiées puissent être corrigées. (S22.6) • Faire appel à des prestataires externes sur des spécificités ou expertises techniques que nous n'aurions pas dans notre collaborateur. (S25.3)	• Danger numéro 1 on va dire. (P12.1) • Danger numéro 1 dans les entreprises actuellement. (P12.2) • Risque qui s'est largement sous estimé parce que ça coûte cher. (P12.3) • nouveau risque, et ca va mettre du temps à appréhender. (P12.4) • Danger, un vrai danger, un danger qui doit être une préoccupation pour toutes les entreprises au delà les banques. (P12.5) • Ça coûte cher et ça prend du temps. (P18.3) • Il faut dire attention. (P19.3) • C'est un risque très très technique, compliquer à cerner. » (P23.12)		• les hackers sont de plus en plus imaginatifs, et c'est la première faille. (A20.1) • les hackers sont toujours en avance de tous le monde. (A20.2) • il ne faut pas sous estimer leurs forces. (A20.3) • les hackers sont très inventifs, très rapides, très compétents. C'est un métier qu'on ne peut pas suivre. (A23.1) • Nous avons fait appel à un cabinet extérieur. (A5.1) • En employant un cabinet, je pourrai faire des liens entre un cabinet, et lui apporté le lien entre les connaissances métier et les problématiques de cyber sécurité. » (A13.1) • On a envisagé un expert métier, un cabinet spécialisé. » (A21.1) • ce cabinet nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en

			coordination avec l'I-BP. (A22.2) • Participer un cabinet au bénéfice du groupe. (A22.6) • Les prestataires informatiques, on sentait qu'on avait besoin, on les a fait venir. (A22.3) • pas les compétences, appel à ces prestataires externes. (A25.2) • servir la mission et réduire les attaques, et des risques qu'on ne peut pas identifier, intervenir des prestataires. (A29.1)
Travail relatif à la cybersécurité (Sd)	• Ça va dépendre des profils des collaborateurs de notre équipe d'audit. (S25.6) • ont des compétences techniques informatiques dans la sécurité, ne font pas forcement appel à un prestataire externe, peut être qu'ils ont des compétences. (S25.7) • Budgets pour recourir à des prestataires externes. (S25.8) • Si on peut faire des missions en internes, on les fait. (S25.9) • Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes. (S25.10) • l'auditeur, nous suivons ces recommandations qui sont suivies toute l'année pour qu'elles soient mise en œuvre. (S26.16) • Nous sommes là pour protéger la banque et protéger aussi nos clients. (S27.1) • Mettre à jour les risques, de les identifier. (S27.5) • Accès à toutes les informations. (S28.1) • Moi j'alerte. (S30.15) • je suis à l'écoute. (S31.4)	• Très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n'avons pas pour l'instant chez nous. (P14.7) • Appeler un expert sur le sujet pour savoir s'il y a une faille ou pas. (P19.4) • préoccupation de tous, parce qu'on peut tous se faire attaquer si on prend des risques. (P16.3) • l'affaire de tous, il faut que ce soit une préoccupation de tous. (P16.1) • il faut que les gens prennent conscience que c'est un danger. (P16.5) • c'est l'affaire de tous. (P16.7) • le monde soit expert sur le sujet. (P17.4) • La cyber sécurité, c'est un métier, une façon de se parler, de s'exprimer. (P21.3) • On peut avoir notre rôle à jouer en termes de détection d'application un peu orpheline dans certains services. (P19.6) • La cybersécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue. (P23.5) • le RSSI c'est son travail. (A24.1) • Il est bien l'expert. (RSSI) (A24.2) • Nouvelle personne qui est venu qui a des compétences techniques en plus. (P24.3) • l'expertise doit rester là où elle est actuellement, il renforce le travail informatique. (P24.4)	• Je sais vous avez interviewé Didier G., ils ont embauché un expert la dessus. (A5.2) • le RSSI c'est son travail. (A24.1) • Il est bien l'expert. (A24.2) • Et en plus dans la banque, il est au sein du service, il est en contacte avec tout le monde. (A24.3) • il garde sa position pour animer le sujet, il faut qu'il puisse être en contacte avec tout le monde. (A24.4) • Je pense que c'est la meilleure position, à mon sens, c'est très bien qu'il soit là bas. (A24.5) • La nouvelle personne va arriver chez Didier G. pour collaborer avec lui. (A15.1) • Il faut qu'il y ait l'expert. (A16.1)

2. <u>Production des catégories par l'analyse structurale</u>

Notre travail présenté en ce qui précède était purement inductif. Nous allons maintenant dégager des unités de sens sur la base de notre description préalable et essentielle. Ces unités de sens sont appelées *« catégories sémiques »* selon Greimas (1986) qui sont constitutives de la logique sociale de l'entretien et de sa forme sémique.

Notre travail sera un travail démonstratif qui se reposera sur quelques principes de base qui constitueront une sorte de fonds communs de l'analyse structurelle. Conformément à notre projet de départ, nous sommes obligés de montrer la démarche en acte en introduisant des équivalents dans la littérature. Nous signalons les multiples choix sur lesquels

repose la mise en œuvre de toute démarche d'inspiration structurale. Donc, notre mise en œuvre repose sur une intelligence préalable du discours que la partie précédente n'a que formaliser.

2.1 Disjonction et Conjonction

Nous allons considérer l'hypothèse de base de l'analyse est de traduire le schème précédent en une combinaison de catégories typiques constitutive du sens général de l'entretien.

Nous assumons que la révolution structurale consiste à analyser toute langue naturelle et tous ensemble signifiant comme un système d'opposition à l'intérieure d'une relation constitutive du sens. Nous s'occupons à des « éléments différentiels » ou des « traits distinctifs » qui assurent l'existence d'une langue. Donc, ce qui est vrai au sens lexical l'est aussi au sens sémantique.

Nous admettons que le sens linguistique d'un mot ne se comprend qu'en restituant la disjonction qui le spécifie et la conjonction qui lui assure son appartenance à une catégorie. La disjonction trouve son origine dans la chaine syntagmatique constitutive du signifiant et la conjonction de l'intégration paradigmatique définissant le signifié.

2.2 Application à l'entretien et à ses trois niveaux

2.2.1 La signification des séquences : l'opposition je sais/je ne sais pas

Pascal qualifie les expériences qu'elle a tiré des différentes phrases de son parcours au moyen d'expression souvent lapidaires :

(S1) : « Si on a un problème, on trouve une solution rapidement. » (§4)

(S2) : « En termes de SSI, ce n'est pas notre confort, c'est vraiment un métier très spécifique. » (§5)

(S3) : « Ce sont des expertises que nous n'avons pas forcement, il y a rien à réaliser des missions sur les SSI. » (§5)

(S4) : « Par contre, moi, j'ai une sensibilité sur tout ce qui est environnement informatique. » (§5)

(S5) : « J'ai quand même cette sensibilité contre les sujets qui ne sont pas connus. » (§5)

(S6) : « Et après, je suis moins expert en ce métier. » (§5)

(S7) : « Et puis, c'est un risque qui s'est largement sous-estimé parce que ça coûte cher. » (§6)

(S8) : « Et que déjà, c'est un nouveau risque, et ça va mettre du temps à appréhender. » (§6)

(S9) : « Non, je n'ai pas les compétences. » (§13)

(S10) : « Mais, en tout cas, moi je n'ai pas les compétences à mon niveau. » (§13)

(S14) : « Pour moi, c'est un nouveau sujet. » (§14)

(S15) : « C'est un nouveau sujet pour nous, il faut savoir à mettre en compétences. » (§14)

(S16) : « Il y a très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n'avons pas pour l'instant chez nous. » (§14)

(S17) : « Ce qui sensibilise l'informatique, ce sont des profils très rares » (§14)

(S18) : « Je ne sais pas. » (§14)

(S19) : « C'est un côté positive qu'on a clairement conscience qu'on a besoin d'une autre personne. » (§15)

(S20) : « On ne peut pas être généraliste sur un sujet pareil. » (§15)

(S21) : « Il faut qu'il y ait l'expert. » (§16)

(S22) : « Mais, c'est l'affaire de tous, il faut que ce soit une préoccupation de tous. » (§16)

(S23) : « Pour moi, c'est une préoccupation de tous... » (§16)

(S24) : « Voilà, pour moi, c'est l'affaire de tous. » (§16)

(S25) : « Non, pour moi non. » (§16)

(S26) : « Parce que l'audit n'a pas de compétence métier. » (§16)

(S27) : « On n'est pas expert. » (§16)

(S28) : « Je disais tout à l'heure que les auditeurs sont généralistes et on n'a pas de compétence… » (§16)

(S29) : « Il faut quelqu'un qui soit dédié à ça. » (§17)

(S30) : « Nous, on en peut pas suivre, on n'a pas les compétences en tout cas. » (§17)

(S31) : « C'est un risque très très technique, compliquer à cerner. » (§17)

(S32) : « Selon moi, le RSSI c'est son travail. » (§18)

(S33) : « Il est bien l'expert. » (§18)

(S34) :« Comme je vous l'ai dit, il y a une nouvelle personne qui est venu qui a des compétences techniques en plus. » (§18)

(S35) : « Moi, je pense que l'expertise doit rester là où elle est actuellement... » (§18)

« C'est le meilleur endroit où ça peut être. » (§18)

(S36) : « Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes. » (§18)

(S37) : « des compétences techniques informatiques dans la sécurité… » (§25)

Nous allons ici faire des hypothèses en restant le plus près possibles du texte retranscrit. Nous allons rétablir les oppositions entre unités de diverses séquences-types :

- Si on a un problème, on trouve une solution rapidement/ En termes de SSI, ce n'est pas notre confort, Ce sont des expertises que nous n'avons pas forcement ;
- On n'est pas expert / Il est bien l'expert ;
- Une nouvelle personne qui est venu qui a des compétences techniques en plus / je n'ai pas les compétences ;
- On ne peut pas être généraliste sur un sujet pareil / On est curieux et généraliste dans notre travail.

L'opposition je sais/je ne sais pas concerne successivement ou simultanément trois catégories : Niveau de formation et progression de la carrière, fonction de superviseur en audit et conséquence de la cybersécurité sur la banque. Ce que Pascal précise ici clairement est qu'elle n'a pas les compétences spécifiques en cybersécurité. Il existe un poste de RSSI et une personne qui est venue l'aider spécialiste et expertise dans ce métier. Elle ajoute que dans le cas de mission d'audit sur les services informatiques, et car il y a manque de compétences techniques, il y a appel à un cabinet externe pour réaliser cette mission.

2.2.2 La signification des actants : pareils/pas pareils et mieux/pire

Nous allons procéder de la même façon pour les actants du récit de Pascal.

Nous résumons dans ce tableau ci-dessous les acteurs pareil et pas pareil à Pascal.

Pareil	Pas Pareil
Directeur de l'audit Interne (A2)	Cabinet extérieur embauché (A4)
Directeur générale (A3)	RSSI Didier G. (A5)
Clients de la banque (A6)	Nouvelle personne embauché pour aider le RSSI (A7)
Auditeur interne (A11)	Prestataires externes informatiques (A8)
Les audités (A12)	Hackers (A14)
Les employés (A13)	

Nous pouvons maintenant analyser le sens de l'opposition Pareil/Pas Pareil en retrouvant les catégories associant la conjonction de deux termes. Nous vérifions que pour Pascal, sont pareils ceux qui n'ont pas les expertises et les

connaissances techniques en cybersécurité, et pas pareils qu'elle, ceux qui ont les compétences techniques en cybersécurité. Pour Pascal le mieux sera que la cybersécurité soit une préoccupation de tous, pas seulement les experts et les RSSI. Le pire c'est de laisser les spécialistes seuls manager la cybersécurité dans la banque en formant plus les hauts employés dans les zones d'informatique et de cybersécurité. Elle signale que le danger vient de partout en disant que c'est facile de trouver une faille pour entrer dans la banque. Le pire sera plus d'attaque et de failles en cybersécurité si elle est laissée seulement à RSSI sans une coopération avec l'audit interne. Le pire c'est de se déceler de la responsabilité de la cybersécurité en justifiant que c'est hors de son expertise et champ d'application.

2.2.3 La signification des arguments : Facile/Pas facile

Pascal précise dans son discours qu'elle n'a pas les compétences en informatique et en cybersécurité. Elle dit je ne sais pas et ce n'est pas dans mon champ d'expertise, elle a une sensibilité sur tout ce qui est environnement informatique. Mais elle oppose son discours en disant :

- Qu'elle a de bonnes connaissances sur toutes les applications et les différents métiers de la banque. Mais, Elle n'a pas les compétences dans ce niveau d'informatique.
- En disant que la cybersécurité est un risque très majeur et important mais elle ne sait rien sur le sujet, elle a une sensibilité contre les sujets qui ne sont pas connus.
- En disant qu'elle est curieuse, généraliste et réalise des missions d'audit sur tous les départements, mais dans le cas de la cybersécurité, ce sont des expertises qu'elle n'a pas forcement, donc, il y a rien à réaliser des missions sur les SSI. (La banque fait recours à un cabinet externe expert en sécurité informatique)
- en disant qu'elle connait seulement l'importance de ces sujets, et rappelle régulièrement tout le monde mais elle ne se contente pas d'apprendre sur le sujet en tant que superviseur d'équipe d'audit
- en disant qu'elle est fidèle et attachée à la banque, mais elle ne préserve pas les intérêts des auditeurs, ni des clients ni du directeur général en limitant sa collaboration comme superviseur à la prévention sur la cybersécurité.

Nous analysons ces oppositions pour trouver la totalité qui donne sens à ces couples, découvrir la conjonction qui englobe cette disjonction.

2.3 La structuration de l'univers sémantique et la logique du récit

Rappelons les résultats acquis à ce stade de l'analyse. Une première opposition je sais/je ne sais pas structure les séquences. Nous l'avons décomposée selon trois propriétés combinées qui permettent de qualifier les renseignements de cybersécurité dans la banque :

- Je ne sais pas = Pas de compétence technique informatique+Pas d'expertise+recours à un cabinet externe ou prestataires externes
- Je sais = Compétence technique spécialisé en informatique+Expertise technique+assurer la cybersécurité

Une seconde opposition pareil/pas pareil structure les segments du récit qui mettent en scène des actants de la vie. Nous en avons trouvé deux propriétés principales qui permettent de qualifier les significations d'une autre « totalité » que l'on peut appeler statut :

- Pareil=Pas d'expertise+Pas de responsabilité
- Pas pareil= Expertise technique+Responsabilité de cybersécurité

Une autre opposition a été introduite pour rendre compte de la structuration du récit des actants : mieux/pire, qui renvoie à une autre « totalité » qu'il faut y avoir une collaboration pour réduire les failles et les cybers attaques.

Une troisième opposition nous a permis de structurer la narration Pascal et de qualifier la relation précédente facile/pas facile. Nous allons extraire donc les propriétés suivantes :

- Facile=expertise technique acquise+compétence technique+connaissance
- Pas Facile=Incompétent domaine informatique+coûte cher+Prend du temps

Nous allons terminer notre analyse par-là construction d'axes croisés permettant d'attribués des propriétés identiques à plusieurs significations dégagées antérieurement. Nous proposons pour l'entretien de Pascal les schémas suivants :

Tableau 1. Situation et perspectives professionnelles de Pascal

	Positives (Je sais)	Négatives (Je ne sais pas)
Possible (Facile)	J'alerte tout le monde	Cabinet Externe et Coopération
Impossible (Pas Facile)	Prestataire externe expert et spécialiste	Préoccupation de tous, il faut du travail.

Tableau 2. Personnages propre et perspectives professionnelles de Pascal

	Semblables (Pareil)	Différents (Pas Pareil)
Positives (Mieux)	Auditeurs internes, Directeur générale, Directeur de l'audit	Cabinet externe spécialiste, Prestataire externe expert
Négatives (Pire)	Employés, clients, Audités	RSSI seul responsabilité

B2. Méthodologie de codage du guide d'entretien du directeur de l'audit interne à l'I-BP

Le codage du guide d'entretien du directeur de l'audit interne

Premier codage de l'entretien

36 questions = 36 séquences

Codage du Segment 1 (§1) :

Donc, moi je suis à l'origine, je suis ingénieur, précisément ingénieur à l'institut de Lyon en Informatique. (S1.1)
Euhhhh, Bon Après, j'ai fait une étude en 3ième cycle en gestion complété ça et puis depuis j'ai fait pas mal de formation continue dans le cadre de mission. (S1.2)
En particulier, je suis certifié donc sésame et Sillac, sont deux certifications d'audit interne international, et je suis aussi… (S1.3)

Codage du Segment 2 (§2) :

Alors, je suis rentré en inspection générale des banques populaires. (S2.1)
Donc répondant à une annonce, et donc après un parcours de quelques années en inspection, j'ai créé d'audit interne pour la structure informatique banque populaire. (S2.2)

Codage du Segment 3 (§3) :

Euhhhh, parce que je dirais que c'est un secteur qui a des moyens déjà, c'est un secteur qui est intéressant, puis voilà c'est un secteur qui me plaisait bien en super affinité. (P3.1)

Codage du Segment 4 (§4) :

Je ne suis pas en Banque Populaire Val de France. (P4.1)

Je suis en informatique Banque Populaire I-BP c'est-à-dire qu'en fait informatique Banque Populaire c'est une plateforme commune pour toutes les banques populaires. (S4.1)

Donc, en fait, nous sommes un on va dire une forme de sous traitons de la banque populaire Val de France, on appelle INGIEU. (P4.2)

C'est-à-dire que toutes les banques populaires Val de France, d'épargnes etc. ont réunis leur moyen informatique dans une société qui s'appelle informatique banque populaire. (S4.2)

Et donc pourquoi, je travaille en Informatique Banque Populaire, parce que je dirai c'est l'une des principales entités informatiques du groupe BPCE donc qui ressemble au banque populaire et caisse d'épargne en France. (S4.3 et P4.3)

Codage du Segment 5 (§5) :

Oui. J'ai déjà travaillé dans… avant de rejoindre le groupe, j'avais travaillé pour la cité générale, la banque postale, le crédit agricole, un petit peu pour le crédit lui-même. (S5.1)

Je connais la plupart des grandes banques françaises. (P5.1)

Codage du Segment 6 (§6) :

Euuuuuuuuuhhh, je dirais aujourd'hui plutôt mon expérience d'après. (P6.1)

Même, si les deux se complètent, les deux se complètent. (P6.2)

Mais, c'est d'avantage mon expérience depuis que je suis rentré dans le groupe. (P6.3)

Codage du Segment 7 (§7) :

Déjà, parce qu'il faut faire quelque chose de sa vie, aussi il faut gagner de l'argent, et aussi parce que parce que je trouve un certain plaisir, un certain intérêt. (P7.1)

Codage du Segment 8 (§8) :

Combien y-a-t-il de départements dans l'entreprise ? Euuhhhhhhhhhh, je ne sais pas le compte, mais je dirai qu'on a cinq grandes directions, euh dans notre entreprise. (P8.1)

Codage du Segment 9 (§9) :

Alors, donc, moi je suis le directeur de l'audit interne. (S9.1)

Donc, mon rôle il est défini par la règlementation française qui est d'assurer le contrôle périodique de mon établissement et du système d'information que nous mettons en œuvre pour les banques. (S9.2)

Donc, c'est-à-dire que je dois réaliser à travers des missions d'audits, une couverture de tous les périmètres pour fournir à mon conseil d'administration une assurance comment dire raisonnable sur la maitrise des risques au sein de l'entreprise. (S9.3 et P9.1)

Codage du Segment 10 (§10) :

Donc, j'ai commencé par être développeur, puis chef de projet, puis directeur de projet pour les applications bancaires. (S10.1)

Puis j'ai fait l'inspection générale du groupe qui est en fait une forme de super audit. (P10.1)

Donc, après l'inspection générale, j'ai rejoint ce poste. (S10.2)

Codage du Segment 11 (§11) :

De la rigueur. (P11.1)

Il faut beaucoup de rigueur. (P11.2)

Il faut beaucoup de diplomatie. (P11.3)

Il faut des bonnes compétences de restitution à l'orale et à l'écrit. (P11.4)

Et un certain nombre de compétence technique sur les systèmes d'information. (P11.5)

Codage du Segment 12 (§12) :

Déjà il faut savoir convaincre, convaincre des comment dire des auditoires exigeants puisque nous reportons devant le conseil d'administration. (P12.1)

Et il faut donc savoir devant le conseil à la fois être fermer avec l'entreprise mais aussi faire en sorte que quand nous délibérons des messages de sein de vocations destructives qui ne bloquent pas les gens. (P12.2)

Et pareils, au cours de nos travaux, nous devons travailler avec… avec…avec nos audités, et il faut savoir voilà avoir un discours adapté c'est-à-dire pour montrer qu'effectivement nous ne sommes pas là pour les juger, mais pour évaluer pour évaluer une situation, évaluer des risques. (S12.1 et P12.3)

Donc, il faut être très prudent parce que sinon on peut avoir des braquages, de même que quand on redonne nos messages, des messages qui ne sont pas de très haut niveau, qui peuvent surmonter à la commission bancaire. (S12.2 et P12.4)

Donc il faut être très comment très… savoir extrêmement mesurer nos propos. (P12.5)

Codage du Segment 13 (§13) :

Avec les réseaux métiers. (S13.1)

Euuuuuhhhhhhhhhh, alors, au réseau métier. (S13.2)

On n'a pas de lien direct. (S13.3)

C'est-à-dire on passe, puisque nous nous battons souvent soit par le contrôle de deuxième niveau c'est-a-dire les responsables de sécurité des systèmes d'informations soit par les directeurs d'audit dédiés dans les banques directement c'est-à-dire comme vous savez Monsieur « COUILLET » à la BPVF. (S13.4 et A13.1)

Après, si le besoin exige, nous pouvons allez voir directement les utilisateurs mais ce n'est pas le cas le plus courant. (P13.1)

Codage du Segment 14 (§14) :

Je pense que c'est un sujet qui est aujourd'hui, c'est Euuuuuhhhhhhhhhh un sujet qui est très Euuuuuhhhhhhhhhh, comment dire c'est un sujet à la mode, mais ce n'est pas le contient, mais c'est plus qui est vraiment au-devant de la scène en termes d'informatique dans le monde bancaire. (P14.1)

C'est-à-dire qu'aujourd'hui dans le monde bancaire, un système d'information il y doit y avoir deux grosses contraintes : Il doit respecter la règlementation et il doit s'assurer de la sécurité des données qui véhiculent. (P14.2)

Et ceci pour plusieurs raisons. (P14.3)

Pour une raison déjà que notre métier bâtit sur la confiance de nos clients, donc, si, Euuuuuuuuuhhh, c'est effectivement nous n'assurons pas la sécurité des données, nous perdrons cette confiance. (P14.4)

En plus, le régulateur nous impose de plus en plus des exigences en termes de cyber sécurité, l'un des derniers en date, c'est le RGPD qui impose une sécurité By Design dans tous nos développements. (P14.5 et A14.1)

Aujourd'hui, c'est un thème qui est extrêmement centrale et qui aussi je dirai, je ne veux pas dire qui gêne, qui est vraiment primordiale, parce que la menace est extrêmement forte. (P14.6)

Et on a régulièrement la preuve de cette menace. (S14.1)

Ce qui était avant, des intentes de cyber sécurité, des choses très occasionnelles, aujourd'hui ce n'est pas le cas du quotidien. (S14.2)

En particulier, quand on regarde les aspects phishing ou des attaques même de Needle, comme on a eu il n'y a pas très longtemps. (S14.3)

Codage du Segment 15 (§15) :

Ce n'est pas hors de mon travail. (P15.1)

Par contre, je ne commente pas les missions à l'extérieur. (P15.2)

C'est confidentiel. (P15.3)

Euuuuuuuuuhhh, je peux vous dire qu'aujourd'hui, lorsqu'on fait une mission de cyber sécurité on s'intéresse à toute la chaine, à toute la chaine, comment de l'application, c'est-à-dire qu'on va à la fois regarder l'application intrinsèquement, à partir de comme elle était conçue, comment on a abordé la sécurité dans les modes de développements. (S15.1)

On regardera les aspects de la production informatique pour voir effectivement est-ce que les éléments nécessaires à la cybersécurité se mettent en place. (S15.2)

On utilisera des ressources spécialisées pour faire des Pen testes, des tests d'intrusion pour vérifier la résistance des applications. (S15.3)

Donc, je ne peux pas rentrer plus dans les détails d'une mission de cyber sécurité. (P15.4)

Codage du Segment 16 (§16) :

L'une des difficultés, c'est en ce qui concerne les Pen testes, c'est de ne pas casser les choses, puisqu'il faut être très **très** prudent puisque nous agissons sur une fraude qui fonctionne en permanence. (P16.1)

Donc, il faut faire extrêmement prudent pour ne pas bien que des simulations d'attaques vraiment abimés les choses. (P16.2)

En particulier, si on veut tester par exemple une résistance à une attaque de type déni de service. (P16.3)

Il faut bien être très **très** prudent pour ne pas effectivement couper le service. (P16.4)

Donc, voilà, c'est un point qui est très **très** **très** important et qui faille pour faire souvent ce type d'audit. (P16.5)

On fait appel à des prestations externes. (A16.1)

Il faut être extrêmement prudent avec ces prestataires qu'on va engager parce qu'il faut qu'ils soient certifiés également dans un nombre d'agences en France, permet de savoir quel sont les prestataires qui sont recommandés par la défense de France. (A16.2)

Mais, il faut être très **très** prudent, et bien sûr il faut être très **très** prudent sur la confidentialité de notre audit, puisque les résultats de notre audit pourraient être une bonne source d'inspiration pour les gens qui voudrait réalisés les attaques. (P16.6)

Codage du Segment 17 (§17) :

Alors, dans la banque, nous nous avons dans chaque établissement, un RSSI, un responsable de la sécurité des systèmes d'information. (S17.1)

Normalement, c'est lui qui est responsable de maintenir la cyber sécurité dans la banque. (S17.2)

C'est Didier G. pour la BPVF. (A17.1)

Et nous nous en avons un ici qui s'appelle Eric Didier qui est celui pour IBP, et il y a plusieurs gestions dans la banque et dans le groupe. (A17.2)

Mais voilà, dans le groupe, nous avons un réseau de RSSI, on en a un en établissement bancaire, un au niveau du groupe, un par centre d'informatique. (S17.2)

Donc, tout simple, et je dirai au niveau du groupe c'est Nathalie Salama qui est la responsable de la sécurité au niveau du groupe. (A17.3)

Codage du Segment 18 (§18) :

Alors, nous nous avons des cursus internes sur lesquels nous avons effectivement un contrôle de suivi pour s'assurer que les collaborateurs l'on bien fait. (S18.1)

Et, si les collaborateurs ne suivent pas leur formation cyber sécurité, ils sont appelés à l'ordre, et de nature, et également appelé à l'ordre pour s'assurer qu'ils le font bien. (S18.2)

On a mis aussi en place, des fausses campagnes pour sensibiliser les collaborateurs au danger de l'ingénierie sociale ou du phishing. (S18.3)

Typiquement, on fait chaque année, une campagne une ou deux campagnes fausses campagnes de phishing pour rappelés les gens qu'il ne faut pas cliquer sur n'importe quoi quand ils reçoivent des mails. (S18.4)

Codage du Segment 19 (§19) :

Oui. Ils sont très sensibles sur ce sujet. (P19.1)

Ils ont fait beaucoup durant ces dernières années de sensibilisation. (P19.2)

Et aujourd'hui, le sujet est vraiment au cœur des préoccupations et il n'y a pas un directeur général de banque qui ne soit pas directement impliqué. (P19.3)

Typiquement, la BPVF, Monsieur Carpentier, j'ai beaucoup travaillé avec lui, parce que c'est un sujet qui juge extrêmement sensible. (A19.1 et P19.4)

Codage du Segment 20 (§20) :

Et bien, nous de toute façon notre rôle a effectivement été de mener des missions d'audit donc de tester la sécurité des différentes composantes du système d'information. (S20.1)

Et à partir de là, les conclusions que nous faisons sont à la fois remontées dans les conseils d'administration de n'importe quel sort. (S20.2 et A20.1)

Mais, ils sont aussi transmis aux régulateurs qui en France, donc et, l'ACPR qui est une institution qui dépend de la banque centrale Européenne. (S20.3 et A20.2)

Donc, ce sujet-là, voilà, au travers de nos missions, nous invitons des recommandations qui en général sont bien suivies, et des recommandations de cyber sécurité qui sont souvent celles les plus priorisés. (S20.4 et P20.1)

Codage du Segment 21 (§21) :

Oui, un minimum une fois par an, un minimum une fois par an. (S21.1)

Codage du Segment 22 (§22) :

Nous nous faisons nos missions d'audit. (S22.1)

A partir des missions, nous établissons des recommandations justement quand nous anticipons une faille de sécurité, nous en donnons une recommandation. (S22.2)

Par rapport à cette faille, en disant qu'il faut combler la faille, ça faites une procédure de sécurité, ça faite une procédure pour intégrer les projets informatiques qui sont défaillantes. (S22.3)

Et donc nous après nous réalisons un suivi de la mise en œuvre et un contrôle de la mise en œuvre sur preuve et si les choses ne sont pas mises en œuvre, il y a un reporting qui part à la direction générale. (S22.4 et A22.1)

Donc, c'est ainsi que nous travaillons. (S22.5)

Codage du Segment 23 (§23) :

Non, ce n'est pas le rôle de l'audit. (P23.1)

Ce n'est pas le rôle de l'audit. (P23.2)

L'audit n'a pas une vocation à être actif. (P23.3)

C’est-à-dire nous nous sommes une fonction de contrôle et c’est légal parce que si on était à la fois responsable de la mise en œuvre des auditeurs, on aurait une confusion des genres et on s’est jugé partie. (P23.4 et S23.1)
Donc, nous nous regardons, nous analysons, nous émettons des recommandations. (S23.2)
Mais, par contre, nous ne sommes jamais chargés de la mise en œuvre et quand on donne une recommandation, nous définissons toujours le Quoi mais pas le Comment on va le traiter, c’est-à-dire qu’il faut avoir un système qui empêche les intrusions mais on ne dit pas quels types de systèmes ou quels types de logiciels, parce que justement nous devons surtout rester neutre et ne pas nous retrouver juger partie. (S23.3 et P23.5)

Codage du Segment 24 (§24) :

Alors, Euhhhhhhhhhhhhhhhhhh, il y a plusieurs raisons. (P24.1)
Déjà il y a une raison règlementaire qui est obligatoire. (P24.2)
La règlementation française oblige les banques à avoir un audit interne. (S24.1)
Ça c’est déjà une première réponse qui est assez forte. (P24.3)
La deuxième réponse c’est qu’un audit interne peut s’inscrire dans la durée et avoir un suivi des plans d’action à long terme. (S24.2)
Ce qui ne pourra pas extrêmement offrir à un auditeur externe. (P24.4)
Donc, c’est un point important. (P24.5)
Et trois, un audit interne est effectivement, je dirai en capacité à mieux comprendre les enjeux d’entreprises et apprécier aussi je dirai les prises du risque et les acceptations du risque. (P24.6)
Parce que je dirai dans une entreprise, si on doit faire de la sécurité, on risque de ne faire que ça, et alors, dans certaines branches, ça peut devenir nécessaire. (P24.7)
Mais, dans la banque, l’audit de la banque, c’est d’abord au cœur du business. (P24.8)
Il faut avoir cette juste vision entre le cœur du business et la sécurité. (P24.9)
Et donc, voilà l’audit interne est donc plus important que l’audit externe. (P24.10)

Codage du Segment 25 (§25) :

Oui, Oui, nous avons des relations régulières. (S25.1)

Alors, je dirai, l’audit a toujours était perçu comme, je ne sais pas comment expliquer ça, il y a une forme de crainte, comme quand on va allez vérifier des sociétés d’inquisition dans l’église catholique, si je peux dire, mais on exagère un peu. (P25.1)

Mais, aujourd’hui, l’image de l’audit a un peu quand même évolué dans le sens ou les gens comprennent les menaces qui arrivent. (P25.2)

Puisque sur la cybersécurité, tout le monde est sensibilisé aux menaces et donc aujourd’hui notre rôle est beaucoup mieux accepté. (P25.3)

Donc, même si quelque part, les gens n’aiment jamais voir l’audit arriver parce qu’ils savent que voilà, une manière ou d’une autre, quand même si ce n’est pas directe, juger leur travail est potentiellement leur adresser un travail supplémentaire pour corriger les erreurs que nous aurons identifiés. (P25.4 et S25.2)

Donc voilà. (P25.5)

Codage du Segment 26 (§26) :

Alors, déjà nous sommes rattachés au directeur général. (A26.1)

Nous avons aussi un accès au conseil d'administration pour le cas échéant. (A26.2)

Nous avons aussi comment dire une protection d'inspection général. (A26.3)

C'est-à-dire que par exemple un directeur de l'audit interne ne peut pas être évoqué sans l'accord de l'inspection générale du groupe. (A26.4)

Donc, ça nous donne une certaine indépendance. (P26.1)

Nous avons aussi des budgets en propre. (S26.1)

Donc, voilà, c'est les principes éléments. (S26.2)

Codage du Segment 27 (§27) :

Ce phénomène existe. (S27.1)

Mais, aujourd'hui, nous intégrons plus un processus de base de maitrise des risques de la sécurité et donc il y a moins ce phénomène de rejet même s'il y a toujours cette crainte qui existe. (S27.2 et P27.1)

Codage du Segment 28 (§28) :

Oui. (P28.1)

Les normes internationales sur l'audit imposent que tout auditeur est au moins cinq jours de formation par an. (S28.1)

Et aujourd'hui, nos formations se font dans le domaine de la sécurité. (S28.2)

Les attaques évoluent continuellement. (P28.2)

Codage du Segment 29 (§29) :

Un chef de mission doit savoir animer son équipe pour en tirer le mieux possible. (A29.1)

Il doit être aussi comme tout auditeur ou directeur d'audit très rigoureux parce que quelque part, il doit, je dirai qualifié le travail des autres, et il doit le faire de manière très **très** précise. (A29.2)

Donc il y a tout un code de déontologie qui a été défini par la profession et qui existe au niveau international et qui est en France produit par l'IFACI, et qui précise bien voilà indépendance, honnêteté. (S29.1)

Il y a tout un code déontologique qui existe pour le chef de mission, et donc le chef de mission qui se dons de tous ses qualités qui sont propres à tous les auditeurs doit être en mesure effectivement d'animer l'avance son équipe et de s'assurer que l'équipe est collectivement compétente pour réaliser sa mission. (A29.3)

Codage du Segment 30 (§30) :

Le phénomène de rejet de l'auditeur interne est un phénomène que j'allais dire, qui est un peu naturel à la base, puisque quelque part, on n'a pas tendance à aimer quand quelqu'un évalue votre travail surtout lorsqu'on sait que potentiellement l'audit amènera des recommandations qui diront que les choses ne vont pas. (P30.1)

Par contre, aujourd'hui, ce phénomène fait moins grille, parce que les gens ont aussi compris, que nous sommes dans un monde où il y a énormément de menace, en termes de cyber sécurité en particulier, et que l'audit est une fonction qui va aider à contrecarrer ces menaces. (P30.2)

Donc, il y a à la fois donc ce rejet parce que les gens naturellement n'aiment pas trop même voir ce qui font par contre il y a cette compréhension du fait qu'aujourd'hui effectivement l'audit est devenu nécessaire. (P30.3)

Codage du Segment 31 (§31) :

Oui, nous dans nos missions d'audit, nous faisons souvent appel à des expertises externes parce que de toute façon nous ne sommes pas polys compétents. (S31.1 et P31.1)

Nous faisons appel à des sociétés qui sont très **très** spécialisées dans la cybersécurité typiquement il y a des groupes comme Thales, ou comme Orange Sécurité. (P31.2 et A31.1)

Donc, voilà, nous faisons souvent appel à des spécialistes de la cybersécurité qui eux ont métier à plein temps de s'assurer des tests par contre ils sont encadrés par des auditeurs de chez nous. (S31.2)

Codage du Segment 32 (§32) :

Déjà c'est un peu le rôle du directeur général d'être garant de cette mise en œuvre. (A32.1)

Et lors de la faille, il y a des reporting qui sont faits au sein du conseil d'administration sur lequel nous indiquons comment les actions étaient mise en œuvre ou si elles prennent de retard dans leur mise en œuvre. (S32.1)

Et donc le directeur général est lui-même challengé par son conseil sachant que la loi aussi maintenant rend responsable des conseils d'administration si les choses n'étaient pas mis en œuvre. (A32.2)

Codage du Segment 33 (§33) :

Nous avons une bonne coordination avec effectivement les auditeurs externes c'est-à-dire que typiquement nous avons en particulier le commissaire au compte qui réalise les audits externes. (A33.1 et S33.1)

Nous avons comment dire les intentes règlementaires c'est-à-dire la BCE et l'ACP qui nous font des audits externes. (A33.2 et S33.2)

Nous avons parfois l'armée qui aussi vient demander des choses, puisqu'en certains cas il peut y avoir des aspects de sécurité nationale. (S33.3)

Donc, d'après l'audit interne, qui est en charge de la relation entre l'établissement et l'audit externe, et nous nous assurons effectivement : un de leurs fournir tous les éléments qui sont nécessaires à leur audit et nous assurons aussi qu'eux même lorsqu'ils émettent des recommandations, aussi ils sont bien pris en compte et il y aura un bien suivi régulier de leur avancement. (S33.4 et P33.1)

Codage du Segment 34 (§34) :

Un auditeur interne, donc, il doit y avoir les compétences comme un chef de mission. (A34.1)

Il doit être intègre, il doit avoir des bons aspects de communication orale et écrite, il doit avoir aussi une forme de diplomatie pour convaincre les audités. (A34.2)

Et après en termes de compétences techniques, je dirai, en faites, il ne faut pas, un auditeur ne peut pas être compétent dans tous les domaines. (A34.3)

Et le directeur de l'audit doit s'assurer que son équipe est compétente collectivement. (A34.4)

Certains sont plus compétents sur la sécurité, le grand système IBP, d'autres sont spécialisés dans tout ce qui est firewall, test d'intrusion. (A34.5)

Donc, voilà, ce qu'il faut c'est avoir des compétences, nous les auditeurs que nous cherchons souvent nous prenons plutôt des gens qui ont déjà travaillé dans le métier de l'informatique pendant quelques années qui sont dans un niveau comme un chef de projet et les formons à l'audit comme ça ils ont cette expérience informatique plus marquée. (A34.6 et S34.1)

Codage du Segment 35 (§35) :

Ils sont tout un petit peu inquiet, mais bon aujourd'hui, ça se passe un peu bien, mais il y a toujours une inquiétude, oui. (P35.1)

Codage du Segment 36 (§36) :

Nous sommes très objectives. (P36.1)

D'ailleurs tout ce que nous disons nous le basons sur des preuves. (S36.1)

Et ensuite, sauf dans des cas très **très très très** exceptionnel ou de malveillance, nous n'attaquons jamais les personnes mais les situations. (S36.2)

On ne dit pas que quelqu'un n'a pas fait son travail, on dit que le système n'est pas au point. (S36.3)

Donc nous ne mettons jamais en cause les gens à titre personnel. (S36.4)

1. Classement des unités codées : Recodage

E. Les séquences-types de l'entretien de P. CEZARD

Nous allons maintenant regrouper et ordonner les séquences dans l'ordre chronologique depuis le départ (S0) jusqu'à la fin de l'entretien (S+). Nous allons joindre toutes les unités concernées (tous les S) en leur donnant un titre résumant leur contenu.

Nous avons divisé l'entretien de Philipe en cinq séquences respectives selon l'ordre chronologique.

5. Niveau de formation et progression de la carrière

S0=S1.1+S1.2+S1.3+S2.1+S2.2+S4.1+S4.2+S4.3+S5.1+S9.1+S10.1+S10.2

6. Fonction de directeur d'Audit Interne : Rôle et missions

Sa=S9.2+S9.3+S12.1+S12.2+S13.1+S13.2+S13.4+S20.1+...+S20.4+S21.1+S22.1+...+S22.5+S23.1+S23.2+S23.3

7. Cybersécurité : contrainte et implication

Sb=S13.3+S14.1+S14.2+S14.3+S15.1+S15.2+S15.3+S17.1+S17.2+S18.1+S18.2+S18.3+S18.4

8. Obligation de l'audit interne et rôle en cybersécurité

Sc=S24.1+S24.2+S25.1+S27.2+S28.1+S28.2+S29.1+S31.1+S31.2+S32.1+S34.1+S36.1+S36.2+S36.3+S36.4

9. Relations de l'audit interne avec autres fonctions

SD=S25.2+S26.1+S26.2+S27.1+S33.1+S33.2+S33.3+S33.4

Nous allons maintenant proposer un premier résumé des séquences-types de l'entretien de Philipe Cezard après avoir effectué le regroupement selon un ordre chronologique.

Résumé des séquences-types de l'entretien de P. Cezard

Au début de l'entretien, P. Cezard nous annonce son parcours professionnel puis son insertion professionnelle dans la BPVF. Il a obtenu son diplôme en ingénieur en informatique à l'institut de Lyon, puis il a acquis plusieurs certifications en audit. Il a été promu dans plusieurs postes. Il a commencé comme développeur, puis chef de projet, puis directeur de projet pour les applications bancaires, puis dans l'inspection générale des banques populaires pour devenir directeur de l'audit dans l'I-BP.

Il explicite son rôle et ses missions comme directeur d'audit dans l'informatique banque populaire I-BP. Il assure le contrôle périodique du système d'information qu'il met en œuvre pour les banques. Il fournit aussi une assurance raisonnable au conseil d'administration sur la maitrise des risques.

Philipe explique qu'il est toujours en bataille avec le contrôle de deuxième niveau soit le directeur d'audit interne ou le responsable de sécurité informatique dans la BPVF au niveau d'interaction en sécurité informatique.

Il établit des recommandations justement quand il anticipe une faille de sécurité et ces recommandations de cybersécurité sont bien suivies. Philipe indique qu'il y un suivi de mise en œuvre et un reporting qui part à la direction générale si les recommandations ne sont pas suivies.

Il annonce qu'il y a le RSSI dans chaque banque qui fait partie du réseau de RSSI et qui est en charge d'assurer la cybersécurité. Il leur introduit des cursus internes et des contrôles de suivi qui doivent être aussi suivi.

Philipe réalise des campagnes pour sensibiliser les collaborateurs au danger des cyberattaques. Ce qui ne suive pas leur formation en cybersécurité sont appelé à l'ordre pour s'assurer qu'ils le font bien.

Dans les missions d'audit en cybersécurité, il justifie l'appel à des expertises externes pour s'assurer des tests et réaliser des simulations où l'audit interne est en surveillance sur ces experts. Il ajoute que les auditeurs internes embauchés ont un contexte en informatique.

Enfin, il admet d'avoir une bonne coordination avec les auditeurs externes en assurant qu'ils émettent des recommandations qui sont prises en compte et suivies

F. <u>Les acteurs du récit de P. Cezard</u>

Nous allons ici identifiés les personnages dans le récit de Philipe. Nous allons inclure Philipe lui-même lorsqu'il se dédouble (« moi, je…).

Nous notons respectivement les acteurs de A1 jusqu'à An.

Le premier actant du récit est Philipe lui-même puisqu'il a utilisé le « je » respectivement 18 fois et le « moi » 2 fois.

Le second actant est les régulateurs.

A2=A14.1+A20.2

Le troisième actant est les prestataires externes.

A3=A16.1+A16.2+A31.1

Le quatrième actant est le RSSI de la BPVF « Didier G. ».

A4=A17.1

Le cinquième actant est le RSSI de l'I-BP « Eric DIDIER ».

A5=A17.2

Le sixième actant est le responsable de sécurité au niveau du groupe « Nathalie SALAMA ».

A6=A17.3

Le septième actant est le conseil d'administration

A7=A20.1+A26.2

Le huitième actant est le directeur général

A8=A19.1+A22.1+A26.1+A32.1+A32.2

Le neuvième actant est l'inspection générale

A9=A26.3+A26.4

Le dixième actant est le chef de mission

A10=A29.1+A29.2+A29.3

L'onzième actant est l'auditeur interne

A11=A34.1+A34.2+A34.3+A34.4+A34.5+A34.6

Le douzième actant est l'auditeur externe

A12=A33.1+A33.2

<u>Les actants du récit de P. Cezard</u>

Le premier actant est P. Cezard lui-même. Nous analysons qu'il a fréquemment utilisé le « je » et le « moi » dans son récit pour donner son avis ou son opinion.

Le deuxième actant est les régulateurs. Ils imposent des exigences à l'audit interne en termes de cybersécurité par exemple une sécurité *by design* dans tous les développements. Ils reçoivent aussi de l'audit interne les conclusions des missions d'audit sur la cybersécurité.

Le troisième actant est les prestataires ou sociétés externes. Philipe explique que ces prestataires certifiés sont très spécialisés dans la cybersécurité par exemple comme *Thales* ou *Orange*. Ces prestataires sont des spécialistes de la cybersécurité qui ont métier à plein temps de s'assurer des tests et de réaliser de simulations et ils sont encadrés par des auditeurs internes.

Le quatrième actant est le RSSI de la BPVF « Didier G. ».

Le cinquième actant est le RSSI de l'I-BP « Eric DIDIER ».

Philipe annonce que c'est le RSSI qui est responsable d'assurer la cybersécurité dans la banque. Il explique que Didier G. est responsable d'assurer la cybersécurité dans la BPVF alors que c'est la responsabilité de Didier de l'assurer dans l'I-BP.

Le sixième actant est le responsable de sécurité du groupe « Nathalie SALAMA ».

Philipe ajoute qu'il existe au sein du groupe un réseau de RSSI dont Nathalie Salama est qualifiée responsable de la sécurité au niveau du groupe.

Le septième actant est le conseil d'administration. Philipe transmet les conclusions et les recommandations et annonce qu'il a un accès à n'importe quel temps au conseil d'administration pour conserver son indépendance.

Le huitième actant est le directeur général. Il y a un *functional reporting* entre le directeur d'audit et le directeur général. Philipe précise que le directeur général doit être garant de la mise en œuvre des constations d'audit et des mesures correctives. Il est lui-même challengé par son conseil si les choses n'étaient pas mis en œuvre.

Le neuvième actant est l'inspection générale. Philipe explique que l'inspection générale préserve l'indépendance et l'objectivité des auditeurs internes.

Le dixième actant est le chef de mission. Philipe décrit que le chef de mission doit savoir animer son équipe pour en tirer le mieux possible. Il le considère comme tout auditeur ou directeur d'audit qui doit être très rigoureux.

L'onzième actant est l'auditeur interne. Philipe exprime que les auditeurs internes doivent être intègres, avoir de bons aspects de communication orale et écrite et avoir une forme de diplomatie pour convaincre les audités. Ils ne peuvent pas être compétents dans tous les domaines. Mais ce qui est important c'est qu'ils aient des compétences en informatiques c'est-à-dire une expérience informatique plus marquée.

Le douzième actant est l'auditeur externe. Ils coordonnent avec les auditeurs internes et réalise l'audit externe en donnant aussi des recommandations pour améliorer le travail.

G. <u>Les classes d'arguments</u>

Ce niveau d'analyse concerne l'ensemble des arguments, démonstrations et propositions de P. Cezard destinés à nous convaincre. Nous allons regroupés l'ensemble des unités codées en P selon des « classes d'arguments » dont chacune représente une étape logique dans un raisonnement.

Nous allons classer les arguments le type de raisonnement que Philipe présente dans ces réponses. Nous en avons repéré six qui font l'objet d'arguments explicites qui sont à la base de ce classement.

Nous avons noté (P1) les propositions de Philipe associé à l'intégration et l'implication dans le secteur bancaire. Il a affirmé plusieurs fois que le secteur bancaire est un secteur intéressant qui lui plaisait. Il valorise aussi la I-BP en la

décrivant comme l'une des principales entités informatiques du groupe BPCE mais il a une faible connaissance du groupe et des départements existants.

- Euhhh, parce que je dirais que c'est un secteur qui a des moyens déjà, c'est un secteur qui est **intéressant**, puis voilà c'est un secteur qui me **plaisait** bien en super affinité. (P3.1)
- Je ne suis pas en Banque Populaire Val de France. (P4.1)
- Donc, en fait, nous sommes un on va dire une forme de sous traitons de la banque populaire Val de France, on appelle INGIEU. (P4.2)
- Et donc pourquoi, je travaille en Informatique Banque Populaire, parce que je dirai c'est l'une des principales entités informatiques du groupe BPCE donc qui ressemble au banque populaire et caisse d'épargne en France. (S4.3 et P4.3)
- Je connais la plupart des grandes banques françaises. (P5.1)
- Euuuuuuuuuhhh, je dirais aujourd'hui plutôt mon expérience d'après. (P6.1)
- Même, si les deux se complètent, les deux se complètent. (P6.2)
- Mais, c'est d'avantage mon expérience depuis que je suis rentré dans le groupe. (P6.3)
- Déjà, parce qu'il faut faire quelque chose de sa vie, aussi il faut gagner de l'argent, et aussi parce que parce que je trouve un certain plaisir, un certain intérêt. (P7.1)
- Combien y-a-t-il de départements dans l'entreprise ? Euuhhhhhhhhhh, je ne sais pas le compte, mais je dirai qu'on a cinq grandes directions, euh dans notre entreprise. (P8.1)

Nous résumons cet ensemble ainsi : *« L'intégration dans le secteur bancaire ».*
Nous avons noté (P2) les expressions de Philipe associés à son travail, ses qualités et missions en tant que directeur d'audit interne dans la banque I-BP.

- Donc, c'est-à-dire que je dois réaliser à travers des missions d'audits, une couverture de tous les périmètres pour fournir à mon conseil d'administration une **assurance** comment dire **raisonnable** sur la maitrise des risques au sein de l'entreprise. (S9.3 et P9.1)
- Puis j'ai fait l'inspection générale du groupe qui est en fait une forme de super audit. (P10.1)
- De la **rigueur**. (P11.1)
- Il faut beaucoup de **rigueur**. (P11.2)
- Il faut beaucoup de **diplomatie**. (P11.3)
- Il faut des bonnes compétences de restitution à l'orale et à l'écrit. (P11.4)
- Et un certain nombre de **compétence technique sur les systèmes d'information**. (P11.5)
- Déjà il faut savoir **convaincre**, **convaincre** des comment dire des auditoires exigeants puisque nous reportons devant le conseil d'administration. (P12.1)
- Et il faut donc savoir devant le conseil à la fois être fermer avec l'entreprise mais aussi faire en sorte que quand nous délibérons des messages de sein de vocations destructives qui ne bloquent pas les gens. (P12.2)
- Et pareils, au cours de nos travaux, nous **devons travailler avec**… avec…avec nos audités, et il faut savoir voilà avoir un discours adapté c'est-à-dire pour montrer qu'effectivement nous ne sommes pas là pour les juger, mais pour évaluer pour évaluer une situation, évaluer des risques. (S12.1 et P12.3)
- Donc, il faut être très prudent parce que sinon on peut avoir **des braquages**, de même que quand on redonne nos messages, des messages qui ne sont pas de très haut niveau, qui peuvent surmonter à la commission bancaire. (S12.2 et P12.4)

- Donc il faut être très comment très… savoir extrêmement mesurer nos propos. (P12.5)
- Après, si le besoin exige, nous pouvons allez voir directement les utilisateurs mais ce n'est pas le cas le plus courant. (P13.1)

Cet ensemble se résume ainsi : *« Compétences et exigences des auditeurs internes ».*
Nous avons noté (P3) les expressions de Philippe relatives à l'importance de la cybersécurité dans le secteur bancaire et son effet sur son travail.

- Je pense que c'est un sujet qui est aujourd'hui, c'est Euuuuuhhhhhhhhhh un sujet qui est très Euuuuuhhhhhhhhhh, comment dire c'est un sujet à la mode, mais ce n'est pas le contient, mais c'est plus qui est vraiment au-devant de la scène en termes d'informatique dans le monde bancaire. (P14.1)
- C'est-à-dire qu'aujourd'hui dans le monde bancaire, un système d'information il y doit y avoir deux **grosses contraintes** : Il doit respecter la règlementation et il doit s'assurer de la sécurité des données qui véhiculent. (P14.2)
- Et ceci pour plusieurs raisons. (P14.3)
- Pour une raison déjà que notre métier bâtit sur la **confiance de nos clients**, donc, si, Euuuuuuuuuhhh, c'est effectivement nous n'assurons pas la sécurité des données, nous perdrons cette confiance. (P14.4)
- En plus, le régulateur nous impose de plus en plus des exigences en termes de cyber sécurité, l'un des derniers en date, c'est le RGPD qui impose une sécurité By Design dans tous nos développements. (P14.5 et A14.1)
- Aujourd'hui, c'est un thème qui est extrêmement centrale et qui aussi je dirai, je ne veux pas dire qui **gêne**, qui est vraiment **primordiale**, parce que la menace est extrêmement forte. (P14.6)
- Ce n'est pas hors de mon travail. (P15.1)
- Par contre, je ne commente pas les missions à l'extérieur. (P15.2)
- C'est confidentiel. (P15.3)
- Donc, je ne peux pas rentrer plus dans les détails d'une mission de cyber sécurité. (P15.4)
- L'une des difficultés, c'est en ce qui concerne les Pen testes, c'est de ne pas casser les choses, puisqu'il faut être **très très prudent** puisque nous agissons sur une fraude qui fonctionne en permanence. (P16.1)
- Donc, il faut faire **extrêmement prudent** pour ne pas bien que des simulations d'attaques vraiment abimés les choses. (P16.2)
- En particulier, si on veut tester par exemple une résistance à une attaque de type déni le service. (P16.3)
- Il faut bien être **très très prudent** pour ne pas effectivement couper le service. (P16.4)
- Donc, voilà, c'est un point qui est **très très très important** et qui faille pour faire souvent ce type d'audit. (P16.5)
- Mais, il faut être **très très prudent**, et bien sûr il faut être **très très prudent** sur la confidentialité de notre audit, puisque les résultats de notre audit pourraient être une bonne source d'inspiration pour les gens qui voudrait réalisés les attaques. (P16.6)
- Oui. Ils sont très **sensibles** sur ce sujet. (P19.1)
- Ils ont fait beaucoup durant ces dernières années de sensibilisation. (P19.2)
- Et aujourd'hui, le sujet est vraiment au cœur des préoccupations et il n'y a pas un directeur général de banque qui ne soit pas directement impliqué. (P19.3)
- Typiquement, la BPVF, Monsieur Carpentier, j'ai beaucoup travaillé avec lui, parce que c'est un sujet qui juge extrêmement sensible. (A19.1 et P19.4)

- Donc, ce sujet-là, voilà, au travers de nos missions, nous invitons des recommandations qui en général sont bien suivies, et des recommandations de cyber sécurité qui sont souvent celles les plus priorisés. (S20.4 et P20.1)

Cet ensemble se résume ainsi : *« S'appuyer sur la prudence et la sensibilisation dans le domaine de cybersécurité doit être primordiale dans le secteur bancaire ».*

Nous avons noté (P4) les expressions et les formules relatives à l'audit interne dans le milieu de cybersécurité.

- Non, ce n'est pas le rôle de l'audit. (P23.1)
- Ce n'est pas le rôle de l'audit. (P23.2)
- L'audit n'a pas une vocation à être actif. (P23.3)
- C'est-à-dire nous nous sommes une fonction de contrôle et c'est légal parce que si on était à la fois responsable de la mise en œuvre des auditeurs, on aurait une confusion des genres et on s'est **jugé partie**. (P23.4 et S23.1)
- Donc, nous nous regardons, nous analysons, nous émettons des recommandations. (S23.2)
- Mais, par contre, nous ne sommes jamais chargés de la mise en œuvre et quand on donne une recommandation, nous définissons toujours le Quoi mais pas le Comment on va le traiter, c'est-à-dire qu'il faut avoir un système qui empêche les intrusions mais on ne dit pas quels types de systèmes ou quels types de logiciels, parce que justement nous devons surtout **rester neutre** et ne pas nous **retrouver juger partie**. (S23.3 et P23.5)
- Alors, Euhhhhhhhhhhhhhhhhhh, il y a plusieurs raisons. (P24.1)
- Déjà il y a une raison règlementaire qui est obligatoire. (P24.2)
- Ça c'est déjà une première réponse qui est assez forte. (P24.3)
- Ce qui ne pourra pas extrêmement offrir à un auditeur externe. (P24.4)
- Donc, c'est un point important. (P24.5)
- Et trois, un audit interne est effectivement, je dirai en capacité à mieux comprendre les enjeux d'entreprises et apprécier aussi je dirai les prises du risque et les acceptations du risque. (P24.6)
- Parce que je dirai dans une entreprise, si on doit faire de la sécurité, on risque de ne faire que ça, et alors, dans certaines branches, ça peut devenir nécessaire. (P24.7)
- Mais, dans la banque, l'audit de la banque, c'est d'abord au cœur du business. (P24.8)
- Il faut avoir cette juste vision entre le cœur du business et la sécurité. (P24.9)
- Et donc, voilà l'audit interne est donc plus important que l'audit externe. (P24.10)
- Nous sommes très **objectives**. (P36.1)

Cet ensemble se résume ainsi : *« L'objectivité de l'auditeur interne limite son implication dans la cybersécurité. L'auditeur donne des recommandations et ne s'intéresse pas à la mise en œuvre de la cybersécurité ».*

Nous avons noté (P5) les expressions et les formules associés à l'identité professionnelles des auditeurs internes :

- Alors, je dirai, l'audit a toujours était perçu comme, je ne sais pas comment expliquer ça, il y a **une forme de crainte**, comme quand on va allez vérifier des sociétés d'inquisition dans l'église catholique, si je peux dire, mais on exagère un peu. (P25.1)
- Mais, aujourd'hui, l'image de l'audit a un peu quand même évolué dans le sens ou les gens comprennent les menaces qui arrivent. (P25.2)

- Puisque sur la cybersécurité, tout le monde est sensibilisé aux menaces et donc aujourd'hui notre **rôle** est beaucoup mieux accepté. (P25.3)
- Donc, même si quelque part, les gens n'aiment jamais voir l'audit arriver parce qu'ils savent que voilà, une manière ou d'une autre, quand même si ce n'est pas directe, juger leur travail est potentiellement leur adresser un travail supplémentaire pour corriger les erreurs que nous aurons identifiés. (P25.4 et S25.2)
- Donc voilà. (P25.5)
- Donc, ça nous donne une certaine **indépendance**. (P26.1)
- Mais, aujourd'hui, nous intégrons plus un processus de base de maitrise des risques de la sécurité et donc il y a moins ce phénomène de rejet même s'il y a toujours cette crainte qui existe. (S27.2 et P27.1)
- Oui. (P28.1)
- Les attaques évoluent continuellement. (P28.2)
- Le phénomène de **rejet** de l'auditeur interne est un phénomène que j'allais dire, qui est un peu naturel à la base, puisque quelque part, on n'a pas tendance à aimer quand quelqu'un évalue votre travail surtout lorsqu'on sait que potentiellement l'audit amènera des recommandations qui diront que les choses ne vont pas. (P30.1)
- Par contre, aujourd'hui, ce phénomène fait moins grille, parce que les gens ont aussi compris, que nous sommes dans un monde où il y a énormément de menace, en termes de cyber sécurité en particulier, et que l'audit est une fonction qui va aider à contrecarrer ces menaces. (P30.2)
- Donc, il y a à la fois donc ce **rejet** parce que les gens naturellement n'aiment pas trop même voir ce qui font par contre il y a cette compréhension du fait qu'aujourd'hui effectivement l'audit est devenu nécessaire. (P30.3)
- Donc, d'après l'audit interne, qui est en charge de la relation entre l'établissement et l'audit externe, et nous nous assurons effectivement : un de leurs fournir tous les éléments qui sont nécessaires à leur audit et nous assurons aussi qu'eux même lorsqu'ils émettent des recommandations, aussi ils sont bien pris en compte et il y aura un bien suivi régulier de leur avancement. (S33.4 et P33.1)
- Ils sont tout un petit peu inquiet, mais bon aujourd'hui, ça se passe un peu bien, mais il y a toujours une inquiétude, oui. (P35.1)

Cet ensemble se résume ainsi : *« L'auditeur interne est souvent rejeté par les audités par sentiment de crainte et de peur. Ils commencent à être un peu plus accepté dans le domaine de cybersécurité puisque c'est une responsabilité globale »*.

Nous avons noté (P6) le manque de spécialisation des auditeurs internes en cybersécurité selon Philipe :

- Oui, nous dans nos missions d'audit, nous faisons souvent appel à des expertises externes parce que de toute façon nous ne sommes pas **polys compétents**. (S31.1 et P31.1)
- Nous faisons appel à des sociétés qui sont **très très spécialisées** dans la cybersécurité typiquement il y a des groupes comme Thales, ou comme Orange Sécurité. (P31.2 et A31.1)

Cet ensemble se résume ainsi : *« Les auditeurs internes ont besoin de renforcement sur l'aspect de cybersécurité puisqu'ils ont un manque de compétence technique dans ce domaine. Ils ont recours à des expertises externes qui sont certifiés et légitimes en France »*.

H. Le schème provisoire de l'entretien

Nous allons tout d'abord restituer le schème en situant les arguments dans leur ordre d'intervention dans le récit et en les mettant en relation « spatiale » avec les deux autres classes d'unités précédemment recodées : les séquences et les actants. Nous allons les présenter dans ce tableau qui constituera un schème provisoire de l'entretien.

Séquences (Sn)	Arguments (Pn)	Actant (An)
Niveau de formation et progression de la carrière (S_0)	• Donc, moi je suis à l'origine, je suis ingénieur, précisément ingénieur à l'institut de Lyon en Informatique. (S1.1) • Euhhhh, Bon Après, j'ai fait une étude en 3ième cycle en gestion complété ça et puis depuis j'ai fait pas mal de formation continu dans le cadre de mission. (S1.2) • En particulier, je suis certifié donc sésame et sillac, sont deux certifications d'audit interne international, et je suis aussi… (S1.3) • Alors, je suis rentré en inspection générale des banques populaires. (S2.1) • Donc répondant à une annonce, et donc après un parcours de quelques années en inspection, j'ai créé d'audit interne pour la structure informatique banque populaire. (S2.2) • Populaire c'est une plateforme commune pour toutes les banques populaires. (S4.1) • C'est-à-dire que toutes les banques populaires Val de France, d'épargnes etc. ont réunis leur moyen informatique dans une société qui s'appelle informatique banque populaire. (S4.2) • Oui. J'ai déjà travaillé dans… avant de rejoindre le groupe, j'avais travaillé pour la cité générale, la banque postale, le crédit agricole, un petit peu pour le crédit lui-même. (S5.1) • Alors, donc, moi je suis le directeur de l'audit interne. (S9.1) • Donc, j'ai commencé par être développeur, puis chef de projet, puis directeur de projet pour les applications bancaires. (S10.1) • Donc, après l'inspection générale, j'ai rejoint ce poste. (S10.2)	• Euhhh, parce que je dirais que c'est un secteur qui a des moyens déjà, c'est un secteur qui est intéressant, puis voilà c'est un secteur qui me plaisait bien en super affinité. (P3.1) • Je ne suis pas en Banque Populaire Val de France. (P4.1) • Donc, en fait, nous sommes un on va dire une forme de sous traitons de la banque populaire Val de France, on appelle INGIEU. (P4.2) • Et donc pourquoi, je travaille en Informatique Banque Populaire, parce que je dirai c'est l'une des principales entités informatiques du groupe BPCE donc qui ressemble au banque populaire et caisse d'épargne en France. (S4.3 et P4.3) • Je connais la plupart des grandes banques françaises. (P5.1) • Euuuuuuuuuhhh, je dirais aujourd'hui plutôt mon expérience d'après. (P6.1) • Même, si les deux se complètent, les deux se complètent. (P6.2) • Mais, c'est d'avantage mon expérience depuis que je suis rentré dans le groupe. (P6.3) • Déjà, parce qu'il faut faire quelque chose de sa vie, aussi il faut gagner de l'argent, et aussi parce que parce que je trouve un certain plaisir, un certain intérêt. (P7.1) • Combien y-a-t-il de départements dans l'entreprise ? Euuuuuhhhhhhhhhh, je ne sais pas le compte, mais je dirai qu'on a cinq grandes directions, euh dans notre entreprise. (P8.1)	Le « Moi » et le « Je » qui réfère à Monsieur Philipe lui-même.
Fonction de directeur d'Audit : Rôle et missions (Sa)	• Donc, mon rôle il est défini par la règlementation française qui est d'assurer le contrôle périodique de mon établissement et du système d'information que nous mettons en œuvre pour les banques. (S9.2) • Donc, c'est-à-dire que je dois réaliser à travers des missions d'audits, une couverture de tous les périmètres pour fournir à mon conseil d'administration une assurance comment dire raisonnable sur la maitrise des risques au sein de l'entreprise. (S9.3 et P9.1) • Et pareils, au cours de nos travaux, nous devons travailler avec… avec…avec nos audités, et il faut savoir voilà avoir un discours adapté c'est-à-dire pour montrer qu'effectivement nous ne sommes pas là pour les juger, mais pour évaluer pour évaluer une situation, évaluer des risques. (S12.1 et P12.3) • Avec les réseaux métiers. (S13.1) • Euuuuuhhhhhhhhhh, alors, au réseau métier. (S13.2)	• Puis j'ai fait l'inspection générale du groupe qui est en fait une forme de super audit. (P10.1) • De la rigueur. (P11.1) • Il faut beaucoup de rigueur. (P11.2) • Il faut beaucoup de diplomatie. (P11.3) • Il faut des bonnes compétences de restitution à l'orale et à l'écrit. (P11.4) • Et un certain nombre de compétence technique sur les systèmes d'information. (P11.5) • Déjà il faut savoir convaincre, convaincre des comment dire des auditoires exigeants puisque nous reportons devant le conseil d'administration. (P12.1) • Et il faut donc savoir devant le conseil à la fois être fermer avec l'entreprise mais aussi faire en sorte que quand nous délibérons des messages de sein de vocations destructives qui ne bloquent pas les gens. (P12.2)	C'est-à-dire on passe, puisque nous nous battons souvent soit par le contrôle de deuxième niveau c'est-a-dire les responsables de sécurité des systèmes d'informations soit par les directeurs d'audit dédiés dans les banques directement c'est-à-dire comme vous savez Monsieur « COUILLET » à la BPVF. (S13.4 et A13.1)

	• Eh bien, nous de toute façon notre rôle a effectivement été de mener des missions d'audit donc de tester la sécurité des différentes composantes du système d'information. (S20.1) • Oui, un minimum une fois par an, un minimum une fois par an. (S21.1) • Nous nous faisons nos missions d'audit. (S22.1) • A partir des missions, nous établissons des recommandations justement quand nous anticipons une faille de sécurité, nous en donnons une recommandation. (S22.2) • Par rapport à cette faille, en disant qu'il faut combler la faille, ça faites une procédure de sécurité, ca faite une procédure pour intégrer les projets informatiques qui sont défaillantes. (S22.3) • Donc, c'est ainsi que nous travaillons. (S22.5) • Donc, nous nous regardons, nous analysons, nous émettons des recommandations. (S23.2) • Donc, il faut être très prudent parce que sinon on peut avoir des braquages, de même que quand on redonne nos messages, des messages qui ne sont pas de très haut niveau, qui peuvent surmonter à la commission bancaire. (S12.2 et P12.4)	• Donc il faut être très comment très… savoir extrêmement mesurer nos propos. (P12.5) • Après, si le besoin exige, nous pouvons allez voir directement les utilisateurs mais ce n'est pas le cas le plus courant. (P13.1)	Et à partir de là, les conclusions que nous faisons sont à la fois remontées dans les conseils d'administration de n'importe quel sort. (S20.2 et A20.1) Mais, ils sont aussi transmis aux régulateurs qui en France, donc et, l'ACPR qui est une institution qui dépend de la banque centrale Européenne. (S20.3 et A20.2) Et donc nous après nous réalisons un suivi de la mise en œuvre et un contrôle de la mise en œuvre sur preuve et si les choses ne sont pas mises en œuvre, il y a un reporting qui part à la direction générale. (S22.4 et A22.1)
Cybersécurité : Contrainte et implication (Sb)	• On n'a pas de lien direct. (S13.3) • Et on a régulièrement la preuve de cette menace. (S14.1) • Ce qui était avant, des intentes de cyber sécurité, des choses très occasionnelles, aujourd'hui ce n'est pas le cas du quotidien. (S14.2) • En particulier, quand on regarde les aspects phishing ou des attaques même de Needle, comme on a eu il n'y a pas très longtemps. (S14.3) • Euuuuuuuuuhhh, je peux vous dire qu'aujourd'hui, lorsqu'on fait une mission de cyber sécurité on s'intéresse à toute la chaine, à toute la chaine, comment de l'application, c'est-à-dire qu'on va à la fois regarder l'application intrinsèquement, à partir de comme elle était conçue, comment on a abordé la sécurité dans les modes de développements. (S15.1) • On regardera les aspects de la production informatique pour voir effectivement est-ce que les éléments nécessaires à la cybersécurité se mettent en place. (S15.2) • On utilisera des ressources spécialisées pour faire des pen testes, des tests d'intrusion pour vérifier la résistance des applications. (S15.3) • Alors, dans la banque, nous nous avons dans chaque établissement, un RSSI, un responsable de la sécurité des systèmes d'information. (S17.1) • Mais voilà, dans le groupe, nous avons un réseau de RSSI, on en a un en établissement bancaire, un au niveau du groupe, un par centre d'informatique. (S17.2)	• Je pense que c'est un sujet qui est aujourd'hui, c'est Euuuuuhhhhhhhhhh un sujet qui est très Euuuuuhhhhhhhhhh, comment dire c'est un sujet à la mode, mais ce n'est pas le contient, mais c'est plus qui est vraiment au-devant de la scène en terme d'informatique dans le monde bancaire. (P14.1) • C'est-à-dire qu'aujourd'hui dans le monde bancaire, un système d'information il y doit y avoir deux grosses contraintes : Il doit respecter la règlementation et il doit s'assurer de la sécurité des données qui véhiculent. (P14.2) • Et ceci pour plusieurs raisons. (P14.3) • Pour une raison déjà que notre métier bâtit sur la confiance de nos clients, donc, si, Euuuuuuuuuhhh, c'est effectivement nous n'assurons pas la sécurité des données, nous perdrons cette confiance. (P14.4) • Aujourd'hui, c'est un thème qui est extrêmement centrale et qui aussi je dirai, je ne veux pas dire qui gêne, qui est vraiment primordiale, parce que la menace est extrêmement forte. (P14.6) • Ce n'est pas hors de mon travail. (P15.1) • Par contre, je ne commente pas les missions à l'extérieur. (P15.2) • C'est confidentiel. (P15.3) • Donc, je ne peux pas rentrer plus dans les détails d'une mission de cyber sécurité. (P15.4) • L'une des difficultés, c'est en ce qui concerne les pen testes, c'est de ne pas casser les choses, puisqu'il faut être très très prudent puisque nous agissons sur une fraude qui fonctionne en permanence. (P16.1)	En plus, le régulateur nous impose de plus en plus des exigences en termes de cyber sécurité, l'un des derniers en date, c'est le RGPD qui impose une sécurité By Design dans tous nos développements. (P14.5 et A14.1) Typiquement, la BPVF, Monsieur Carpentier, j'ai beaucoup travaillé avec lui, parce que c'est un sujet qui juge extrêmement sensible. (A19.1 et P19.4)

	• Alors, nous nous avons des cursus internes sur lesquels nous avons effectivement un contrôle de suivi pour s'assurer que les collaborateurs l'on bien fait. (S18.1) • Et, si les collaborateurs ne suivent pas leur formation cyber sécurité, ils sont appelés à l'ordre, et de nature, et également appelé à l'ordre pour s'assurer qu'ils le font bien. (S18.2) • On a mis aussi en place, des fausses campagnes pour sensibiliser les collaborateurs au danger de l'ingénierie sociale ou du phishing. (S18.3) • Typiquement, on fait chaque année, une campagne une ou deux campagnes fausses campagnes de phishing pour rappelés les gens qu'il ne faut pas cliquer sur n'importe quoi quand ils reçoivent des mails. (S18.4) • Donc, ce sujet-là, voilà, au travers de nos missions, nous invitons des recommandations qui en général sont bien suivies, et des recommandations de cyber sécurité qui sont souvent celles les plus priorisés. (S20.4 et P20.1)	• Donc, il faut faire extrêmement prudent pour ne pas bien que des simulations d'attaques vraiment abimés les choses. (P16.2) • En particulier, si on veut tester par exemple une résistance à une attaque de type déni de service. (P16.3) • Il faut bien être très très prudent pour ne pas effectivement couper le service. (P16.4) • Donc, voilà, c'est un point qui est très très très important et qui faille pour faire souvent ce type d'audit. (P16.5) • Mais, il faut être très très prudent, et bien sûr il faut être très très prudent sur la confidentialité de notre audit, puisque les résultats de notre audit pourraient être une bonne source d'inspiration pour les gens qui voudrait réalisés les attaques. (P16.6) • Oui. Ils sont très sensibles sur ce sujet. (P19.1) • Ils ont fait beaucoup durant ces dernières années de sensibilisation. (P19.2) • Et aujourd'hui, le sujet est vraiment au cœur des préoccupations et il n'y a pas un directeur général de banque qui ne soit pas directement impliqué. (P19.3)
Obligation de l'audit interne et rôle en cybersécurité (Sc)	• La règlementation française oblige les banques à avoir un audit interne. (S24.1) • La deuxième réponse c'est qu'un audit interne peut s'inscrire dans la durée et avoir un suivi des plans d'action à long terme. (S24.2) • Oui, Oui, nous avons des relations régulières. (S25.1) • Les normes internationales sur l'audit imposent que tout auditeur est au moins cinq jours de formation par an. (S28.1) • Et aujourd'hui, nos formations se font dans le domaine de la sécurité. (S28.2) • Donc il y a tout un code de déontologie qui a été défini par la profession et qui existe au niveau international et qui est en France produit par l'IFACI, et qui précise bien voilà indépendance, honnêteté. (S29.1) • Donc, voilà, nous faisons souvent appel à des spécialistes de la cybersécurité qui eux ont métier à plein temps de s'assurer des tests par contre ils sont encadrés par des auditeurs de chez nous. (S31.2) • Et lors de la faille, il y a des reporting qui sont faits au sein du conseil d'administration sur lequel nous indiquons comment les actions étaient mise en œuvre ou si elles prennent de retard dans leur mise en œuvre. (S32.1) • D'ailleurs tout ce que nous disons nous le basons sur des preuves. (S36.1) • Et ensuite, sauf dans des cas très très très très exceptionnel ou de malveillance, nous n'attaquons jamais les personnes mais les situations. (S36.2) • On ne dit pas que quelqu'un n'a pas fait son travail, on dit que le système n'est pas au point. (S36.3) • Donc nous ne mettons jamais en cause les gens à titre personnel. (S36.4)	• Non, ce n'est pas le rôle de l'audit. (P23.1) • Ce n'est pas le rôle de l'audit. (P23.2) • L'audit n'a pas une vocation à être actif. (P23.3) • C'est-à-dire nous nous sommes une fonction de contrôle et c'est légal parce que si on était à la fois responsable de la mise en œuvre des auditeurs, on aurait une confusion des genres et on s'est jugé partie. (P23.4 et S23.1) • Donc, nous nous regardons, nous analysons, nous émettons des recommandations. (S23.2) • Mais, par contre, nous ne sommes jamais chargés de la mise en œuvre et quand on donne une recommandation, nous définissons toujours le Quoi mais pas le Comment on va le traiter, c'est-à-dire qu'il faut avoir un système qui empêche les intrusions mais on ne dit pas quels types de systèmes ou quels types de logiciels, parce que justement nous devons surtout rester neutre et ne pas nous retrouver juger partie. (S23.3 et P23.5) • Alors, Euhhhhhhhhhhhhhhhhhh, il y a plusieurs raisons. (P24.1) • Déjà il y a une raison règlementaire qui est obligatoire. (P24.2) • Ça c'est déjà une première réponse qui est assez forte. (P24.3) • Ce qui ne pourra pas extrêmement offrir à un auditeur externe. (P24.4) • Donc, c'est un point important. (P24.5) • Et trois, un audit interne est effectivement, je dirai en capacité à mieux comprendre les enjeux d'entreprises et apprécier aussi je dirai les prises du risque et les acceptations du risque. (P24.6) • Parce que je dirai dans une entreprise, si on doit faire de la sécurité, on risque de ne faire que ça, et alors, dans certaines branches, ça peut devenir nécessaire. (P24.7) • Mais, dans la banque, l'audit de la banque, c'est d'abord au cœur du business. (P24.8) • Il faut avoir cette juste vision entre le cœur du business et la sécurité. (P24.9)

		• Et donc, voilà l'audit interne est donc plus important que l'audit externe. (P24.10) • • • • Mais, aujourd'hui, nous intégrons plus un processus de base de maitrise des risques de la sécurité et donc il y a moins ce phénomène de rejet même s'il y a toujours cette crainte qui existe. (S27.2 et P27.1) • Oui, nous dans nos missions d'audit, nous faisons souvent appel à des expertises externes parce que de toute façon nous ne sommes pas polys compétents. (S31.1 et P31.1) •
Relations de l'audit interne avec autres fonctions (Sd)	• Nous avons parfois l'armée qui aussi vient demander des choses, puisqu'en certains cas il peut y avoir des aspects de sécurité nationale. (S33.3)	• Donc, d'après l'audit interne, qui est en charge de la relation entre l'établissement et l'audit externe, et nous nous assurons effectivement : un de leurs fournir tous les éléments qui sont nécessaires à leur audit et nous assurons aussi qu'eux même lorsqu'ils émettent des recommandations, aussi ils sont bien pris en compte et il y aura un bien suivi régulier de leur avancement. (S33.4 et P33.1) • Donc, même si quelque part, les gens n'aiment jamais voir l'audit arriver parce qu'ils savent que voilà, une manière ou d'une autre, quand même si ce n'est pas directe, juger leur travail est potentiellement leur adresser un travail supplémentaire pour corriger les erreurs que nous aurons identifiés. (P25.4 et S25.2)

2. Production des catégories par l'analyse structurale

Notre travail présenté en ce qui précède était purement inductif. Nous allons maintenant dégager des unités de sens sur la base de notre description préalable et essentielle. Ces unités de sens sont appelées *« catégories sémiques »* selon Greimas qui sont constitutives de la logique sociale de l'entretien et de sa forme sémique.

Notre travail sera un travail démonstratif qui se reposera sur quelques principes de base qui constitueront une sorte de fonds communs de l'analyse structurelle. Conformément à notre projet de départ, nous sommes obligés de montrer la démarche en acte en introduisant des équivalents dans la littérature. Nous signalons les multiples choix sur lesquels repose la mise en œuvre de toute démarche d'inspiration structurale. Donc, notre mise en œuvre repose sur une intelligence préalable du discours que la partie précédente n'a que formaliser.

a. Disjonction et Conjonction

Nous allons considérer l'hypothèse de base de l'analyse est de traduire le schème précédent en une combinaison de catégories typiques constitutive du sens général de l'entretien.

Nous assumons que la révolution structurale consiste à analyser toute langue naturelle et tous ensemble signifiant comme un système d'opposition à l'intérieure d'une relation constitutive du sens. Nous s'occupons à des « éléments différentiels » ou des « traits distinctifs » qui assurent l'existence d'une langue. Donc, ce qui est vrai au sens lexical l'est aussi au sens sémantique.

Nous admettons que le sens linguistique d'un mot ne se comprend qu'en restituant la disjonction qui le spécifie et la conjonction qui lui assure son appartenance à une catégorie. La disjonction trouve son origine dans la chaine syntagmatique constitutive du signifiant et la conjonction de l'intégration paradigmatique définissant le signifié.

b. Application à l'entretien et à ses trois niveaux

i. La signification des séquences : l'opposition je sais/je ne sais pas

Cezard qualifie les expériences qu'elle a tiré des différentes phrases de son parcours au moyen d'expression souvent lapidaires :

(S1) : « Mes missions d'audit sont variées. » (§3)

(S2) : « on identifie des risques … » (§3)

(S3) : « Nous on n'intervient pas sur la sécurité de système d'information. » (§6)

(S4) : « Ce que je peux vous dire c'est qu'on a eu mission l'année dernière mais comme on n'est des auditeurs généralistes, on a dû faire appel à des cabinets externes. » (§6)

(S5) : « Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT. » (§6)

(S6) : « on est des auditeurs généralistes mais pas des auditeurs spécialisés des systèmes d'information... » (§6)

(S7) : « En interne chez nous, on n'a pas d'auditeur spécialisé en sécurité du système d'information. (§7)

(S8) : « On n'a pas d'auditeur qui soit spécialisé en informatique. » (§7)

(S9) : « pour voir si le système d'informatique est bien verrouillé, il faut certaine compétence d'informatique. » (§7)

(S10) : « On n'a pas en interne… on fait appel à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. » (§7)

(S11) : « On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était une diversité de métier intéressant et une diversité d'opportunité également de carrière. » (§8)

(S12) : « Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchies sur des améliorations sur le contrôle interne. » (§11)

(S13) : « c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque, c'est ce qui me valorise en gros. » (§11)

(S14) : « Ce que je sais qu'avec le contrôle et les habilitations, c'est vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, qu'il avait regardé tous les dispositifs de contre de test d'intrusion pour voir si notre banque réalise bien de test d'intrusion. » (§15)

(S15) : « C'est ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y un système qui est développer par IBP. » (§15)

(S16) : « C'est l'application privative dans tous les services et ils ont fait des tests pour voir s'ils étaient bien verrouillés. » (§15)

(S17) : « Sur cette mission-là, la directrice de l'audit, l'ancienne directrice de l'audit qui est partie maintenant, elle avait choisi qu'on fait s'appelé a une cabine extérieure parce qu'elle considère qu'on a vais pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives. » (§17)

(S18) : « Et je pense qu'elle avait raison parce qu'on a vais pas toutes les compétences requises pour par exemple faire des tests d'intrusion. » (§17)

(S19) : « On n'a pas les compétences en interne au niveau de la sécurité de système d'information qui est nouveau comme même une problématique intéressante on n'a pas d'auditeur spécialisé en ce système d'information. » (§17)

(S20) : « Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. » (§18)

(S21) : « C'est le résultat de l'audit qui a dit attention parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevés c'est que justement le RSSI n'étais pas suffisamment proactif. » (§18)

(S22) : « C'est pourquoi la solution a été d'embauche un autre RSSI pour couvrir à temps complet. » (§18)

(S23) : « Tous ce qui développe des applications privatives dois prendre en compte cette impérative de sécurité quand il développe des applications privatives et faire une coordination avec le RSSI justement. » (§19)

(S24) : « Puis comme je vous l'avez dit tout à l'heure, dans la vie, tous les jours comme je vous l'ai dit, tout est concerner. » (§24)

(S25) : « Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI. » (§26)

(S26) : « pour moi ce n'est pas notre rôle de maintenir tout seul la cybersécurité, c'est avec la direction des risques, c'est avec les autres services avec les services qui développe des applications, des services informatiques. » (§27)

(S27) : « Oui, nous il nous manque les compétences internes parce que pour moi il faut des auditeurs spécialisés en système d'information. » (§31)

(S28) : « Un auditeur généraliste aura du mal à évaluer la force, qualité de contrôle interne d'informatique s'il ne connait rien dans l'informatique. » (§31)

(S29) : « il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT. » (§31)

(S30) : « Oui c'est ça, après il faut avoir des moyennes et puis il faut avoir l'envi de suffisamment mener une mission là-dessus vous savez c'est toujours l'histoire entre le besoin et le coût etc. » (§32)

(S31) : « Mais déjà si en interne on arrive on a des failles, il faut les résoudre déjà avec les gens qu'on a remplacés et il n'y a pas de solutions qu'avec les recrutements externes pour régulariser ces problèmes. » (§35)

(S32) : « Là justement On a demandé, il y a le rapport qu'on a fait l'année dernier avec les cabinets externes qu'il y a recrutement plus au niveau de RSSI. » (§36)

Nous allons ici faire des hypothèses en restant le plus près possibles du texte retranscrit. Nous allons rétablir les oppositions entre unités de diverses séquences-types :

- Nos missions d'audit sont variées, On identifie tous les risques / Nous on n'intervient pas sur la sécurité de système d'information.
- Une diversité des missions, une diversité de métier intéressant et une diversité d'opportunité également de carrière / pour voir si le système d'informatique est bien verrouillé, il faut certaine compétence d'informatique qu'on n'a pas.
- On est des auditeurs généralistes/ pas des auditeurs spécialisés des systèmes d'information, on n'a pas d'auditeur en IT.
- Faire réfléchies sur des améliorations sur le contrôle interne, proposer des rapports avec des recommandations / Pas proposer des recommandations en sécurité informatique par manque de compétence.
- Réussir à l'application privative parce qu'il y un système qui est développer par IBP / on n'avait pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives, Pas de compétences requises pour par exemple faire des tests d'intrusion.
- Pas les compétences en interne au niveau de la sécurité de système d'information qui est nouveau comme même une problématique intéressante on n'a pas d'auditeur spécialisé en ce système d'information / le résultat de l'audit : d'embaucher un autre RSSI pour couvrir à temps complet.
- Rapport d'audit suggère d'améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI et d'auditeurs spécialisés en sécurité informatique / Rapport pas totalement suivi contrainte de besoin et de coût.

L'opposition je sais/je ne sais pas concerne successivement ou simultanément toutes les catégories ou séquences citées (S0 à Sd). Cezard précise que le service d'audit interne est incompétent en cybersécurité. Il ajoute que le RSSI est responsable d'assurer la cybersécurité. Le résultat d'audit suggère l'embauche d'un deuxième RSSI pour couvrir tous les risques de la banque en sécurité informatique. Philipe insiste sur le recours au cabinet externe « ITEKIA » en cas de mission d'audit sur les services informatiques car il y a manque de compétences techniques et manque de compétence de réussir à l'application privative. Le service d'audit ne sait pas vérifier le système développé par l'I-BP. Enfin, le rapport d'audit n'a pas totalement été suivi pour embaucher des auditeurs internes spécialistes en IT par contrainte de besoin et de coûts.

ii. La signification des actants : pareils/pas pareils et mieux/pire

Nous allons procéder de la même façon pour les actants du récit de Philipe.
Nous résumons dans ce tableau ci-dessous les acteurs pareil et pas pareil à Cezard.

Pareil	Pas Pareil
Chefs de missions (A2)	Cabinet extérieur « ITEKIA » (A4)
Auditeurs Internes (A3)	I-BP (A6)
BPVF (A5)	RSSI Didier G. (A8)
Agnès Bayard (A7)	Nouvelle RSSI embauché pour aider Didier G. (A9)
Directeur Général (A10)	La direction des risques (A14)
Les audités (A11)	
L'inspection générale (A12)	
Les employés (A13)	

Nous pouvons maintenant analyser le sens de l'opposition Pareil/Pas Pareil en retrouvant les catégories associant la conjonction de deux termes. Nous vérifions que pour Philipe Cezard, sont pareils ceux qui n'ont pas les expertises et les connaissances techniques en cybersécurité, et pas pareils que lui, ceux qui ont les compétences techniques en cybersécurité. Pour Philipe le mieux sera que la cybersécurité soit une préoccupation de tous, que le RSSI coopère avec les autres employés pas seulement les experts et les cabinets externes, qu'il coopère aussi avec les auditeurs internes. Le pire c'est de laisser le RSSI seul responsable d'assurer la cybersécurité dans la banque. Philipe signale qu'il est nécessaire à tous les employés de protéger leurs données informatiques. (Mots de passes, ordinateurs…)
Le pire c'est d'avoir un conflit interne entre les auditeurs internes et les employés en termes de sécurité informatique. Aussi, le pire est de ne pas exécuter les points d'amélioration du rapport d'audit comme l'embauche d'auditeurs spécialisés à temps plein par contrainte de besoin et de coûts. Il faut en interne que l'auditeur interne spécialisé résous des failles en sécurité informatique pas avec des cabinets externes. De même, le pire c'est de ne pas avoir les compétences en interne pour appliquer les applications privatives développées par I-BP. Ces applications vérifier par le cabinet externe « ITEKIA » protègent la sécurité informatique de la banque.

iii. La signification des arguments : Facile/Pas facile

Philipe annonce qu'il y a un manque d'auditeur interne spécialisé dans le service d'audit. Ceci leur empêche de vérifier les applications privatives développées par I-BP et de ne pas intervenir sur les missions d'audit sur le département informatique.

Il assure que les auditeurs internes ne sont pas spécialistes en sécurité informatique, ils ont un manque de compétence en sécurité informatique. Mais, il oppose son discours en disant :

- qu'il réalise des missions d'audits variés sur tous les services de la banque. Mais il ne réalise pas de mission sur le service d'informatique pour manque de compétences.
- en disant que la cybersécurité est la préoccupation de tous et il faut protéger nos données et nos informations mais en disant que c'est une responsabilité autonome du RSSI.
- en disant qu'il est généraliste et identifie tous les risques, mais dans le cas de la cybersécurité, un risque majeur, ce sont des expertises qu'il n'a pas, on n'intervient pas sur le service de sécurité informatique. La banque fait recours au cabinet externe « ITEKIA » expert en sécurité informatique.
- en disant qu'il y a besoin d'embaucher des auditeurs internes spécialisés en IT ou sécurité informatique. Mais, ce n'est pas possible par contrainte de besoin et de coût. (Il n'est pas suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission, c'est coûteux.)

Nous analysons ces oppositions pour trouver la totalité qui donne sens à ces couples, découvrir la conjonction qui englobe cette disjonction.

c. <u>La structuration de l'univers sémantique et la logique du récit</u>

Rappelons les résultats acquis à ce stade de l'analyse. Une première opposition je sais/je ne sais pas structure les séquences de Philipe. Nous l'avons décomposée selon trois propriétés combinées qui permettent de qualifier les renseignements de cybersécurité dans la banque :

- Je ne sais pas = Pas de compétence technique informatique+Pas réussir à l'application privative+recours à un cabinet externe « ITEKIA »
- Je sais = Compétence technique spécialisé en informatique+Auditeur interne spécialisé+Réussir à l'application privative+Assurer la cybersécurité

Une seconde opposition pareil/pas pareil structure les segments du récit qui mettent en scène des actants de la vie de Cezard. Nous en avons trouvé deux propriétés principales qui permettent de qualifier les significations d'une autre « totalité » que l'on peut appeler statut :

- Pareil=Pas d'expertise+Pas de responsabilité+Pas d'ordonnance de recommandations
- Pas pareil= Expertise technique+Responsabilité de cybersécurité+Ordonnance de recommandations

Une autre opposition a été introduite pour rendre compte de la structuration du récit des actants : mieux/pire, qui renvoie à une autre « totalité » qu'il faut y avoir une collaboration pour réduire les failles et les cybers attaques.

Une troisième opposition nous a permis de structurer la narration de Philipe Cezard et de qualifier la relation précédente facile/pas facile. Nous allons extraire donc les propriétés suivantes :

- Facile=expertise technique+compétence technique en SI+recommandations
- Pas Facile=Incompétent domaine informatique+Contrainte du coût+Contrainte de Besoin

Nous allons terminer notre analyse par-là construction d'axes croisés permettant d'attribués des propriétés identiques à plusieurs significations dégagées antérieurement. Nous proposons pour l'entretien de Philipe les schémas suivants :

Tableau 1. Situation et perspectives professionnelles de Philipe

	Positives (Je sais)	Négatives (Je ne sais pas)
Possible (Facile)	Préoccupation de tous et du RSSI	Cabinet Externe « ITEKIA »
Impossible (Pas Facile)	Embauche des auditeurs internes spécialisés en sécurité informatique et coopération avec le RSSI (Réalisent des missions sur le SI et en donne des recommandations, réussir à l'application privative. développée par l'I-BP)	Ne pas suivre les recommandations du rapport d'audit par contrainte de besoin et de coût. Conflit entre le RSSI et les employés relatifs à la réussite de l'application privative.

Tableau 2. Personnages propre et perspectives professionnelles de Philipe

	Semblables (Pareil)	Différents (Pas Pareil)
Positives (Mieux)	Auditeurs internes, Directeur générale, Directeur de l'audit, Chefs de missions	Cabinet externe « ITEKIA », I-BP
Négatives (Pire)	Employés, clients, Audités	RSSI, seul responsabilité

B3. Méthodologie de codage du guide d'entretien du chef de mission d'audit à la BPVF

Le codage du guide d'entretien du chef de mission d'audit interne à la BPVF

Premier codage de l'entretien

41 questions = 41 séquences

Codage du Segment 1 (§1) :

J'ai fait une école de commerce à paris dans un institut supérieur du commerce. (S1.1)

Ensuite, j'ai fait un DECF un diplôme de comptabilité. (S1.2)

J'ai commencé à faire ma carrière dans l'audit comptable dans un cabinet d'expertise comptable en audit externe et en suite j'ai rejoint la Banque populaire de Bourgain France compte en audit interne. (S1.3)

Et j'ai fait une mobilité group pour venir à la Banque populaire val de France toujours en audit interne. (S1.4)

Codage du Segment 2 (§2) :

J'ai cherché par internet pour la Banque populaire Bourgain France compte et après c'est une mobilité. (S2.1)

Si ton cv est organisé en Banque populaire régional et on peut changer de région donc j'ai changé de région donc j'ai fait une mobilité. (S2.2 et P2.1)

Codage du Segment 3 (§3) :

Mes missions d'audit sont variées. (P3.1)

Ça peut être d'audit sur les fraudes, sur les chèques, sur la sécurité du système d'endogène. (S3.1)

J'étais intervenue également des audits sur le réseau multi marché donc audit d'agence. (S3.2)

Voilà, j'interviens en tant que chef des missions et du coup on doit élaborer un programme de travail qui identifie des risques préalables à mettre en place du contrôle pour valider le programme du travail, des tests voilà et mettre en

rapport avec des recommandations sur les points risques qu'on a identifiés mais des coûts intérieurs sur des missions travaillées. (S3.3 et P3.2)

Codage du Segment 4 (§4) :

J'ai fait une école de commerce de comptabilité sur l'entrée en audit externe, c'est dans les cabinets d'expertise comptable donc j'ai fait l'audit. (S4.1)

Et j'allais voir les entreprises, mais j'étais externe de l'entreprise et du coup je voulais faire de l'audit interne, un audit à l'intérieur de l'entreprise, mais c'été la suite logique de l'audit externe. (S4.2 et P4.1)

Codage du Segment 5 (§5) :

La rigueur, organisation, parce qu'il fait qualifier. (A5.1)

Empathie parce qu'il faut être d'ambiance quand même avec les auditée. (A5.2)

Capacité d'analyser des synthèses parce qu'il faut synthétiser tous les travaux qui sont fait par les auditeurs donc il faut avoir une capacité pour synthétiser tous les problématiques relevés. (A5.3)

Prise de hauteur pour arriver à avoir prendre de la hauteur, prendre du reçu. En fait, on n'étudie pas point de taille mais avec ces points de taille il faut arrive à prendre de la hauteur pour synthétiser en fait pour voir les problèmes. (A5.4)

L'auditeur de plus y détail tous c'est travaux, etc. (A5.5)

Le chef des missions il faut prendre de hauteur pour synthétiser les problématiques relevées par l'auditeur. (A5.6)

Codage du Segment 6 (§6) :

Nous on n'intervient pas sur la sécurité de système d'information. (S6.1)

Ce que je peux vous dire c'est qu'on a eu mission l'année dernière mais comme on n'est des auditeurs généralistes, on a dû faire appel à des cabinets externes. (S6.2 et P6.1)

Donc nous avons travaillé avec des cabinets externes qui ont auditée le système d'information de nos banques. (A6.1)

Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT. (P6.2 et S6.3)

En fait, on n'est des auditeurs généralistes de banque mais pas des auditeurs spécialisés des systèmes d'information, il y a des cabinée. (P6.3 et S6.4)

Là c'est le cabinet d'« ITEKIA » spécialisé en système d'information qui est venu chez nous, travailler en relation avec nous. (A6.2)

Mais nous on faisait plus des relations avec les auditée. (S6.5)

On fait un peu la bottelette, c'est eux qui faisaient l'investigation. (A6.3 et S6.6)

Codage du Segment 7 (§7) :

En interne chez nous, on n'a pas d'auditeur spécialisé en sécurité du système d'information. (P7.1)

On n'a pas d'auditeur qui soit spécialisé en informatique. (P7.2)

Et pour voir si le système d'informatique est bien verrouillé, il faut certaine compétence d'informatique. (S7.1)

On n'a pas en interne donc on a fait appeler à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. (A7.1 et S7.2)

Codage du Segment 8 (§8) :

On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était une diversité de métier intéressant et une diversité d'opportunité également de carrière. (S8.1 et P8.1)

On peut travailler dans le commercial, dans le développement, donc une diversité de métier qui est proposé c'est ce qui m'a attiré dans le secteur bancaire. (P8.2)

Codage du Segment 9 (§9) :

Là c'est un choix familial en fait de rejoindre ma famille qui est cité dans une région dans l'appartement des avelines. (P9.1)

Donc la Banque populaire parce que c'est une banque mutualise qui respecte les valeurs humaines comme un demi-collaborateur. (P9.2 et A9.1)

Ce n'est pas une immense machine, c'est une banque qui value l'humain. (A9.2)

Voilà pour la valeur, pour l'état humain et pour le rapprochement géographique familial. (A9.3)

Codage du Segment 10 (§10) :

Oui je pense après. (P10.1)

J'aurai la barrière de l'anglais. (P10.2)

On a beaucoup des banques nationales qui demande qu'on soi bi-langue et qu'on écrit et on parle l'anglais donc je pense que ça va se constituer en France. (A10.1 et S10.1)

Si non, je pense qu'on est capable de travailler dans n'importe quelle banque. (P10.3)

À mon avis c'est le même mais il y a changement de système d'information mais si non c'est la même technique d'audit. (P10.4)

Donc je pense oui je peux travailler dans un autre établissement sauf la problématique de l'anglais. (P10.5)

Codage du Segment 11 (§11) :

Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchies sur des améliorations sur le contrôle interne. (S11.1 et P11.1)

Donc c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque, c'est ce qui me valorise en gros. (S11.2 et P11.2)

Codage du Segment 12 (§12) :

Alors, ça c'est une bonne question, pour gainer ma vie, pour avoir un salaire à la fin du mois et également pour m'épanouir parce que je pense que le travail ça permis d'accomplir cément personnelle et puis également une problématique matérielle pour gagner sa vie. (S12.1 et P12.1)

Codage du Segment 13 (§13) :

Dans la banque populaire val de France, les salariés totaux c'est 2200. (A13.1)

Il y a le réseau commercial, la direction des crises, je ne sais pas exactement mais 6 ou 7 départements j'imagine, des départements fractionnels ou des départements commerciaux. (P13.2)

Il y a de développement, finance, il y a le réseau multi marché donc tout ce qui est les agences, toutes les fonctions risque et contrôle, audit etc. qui sont attachées directement à la direction générale. (S16.1)

Il y a tous ce que les gestions privée et entreprise, les marchés de l'entreprise donc 5 ou 6 départements. (S16.2)

Codage du Segment 14 (§14) :

Protection, contre des attaques externes sur le système d'information. (P14.1)

Protection des données également parce qu'on a des données des clients qui sont confidentielles, il faut qu'elles soient protégées. (P14.2)

Et également protection contre les attaques malveillantes et l'espionnage. (P14.3)

Voilà ce genre des choses c'est vraiment la protection du système d'information pour éviter qu'il y a des intrusions. (P14.4 et S14.1)

Codage du Segment 15 (§15) :

Je ne sais pas, je n'ai pas le rapport sur les yeux. (P15.1)
Ce que je sais qu'avec le contrôle et les habilitations, c'est vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, qu'il avait regardé tous les dispositifs de contre de test d'intrusion pour voir si notre banque réalise bien de test d'intrusion. (S15.1 et P15.1)
C'est ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y a un système qui est développer par IBP. (A15.1 et P15.2)
Et cela qu'on avait tendance à passer comme c'est IBP qui protège tous or il y a des applications développer chez nous en interne donc ils ont recensé. (A15.2 et S15.2)
C'est l'application privative dans tous les services et ils ont fait des tests pour voir s'ils étaient bien verrouillés. (A15.3 et S15.3)
Ils ont même réalisé des tests d'intrusion. (A15.4)
Ils ont réalisé eux-mêmes des tests d'intrusion donc vous imaginez pour faire ça il faut quand même certaine compétence informatique ce qui explique que nous ne pouvons pas le faire. (A15.4 et P15.3)

Codage du Segment 16 (§16) :

Justement, pour par exemple ce type de 2 choses : ils ont comme ça put faire des tests d'intrusion pour voir si ont été bien verrouillé parce que nous on n'a pas pu faire en interne. (A16.1 et P16.1)

Codage du Segment 17 (§17) :

Sur cette mission-là, la directrice de l'audit, l'ancienne directrice de l'audit qui est partie maintenant, elle avait choisi qu'on fait s'appelé a une cabine extérieure parce qu'elle considère qu'on a vais pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives. (A17.1 et S17.1)
Et je pense qu'elle avait raison parce qu'on a vais pas toutes les compétences requises pour par exemple faire des tests d'intrusion. (A17.2 et P17.1)
Donc nous sur les audits bancaires, on se débrouille. (S17.2)
C'est à dire on a des compétences en interne pour faire nos audits surtout sur le domaine bancaire, protection clientèle, les contrats crédits, tout ce qui est risque bancaire. (S17.3)
On a les compétences en interne au niveau de la sécurité du système d'information qui est nouveau quand même une problématique intéressante on n'a pas d'auditeur spécialisé en ce système d'information. (S17.4 et P17.2)
C'est pour cela on a fait appeler à ce cabinet. (A17.2)

Codage du Segment 18 (§18) :

Mais pas dans notre service d'audit interne, je ne sais pas son poste mais ça peut être : RSSI responsable sécurité du système d'information. (A18.1 et P18.1)
Oui effectivement il y a une deuxième personne et ça été une suite à notre mission qu'on a fait l'année dernière. (S18.1)
Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. (A18.2 et S18.2)
En fait c'est le résultat de l'audit qui a dit attention en demi et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevés c'est que justement le RSSI n'était pas suffisamment proactif. (A18.3 et S18.3)

Ça serait près des services que tout est bien fait quand tu avais un développement d'implication privative parce que quand tu développes une implication privative il fait prendre en compte la sécurité des systèmes d'information. (S18.3)

Et ça le cabinet externe a trouvé que justement on ne prenait pas suffisamment compte la sécurité du système d'information pour développer des applications privatives. (A18.4 et S18.4)

C'est pourquoi la solution a été d'embaucher un autre RSSI pour couvrir à temps complet. (A18.5 et S18.5)

C'est ça exactement mais je ne conne pas le nom de l'employée. (S18.6)

Codage du Segment 19 (§19) :

C'est le RSSI justement, et tous les services également en fait. (A19.1)

Tous ce qui développe des applications privatives dois prendre en compte cette impérative de sécurité quand il développe des applications privatives et faire une coordination avec le RSSI justement. (S19.1 et A19.2)

Codage du Segment 20 (§20) :

Oui alors, oui mais en particulier quand même oui, oui, mais ils ne sont pas tôt parce que nous également on doit faire attention à bien verrouiller nos ordinateurs, à pas donner des informations confidentielles etc. (A20.1 et S20.1)

D'une certaine manière, ils ont raisons mais il y a également tous ce qui développe des applications privatives doit venir compte. (A20.2 et S20.2)

Et ça n'est pas fait jusqu'à présent et le RSSI doit être impliqué dans tous les développements d'implication privative dans la banque. (A20.3 et P20.1)

Codage du Segment 21 (§21) :

On n'a pas eu temps de ça, en faite pour vous dire après la mission qu'on a fait avec le cabinet « ITEKIA ». (A21.1 et P21.1)

Ils ont fait une formation avec les autres banques populaires pour justement réaliser la même mission que nous mais dans les autres banques en fait on était un peu la banque pilote. (S21.1 et A21.2)

On a fait mission avec cette cabine externe et après ça ils ont fait une formation pour les autres auditeurs internes des autres banques suit à ça. (A21.3 et S21.2)

Une formation pour la cyber sécurité. (S21.3)

Codage du Segment 22 (§22) :

Il y en a d'autre mais je n'ai pas le rapport sous la main. (S22.1)

Je vous transmet le rapport par courrier après notre entretien. (S22.2)

Codage du Segment 23 (§23) :

Oui, oui, ouii c'est même le directeur général qu'à demander. (A23.1)

Codage du Segment 24 (§24) :

Réaliser des missions là-dessus. (S24.1)

Puis comme je vous les ai dites tout allure dans la vie tous les jours comme je vous l'ai dit, tout est concerner. (S24.2)

Donc il faut voilà être vigilant sur nos codes, ne pas laisser trainer le mot de passe puis si non dans nos cadres de mission les missions d'audit comme de même nature comme on a fait l'année dernière même si c'est avec un cabinet qu'on a intervenu pour rédiger le rapport etc. (S24.3 et A24.1)

Codage du Segment 25 (§25) :

Oui je pense oui. (P25.1)

Codage du Segment 26 (§26) :

Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI. (S26.1 et P26.1)

C'est en cours d'amélioration. (P26.2)

Et l'année prochaine, on fait des missions d'audit groupe donc qui vont être pilotée par des chefs de missions justement de l'informatique locale donc on va continuer à investiguer et faire des missions sur cette thématique pour la renforcer. (S26.2 et A26.1)

Parce que c'est nouveau en fait la problématique de RSSI ce n'est pas tellement pris en compte jusqu'à présent mais il faut aller de plus en plus. (A26.2 et P26.3)

Codage du Segment 27 (§27) :

Non mois je n'ai pas tout à fait d'accord. (P27.1)

Nous on est en 3ième niveaux, nous ont vient vérifier. (P27.2)

C'est bien fait mais nous on intervient en 3ième rideau. (P27.3)

Donc, pour moi ce n'est pas notre rôle de maintenir tout seul la cybersécurité, c'est avec la direction des risques, c'est avec les autres services avec les services qui développe des applications, des services informatiques. (P27.4)

Mais il n'y a pas que l'audit, nous on vient en derrière ce que je puisse dire donc on n'est pas, ce n'est pas que à nous de les faire. (P27.5)

Codage du Segment 28 (§28) :

Ce ne serait pas suffisant d'avoir que des auditeurs externes presque nous on est en plein temps dans la banque pour auditer en permanence. (A28.1 et S28.1)

Il y a tellement des trucs qu'audité, un audit externe il faudra qu'il soit là tout le temps ça serait pas possible pour moi c'est obligatoire d'avoir un audit interne. (P28.1)

Codage du Segment 29 (§29) :

Il doit avoir un principe d'indépendance c'est-à-dire nous on est là pour vérifier donc on doit être indépendant des personnes qu'on audit parce qu'on doit surveiller si les normes sont bien appliquées. (P29.1)

Donc il ne faut pas de collision entre guillemet, il faut qu'on soit disponible, professionnelle, à l'écoute il faut qu'on ne vaille pas trop parce qu'on vient déranger les gens dans le travail. (P29.2)

Donc il faut prendre en compte les impérative des autres employées. (A29.1)

Donc il y a tout en aspe de professionnaliste mais à la fois d'empathie et d'indépendance c'est tout ça pour moi l'auditeur. (P29.3)

Codage du Segment 30 (§30) :

Là justement il faut que l'auditeur adopte le comportement d'indépendance, pour moi c'est comme ça qu'on peut, il faut qu'on pas être en conflit interne. (A30.1 et P30.1)

Exemple : il ne faut pas avoir un poste en direction quand on va auditer une direction parce qu'on ne va pas être indépendant par rapport à ce qu'on va dire on va être trop gentille pour avoir le post. (A30.2 et P30.2)

Codage du Segment 31 (§31) :

Oui, nous il nous manque les compétences internes parce que pour moi il faut des auditeurs spécialisé s en système d'information. (P31.1 et S31.1)

Un auditeur généraliste aura du mal à évaluer la force, qualité de contrôle interne d'informatique s'il ne connait rien dans l'informatique. (A31.1)

Donc il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT. (P31.2)

Codage du Segment 32 (§32) :

Oui c'est ça, après il faut avoir des moyennes et puis il faut avoir l'envi de suffisamment mener une mission là-dessus vous savez c'est toujours l'histoire entre le besoin et le coût etc. (P32.1)

Codage du Segment 33 (§33) :

Je pense que ça peut être de refaire ce qu'on a fait l'année dernier c'est-à-dire de recourir un cabinet externe. (A33.1)

Codage du Segment 34 (§34) :

Le besoin n'est pas, disons qu'on a eu une mission peut-être dans l'année. (P34.1)

Chaque année on va avoir une mission à mener sur le système d'information je pense que ce n'est pas suffisant pour nécessiter. (P34.2)

Aujourd'hui en tous cas, ça ne semble pas suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission. (P34.3 et A34.1)

Codage du Segment 35 (§35) :

Je comprends il est en croissance mais le nécessaire chez nous est d'avoir un auditeur en temps plein c'est pour l'instant. (P35.1 et A35.1)

Mais je suis d'Accord avec vous. (P35.2)

C'est ce que la banque est entraîne de faire de renforcer ses systèmes parce qu'il n'y a pas que des niveaux humains également contrer à la place. (P35.3 et S35.2)

Il faut que tous les services soient impliqués. (P35.3)

Les services informatiques aussi donc voilà on peut déjà renforcer ce qu'on a fait et ensuite voir ce qu'il faut recruter d'autre. (S35.3)

Mais déjà si en interne on arrive on a des failles, il faut les résoudre déjà avec les gens qu'on a remplacés et il n'y a pas de solutions qu'avec les recrutements externes pour régulariser ces problèmes. (S35.4 et P35.4)

Codage du Segment 36 (§36) :

Là justement on a demandé, il y a le rapport qu'on a fait l'année dernier avec les cabinets externes qu'il y a recrutement plus au niveau de RSSI. (S36.1)

Donc on est plutôt dans le sens il faut qu'on renforce, les moyens de sécurité à situer ont été plutôt dans l'aspect là mais pas dans l'aspect des coûts. (P36.1)

Codage du Segment 37 (§37) :

Là c'est la direction des risques, elle est chargé de prendre à compte la recommandation sur le fait d'augmenter, les rejoint des moyennes allouer à la sécurité des systèmes d'information. (S37.1 et A37.1)

Donc ce qui affecte la direction des risques, c'est à eux de devoir mettre en œuvre les mesures, le plan d'action avec une date de séance. (S37.2 et A37.2)

Donc ils n'ont pas de liberté de prendre en compte la recommandation. (P37.1)

Codage du Segment 38 (§38) :

On avait un programme de travail qui a été établie avec l'inspection générale de BPCE et programme de travail a été mené par le cabinet extérieur. (A38.1 et A38.2)

Mais il passait par nous pour tout ce qui été document à demander au collègue interne. (S38.1)

Et on les renvoyer les documents sur un message resécurisé crypté, nous on coordonne comme ça. (S38.2 et P38.1)

Codage du Segment 39 (§39) :

Il doit organiser sa journée, planifier ses rendez-vous, mener des entretiens, réaliser des tests pour vérifier tous ce qu'on lui a dit est correcte, synthétiser tous ce qu'on a dit pour rédiger un rapport. (A39.1 et P39.1)

Codage du Segment 40 (§40) :

Oui, il pense que l'audit est un rôle de gendarme mais on n'est pas là que pour ça. (P40.1 et A40.1)

C'est-à-dire quand on fait partie de l'entreprise puis quand on veut faire avancer une entreprise en proposant des actes amélioration. (P40.2)

Mais pas que des gendarmes. (P40.3)

Mais ça dépend des audités. (A40.2)

Il y a des audités qui ont compris qu'on est là pour donner une valeur ajoutée et autre qui nous vois uniquement comme des gendarmes et qui ont peur. (A40.3 et P40.4)

Et ça c'est un travail de pédagogie à faire quand on fait la mission. (P40.5)

C'est pour expliquer qu'on est là pour travailler avec eux mais pas de faire des gendarmes. (P40.6)

Codage du Segment 41 (§41) :

Il faut communiquer, pédagogie puis voilà professionnelle. (P41.1)

2. Classement des unités codées : Recodage

I. Les séquences-types de l'entretien de Thomas D.

Nous allons maintenant regrouper et ordonner les séquences dans l'ordre chronologique depuis le départ (S0) jusqu'à la fin de l'entretien (S+). Nous allons joindre toutes les unités concernées (tous les S) en leur donnant un titre résumant leur contenu.

Nous avons divisé l'entretien de Thomas D. en cinq séquences respectives selon l'ordre chronologique.

10. Niveau de formation et progression de la carrière

S0=S1.1+...+S1.4+S2.1+S2.2+S4.1+S4.2+S10.1+S12.1+S16.1+S16.2

11. Fonction de Chef de mission en audit : Rôle et missions

Sa=S3.1+S3.2+S3.3+S6.5+S6.6+ S8.1+S11.1+S11.2+S15.1+S15.3+S15.1+S15.3

12. Cybersécurité : contrainte et implication

Sb=S6.1+...+S6.4+S7.1+S7.2+S14.1+S17.2+S17.3+S17.4+S19.1+S20.1+S20.2+S21.1+S21.2+S21.3+S22.1+S22.2+S24.1+S24.2+S24.3

13. Conséquence de la cybersécurité sur la banque

Sc=S18.1+…+S18.6

14. Travail relatif à la cybersécurité

SD=S26.1+S26.2+S26.3+S31.1+S35.2+S35.3+S35.4+S36.1+S37.2+S38.2

Nous allons maintenant proposer un premier résumé des séquences-types de l'entretien de Thomas D. après avoir effectué le regroupement selon un ordre chronologique.

Résumé des séquences-types de l'entretien de Thomas D.

Au début de l'entretien, Thomas D. nous annonce son parcours professionnel puis son insertion professionnelle dans la BPVF. Il a obtenu un diplôme de comptabilité, puis il commence sa carrière dans l'audit comptable dans un cabinet d'expertise comptable en audit externe. Ensuite, il a fait une mobilité group pour venir à la BPVF en audit interne.

Il explicite son rôle et ses missions comme chef de mission d'audit dans la BPVF.

Il intervient sur le réseau multi marché, c'est-à-dire l'audit d'agence. Il identifie les risques préalables à mettre en place du contrôle pour valider le programme du travail, et réalise des tests. Il présente son travail aux directions et les encourage à introduire des améliorations sur le contrôle interne. Il propose aussi des rapports avec des recommandations à la direction générale.

Thomas explique qu'il n'intervient pas sur la sécurité de systèmes informatiques. Il justifie l'appel à un cabinet externe pour réaliser une mission d'audit interne sur le système informatique par un manque de compétence informatique. Il admet que son service n'a pas d'auditeur spécialisé en informatique mais seulement des auditeurs généralistes. Il termine en disant qu'il n'est pas suffisant d'avoir des auditeurs externes spécialisés, il faut auditer en permanence.

Il confirme de faire une coordination avec le RSSI en tout ce qui concerne sécurité informatique. Il parle de responsabilité personnelle en faisant attention à la sécurité des ordinateurs personnels. Par exemple, il certifie de ne pas donner des informations confidentielles ni des mots de passe pour éviter le danger.

Thomas légitime l'embauche d'un deuxième RSSI car le travail du premier en cybersécurité était insuffisant. C'était la décision de la direction générale et du cabinet externe. Enfin, il parle du rapport d'audit qui a amélioré des points faibles en sécurité informatique comme l'embauche d'un nouvel RSSI.

J. Les acteurs du récit de Thomas D.

Nous allons ici identifiés les personnages dans le récit de Thomas. Nous allons inclure Thomas lui-même lorsqu'il se dédouble (« moi, je…).

Nous notons respectivement les acteurs de A1 jusqu'à An.

Le premier actant du récit est Thomas lui-même puisqu'il a utilisé le « je » respectivement 26 fois et le « moi » 8 fois.

Le second actant est le chef de mission en général.

A2= A5.1+A5.2+A5.3+A5.4+A5.6+A20.1+A24.1+A26.2

Le troisième actant est l'auditeur interne.

A3=A5.5+A30.1+A30.2+A31.1+A34.1+A35.1+A39.1+A40.1

Le quatrième actant est le cabinet extérieur « ITEKIA » embauché par la banque.

A4=A6.1+A6.2+A6.3+A7.1+A18.4+A21.1+A21.3+A33.1

Le cinquième actant est la Banque Populaire Val de France BPVF.

A5=A9.2+A9.3+A13.1

Le sixième actant est l'I-BP.

A6=A15.1+A15.2+A15.3+A15.4+A15.5+A16.1

Le septième actant est l'ancienne directrice d'audit « Agnès Bayard »

A7=A17.1+A17.2

Le huitième actant est le RSSI « Didier G. »

A8=A18.1+A18.3+A19.1+A20.3+A26.2

Le neuvième actant est le nouveau RSSI embauché

A9=A18.2+A18.5

Le dixième actant est le directeur général.

A10=A23.1

Le onzième actant est les audités.

A11=A40.2+A40.3

Le douzième actant est l'inspection générale.

A12=A38.1

Le treizième actant est les employés.

A13=A20.1+A24.1+A29.1

Le quatorzième actant est la direction des risques

A14=A37.1 et A37.2

Les actants du récit de Thomas D.

Le premier actant est Thomas D. lui-même. Nous analysons qu'il a fréquemment utilisé le « je » et le « moi » dans son récit pour donner son avis ou son opinion.

Le deuxième actant est le chef de mission. Il doit avoir une capacité d'analyse et qu'il prend de hauteur pour synthétiser les problèmes relevés par les auditeurs internes. Il pilote aussi les missions d'audit groupe.

Le troisième actant est l'auditeur interne. Selon Thomas, il doit savoir tous les détails du travail, il doit être indépendant pour échapper au conflit avec les autres, il doit être objectif aussi dans son travail. Thomas qualifie les auditeurs internes comme généralistes mais incompétents en sécurité informatique. Il justifie le recours à un cabinet externe au lieu d'un auditeur interne spécialisé en informatique en admettant qu'il ne suffit pas d'avoir un auditeur à temps plein spécialisé pour une seule mission. Enfin, il ne s'accorde pas avec l'idée que l'audit est un rôle de gendarme.

Le quatrième actant est le cabinet externe embauché « ITEKIA » spécialisé en sécurité informatique. « ITEKIA » est pour auditer le système d'information dans la banque. Thomas explique que le cabinet faisait l'investigation alors que l'audit interne faisait la bottelette, c'est-à-dire un travail très réduit relatif à l'observation en grande partie. Il confirme le recours à ce cabinet par manque d'expertise en sécurité informatique dans le département d'audit interne. Le cabinet externe a trouvé qu'il n'y a pas d'attention suffisante sur la sécurité du système d'information pour développer des applications privatives. L'appel à ce cabinet externe est essentiel chaque année pour réaliser des missions sur la sécurité informatique.

Le cinquième actant est la BPVF. Thomas a une riche connaissance de sa banque. Il l'a caractérisé en disant qu'elle respecte les valeurs humaines, elle value l'homme et c'est pourquoi il l'a valorisé.

Le sixième actant est l'I-BP. Selon Thomas, I-BP a développé des applications privatives en sécurité informatique. Elle assure une protection à la banque dans tous les services grâce aux applications privatives et elle a fait des tests pour voir s'ils étaient bien verrouillés et des tests d'intrusion. Thomas admet que l'I-BP est capable de réaliser ce travail car le service d'audit ne peut pas le faire. Son service est incompétent en sécurité informatique. Il limite la participation de l'audit à faire réussir les applications privatives.

Le septième actant est l'ancienne directrice d'audit interne « Agnès BAYARD ».

Elle a choisi le cabinet externe « ITEKIA » pour réaliser des missions sur le département informatique. Elle justifie son choix en admettant que l'audit interne n'a pas les compétences techniques pour savoir s'il y a des failles au niveau des applications privatives. Thomas légitime le choix d'Agnès en soulignant que l'audit interne n'avait pas toutes les compétences requises pour par exemple faire des tests d'intrusion.

Le huitième actant est le RSSI « Didier G. ». Thomas annonce que le résultat de l'audit a qualifié le RSSI comme pas suffisamment proactif. Il avoue que le RSSI est responsable de la sécurité informatique dans la banque mais qu'il a besoin d'aide. Il insiste sur une collaboration entre le RSSI et tous personnels relatifs aux applications privatives. En plus, il explique que le RSSI doit être impliqué dans tous les développements d'implication privative dans la banque. Il termine en disant que la problématique de RSSI est nouvelle et pas prise en compte.

Le neuvième actant est le nouveau RSSI embauché dans la banque.

Le nouvel RSSI a été embauche par la direction parce que Didier G. intervenait en mi-temps et ça n'était pas suffisant. Il va renforcer le travail de sécurité informatique avec Didier pour couvrir à temps complets tous les services.

Le dixième actant est le directeur général. Il a demandé aussi de renforcer la cybersécurité dans la banque en informant la direction générale de tous les impacts de la cybercriminalité.

L'onzième actant est les audités. Thomas les classe en deux catégories. Ceux qui savent que l'audit interne viennent donner une valeur ajoutée et ceux qui considèrent les auditeurs internes comme des gendarmes et ils ont peur d'eux.
Le douzième actant est l'inspection générale. Elle a lancé un programme avec la BPVF pour renforcer la cybersécurité mais qui a été mené par le cabinet externe « ITEKIA ».
Le treizième actant est les employés. Thomas les a mentionnés indirectement. Il leur demande d'être plus attentif sur leurs ordinateurs, de ne pas donner des informations confidentielles, d'être vigilant sur leurs codes. Il assume indirectement que la cybersécurité est le problème de tous les employés.
Le quatorzième actant est la direction des risques. Thomas explique qu'elle est en charge de prendre à compte la recommandation en ce qui concerne la sécurité d'information. C'est eux qui doivent mettre en œuvre les mesures, le plan d'action avec une date de séance et ils n'ont pas de liberté de prendre en compte la recommandation.

K. Les classes d'arguments

Ce niveau d'analyse concerne l'ensemble des arguments, démonstrations et propositions de Thomas D. destinés à nous convaincre. Nous allons regroupés l'ensemble des unités codées en P selon des « classes d'arguments » dont chacune représente une étape logique dans un raisonnement.
Nous allons classer les arguments le type de raisonnement que Thomas présente dans ces réponses. Nous en avons repéré sept qui font l'objet d'arguments explicites qui sont à la base de ce classement.
Nous avons noté (P1) les propositions de Thomas associé à l'intégration et l'implication dans son travail dans la banque. Il a affirmé plusieurs fois qu'il a fait une mobilité d'une banque à la BPVF. Il justifie ce changement en avouant qu'il voulait allez de l'audit externe à l'audit interne. Il annonce aussi qu'il favorise le travail dans la BPVF française car il a la barrière de l'anglais. Il rassure que toutes les banques aient les mêmes techniques d'audits mais différents systèmes d'informations.

- Si ton cv est organisé en Banque populaire régional et on peut changer de région donc j'ai changé de région donc j'ai **fait une mobilité**. (S2.2 et P2.1)
- Et j'allais voir les entreprises, mais j'étais externe de l'entreprise et du coup j'ai voulu faire de l'audit interne, un audit à l'intérieur de l'entreprise, mais c'été la suite logique de l'audit externe. (S4.2 et P4.1)
- On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était **une diversité de métier** intéressant et une diversité d'opportunité également de carrière. (S8.1 et P8.1)
- On peut travailler dans le commercial, dans le développement, donc une diversité de métier qui est proposé c'est ce qui m'a attiré dans le secteur bancaire. (P8.2)
- Là c'est un choix familial en fait de rejoindre ma famille qui est cité dans une région dans l'appartement des avelines. (P9.1)
- Donc la Banque populaire parce que c'est une banque **mutualise** qui respecte les valeurs humaines comme un demi-collaborateur. (P9.2 et A9.1)
- Oui je pense après. (P10.1)
- J'aurai **la barrière de l'anglais**. (P10.2)
- On a beaucoup des banques nationales qui demandent qu'on soit bi-langue et qu'on écrit et on parle l'anglais donc je pense que ça va se constituer en France. (A10.1 et S10.1)
- Si non, je pense qu'on est capable de travailler dans n'importe quelle banque. (P10.3)

- À mon avis c'est le même mais il y a changement des systèmes d'information mais si non c'est la même technique d'audit. (P10.4)
- Donc je pense oui je peux travailler dans un autre établissement sauf la problématique de l'anglais. (P10.5)
- Alors, ça c'est une bonne question, pour gainer ma vie, pour avoir un salaire à la fin du mois et également pour m'épanouir parce que je pense que le travail ça permis d'accomplir sa vie personnelle et puis également une problématique matérielle pour gagner sa vie. (S12.1 et P12.1)
- Il y a le réseau commercial, la direction des crises, je ne sais pas exactement mais 6 ou 7 départements j'imagine, des départements fractionnels ou des départements commerciaux. (P13.2)

Nous résumons cet ensemble ainsi : *« L'adéquation et le rattachement au travail dans la BPVF ».*
Nous avons noté (P2) les expressions de Thomas associés à son travail comme chef de mission dans la banque.

- Mes missions d'audit sont **variées**. (P3.1)
- Voilà, j'interviens en tant que chef de mission et du coup on doit élaborer un programme de travail qui identifie des risques préalables à mettre en place du contrôle pour valider le programme du travail, des tests voilà et mettre en rapport avec des recommandations sur les point risques qu'on a identifiés mais des coûts intérieurs sur des missions travaillées. (S3.3 et P3.2)
- Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchir sur des améliorations sur le contrôle interne. (S11.1 et P11.1)
- Donc c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque, **c'est ce qui me valorise en gros**. (S11.2 et P11.2)

Cet ensemble se résume ainsi : *« Travail d'audit qui identifie les risques et crée de la valeur ajoutée à la banque grâce à la proposition des recommandations ».*
Nous avons noté (P3) toutes les formules associées au recours au cabinet externe « ITEKIA » spécialisé en sécurité informatique.

- Ce que je peux vous dire c'est qu'on a eu mission l'année dernière mais comme on **est** des auditeurs généralistes, on a dû faire appel à **des cabinets externes**. (S6.2 et P6.1)
- Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas **d'auditeur en IT**. (P6.2 et S6.3)
- En fait, on **est** des auditeurs généralistes de banque mais **pas** des auditeurs spécialisés de systèmes d'information, il y a **des cabinets**. (P6.3 et S6.4)
- En interne chez nous, on **n'a pas** d'auditeur spécialisé en sécurité du système d'information. (P7.1)
- On **n'a pas** d'auditeur qui soit spécialisé en informatique. (P7.2)
- C'est ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y a un système qui est développer par IBP. (A15.1 et P15.2)
- Ils ont réalisé eux-mêmes des tests d'intrusion donc vous imaginez pour faire ça il faut comme même certaine compétence informatique ce qui explique que nous **ne** pouvons **pas** le faire. (A15.4 et P15.3)
- Justement, pour par exemple ce type de 2 choses : ils ont comme ça put faire des tests d'intrusion pour voir si ont été bien verrouillé parce que nous on **n'a pas pu faire** en interne. (A16.1 et P16.1)
- Et je pense qu'elle avait raison parce qu'on **n'**avait **pas** toutes les compétences requises pour par exemple faire des tests d'intrusion. (A17.2 et P17.1)

- On **n'**a **pas** les compétences en interne au niveau de la sécurité de système d'information qui est nouveau quand même **une problématique intéressante** on **n'**a **pas** d'auditeur spécialisé en ce système d'information. (S17.4 et P17.2)
- On n'a pas eu temps de ça, en fait pour vous dire après la mission qu'on a fait avec le cabinet « ITEKIA ». (A21.1 et P21.1)
- Oui, nous il nous **manque** les compétences internes parce que pour moi il faut des auditeurs spécialisés en système d'information. (P31.1 et S31.1)
- Donc il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT. (P31.2)

Cet ensemble se résume ainsi : *« L'absence d'un auditeur spécialisé en sécurité informatique implique le recours au cabinet externe ITEKIA pour réaliser les missions d'audit sur le département informatique ».*

Nous avons noté (P4) les expressions et les formules relatives à la cybersécurité.

- **Protection**, contre des attaques externes sur le système d'information. (P14.1)
- **Protection** des données également parce qu'on a des données des clients qui sont confidentielles, il faut qu'elles soient protégées. (P14.2)
- Et également **protection** contre les attaques malveillantes et l'espionnage. (P14.3)
- Voilà ce genre des choses c'est vraiment la **protection** du système d'information pour éviter qu'il y a des intrusions. (P14.4 et S14.1)
- Je ne sais pas, je n'ai pas le rapport sur les yeux. (P15.1)
- Ce que je sais qu'avec le contrôle et les habilitations, c'est vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, qu'il avait regardé tous les dispositifs de contre de test d'intrusion pour voir si notre banque réalise bien de test d'intrusion. (S15.1 et P15.1)

Cet ensemble se résume ainsi : *« La cybersécurité, c'est protéger le système informatique ».*

Nous avons noté (P5) les expressions et les formules associés à qui est responsable d'assurer la cybersécurité :

- Mais pas dans notre service d'audit interne, je ne sais pas son poste mais ça peut être : **RSSI** responsable sécurité du système d'information. (A18.1 et P18.1)
- Et ça n'est pas fait jusqu'à présent et le **RSSI** doit être impliqué dans tous les développements d'implication privative dans la banque. (A20.3 et P20.1)
- Oui je pense oui. (P25.1)
- Parce que c'est nouveau en fait la problématique de **RSSI** ce n'est pas tellement pris en compte jusqu'à présent mais il faut aller de plus en plus. (A26.2 et P26.3)
- Non mois je n'ai pas tout à fait d'accord. (P27.1)
- Nous on est en 3ième niveaux, nous, on vient **vérifier**. (P27.2)
- C'est bien fait mais nous on intervient en 3ième rideau. (P27.3)
- Donc, pour moi ce **n'**est **pas notre rôle** de maintenir tout seul la cybersécurité, c'est avec la direction des risques, c'est avec les autres services, avec les services qui développent des applications, des **services informatiques**. (P27.4)
- Mais il n'y a pas que l'audit, nous on vient en derrière ce que je puisse dire donc on **n'**est **pas**, ce **n'**est **pas** à nous de les faire. (P27.5)

Cet ensemble se résume ainsi : *« Le RSSI est responsable d'assurer la cybersécurité car l'audit est en charge de la surveillance en troisième niveau ».*

Nous avons noté (P6) le profil de l'auditeur selon Thomas :

- Il y a tellement des trucs qu'audité, un audit externe il faudra qu'il soit là tout le temps ça ne serait pas possible pour moi c'est **obligatoire** d'avoir un audit interne. (P28.1)
- Il doit avoir un principe d'**indépendance** c'est-à-dire nous on est là pour vérifier donc on doit être **indépendant** des personnes qu'on audite parce qu'on doit surveiller si les normes sont bien appliquées. (P29.1)
- Donc il ne faut **pas de collision** entre guillemet, il faut qu'on soit disponible, **professionnelle**, **à l'écoute,** il faut qu'on ne vaille pas trop parce qu'on vient déranger les gens dans le travail. (P29.2)
- Donc il y a tout en aspe de **professionnalisme** mais à la fois d'**empathie** et d'**indépendance** c'est tout ça pour moi l'auditeur. (P29.3)
- Là justement il faut que l'auditeur adopte le comportement d'**indépendance**, pour moi c'est comme ça qu'on peut, il faut qu'on pas être en conflit interne. (A30.1 et P30.1)
- Exemple : il ne faut pas avoir un poste en direction quand on va auditer une direction parce qu'on ne va pas être indépendant par rapport à ce qu'on va dire on va être trop gentille pour avoir le poste. (A30.2 et P30.2)
- Oui c'est ça, après il faut avoir des moyennes et puis il faut avoir l'envie de suffisamment mener une mission là-dessus vous savez c'est toujours l'histoire entre le besoin et le coût etc. (P32.1)
- Il doit organiser sa journée, planifier ses rendez-vous, mener des entretiens, réaliser des tests pour vérifier tous ce qu'on lui a dit est correcte, synthétiser tous ce qu'on a dit pour **rédiger** un rapport. (A39.1 et P39.1)
- Oui, il pense que l'audit est un **rôle de gendarme** mais on n'est pas là que pour ça. (P40.1 et A40.1)
- C'est-à-dire quand on fait partie de l'entreprise puis quand on veut faire avancer une entreprise en proposant des actes amélioration. (P40.2)
- Mais **pas que des gendarmes**. (P40.3)
- Il y a des audités qui ont compris qu'on est là pour donner **une valeur ajoutée** et autre qui nous vois uniquement comme des gendarmes et qui ont peur. (A40.3 et P40.4)
- Et ça c'est un travail de pédagogie à faire quand on fait la mission. (P40.5)
- C'est pour expliquer qu'on est là pour travailler avec eux mais pas de faire **des gendarmes**. (P40.6)
- Il faut communiquer, pédagogie puis voilà professionnelle. (P41.1)

Cet ensemble se résume ainsi : *« Double identité professionnelle des auditeurs internes dans leur travail ».*

Nous avons noté (P7) les expressions et les formules relatives à la mission d'audit réalisée sur la cybersécurité.

- Il y avait quelques points de faiblesses mais justement ce rapport a permis de commencer à améliorer des choses en termes de **dispositif du contrôle de recrutement de RSSI**. (S26.1 et P26.1)
- C'est en cours d'amélioration. (P26.2)
- Le besoin n'est pas, disons qu'on a eu une mission peut-être dans l'année. (P34.1)
- Chaque année on va avoir une mission à mener sur le système d'information je pense que ce n'est pas suffisant pour nécessiter. (P34.2)
- Aujourd'hui en tous cas, ça **ne** semble **pas** suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission. (P34.3 et A34.1)

- Je comprends il est en croissance mais le nécessaire chez nous est d'avoir un auditeur en temps plein c'est pour l'instant. (P35.1 et A35.1)
- Mais je suis d'Accord avec vous. (P35.2)
- C'est ce que la banque est entraîné de faire de renforcer ses systèmes parce qu'il **n'**y a **pas** que des niveaux humains également contrer à la place. (P35.3 et S35.2)
- Il faut que tous les services soient impliqués. (P35.3)
- Mais déjà si en interne on arrive on a des failles, il faut les résoudre déjà avec les gens qu'on a remplacés et il n'y a pas de solutions **qu'avec les recrutements externes** pour régulariser ces problèmes. (S35.4 et P35.4)
- Donc on est plutôt dans le sens il faut qu'on renforce, les moyens de sécurité à situer ont été plutôt dans l'aspect-là mais **pas dans l'aspect des coûts**. (P36.1)
- Donc ils n'ont pas de liberté de prendre en compte la recommandation. (P37.1)
- Et on les renvoyer les documents sur un message sécurisé crypté, nous on coordonne comme ça. (S38.2 et P38.1)

Cet ensemble se résume ainsi : *« Les résultats du rapport d'audit ne sont pas toutes suivies par contrainte de coûts ». Thomas explique que le rapport d'audit a recommandé :*

- *L'amélioration du dispositif de contrôle en termes de recrutement de RSSI.*
- *La nécessité d'un auditeur spécialisé en informatique à temps plein.*
- *Le manque de compétences techniques en sécurité informatique au niveau humain ce qui empêche le renforcement du système informatique.*
- *L'implication de tous les services dans l'assurance de la cybersécurité.*
- *Recours à un cabinet externe spécialisé pour régulariser les problèmes car il y a toujours manque de compétence en sécurité informatique.*
- *La faille de la mise en place des moyens de sécurité par contrainte de coût.*
- *Le non-suivi ou la non mise en œuvre de toutes les recommandations du rapport.*

L. Le schème provisoire de l'entretien

Nous allons tout d'abord restituer le schème en situant les arguments dans leur ordre d'intervention dans le récit et en les mettant en relation « spatiale » avec les deux autres classes d'unités précédemment recodées : les séquences et les actants. Nous allons les présenter dans ce tableau qui constituera un schème provisoire de l'entretien.

Séquences (Sn)	Arguments (Pn)	Actant (An)

Niveau de formation et progression de la carrière (S_0)	• J'ai fait une école de commerce à paris dans institue supérieur du commerce. (S1.1) • Ensuite, j'ai fait un DECF un diplôme de comptabilité. (S1.2) • J'ai commencé à faire ma carrière dans l'audit comptable dans cabine d'expertise comptable en audit externe et en suite j'ai rejoint la Banque populaire de Bourgain France compte en audit interne. (S1.3) • Et j'ai fait une mobilité group pour venir à la Banque populaire val de France toujours en audit interne. (S1.4) • J'ai cherché par internet pour la Banque populaire Bourgain franc compte et après c'est une mobilité. (S2.1) • J'ai fait une école de commerce de comptabilité sur l'entre an audit externe, c'est dans les cabinets d'expertise comptable donc j'ai fait l'audit. (S4.1)	• Si ton cv est organisé en Banque populaire régional et on peut changer de région donc j'ai changé de région donc j'ai fait une mobilité. (S2.2 et P2.1) • Mes missions d'audit sont variées. (P3.1) • Et j'allais voir les entreprises, mais j'étais externe de l'entreprise et du coup j'ai voulez faire de l'audit interne, un audit à l'intérieur de l'entreprise, mais c'été la suite logique de l'audit externe. (S4.2 et P4.1) • On peut travailler dans le commercial, dans le développement, donc une diversité de métier qui est proposé c'est ce qui m'a attiré dans le secteur bancaire. (P8.2) • Là c'est un choix familial en fait de rejoindre ma famille qui est cité dans une région dans l'appartement des avelines. (P9.1) • Donc la Banque populaire parce que c'est une banque mutualise qui respecte les valeurs humaines comme un demi-collaborateur. (P9.2 et A9.1)	• Le « Moi » et le « Je » qui réfère à Monsieur Thomas lui-même. • Ce n'est pas une immense machine, c'est une banque qu'a value l'humain. (A9.2) • Voilà pour la valeur, pour l'état humain et pour le rapprochement géographique familial. (A9.3) • C'est ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y a un système qui est développer par IBP. (A15.1 et P15.2) • C'est IBP qui protège tous or il y a des applications développer chez nous en interne donc ils ont recensé. (A15.2 et S15.2)
Fonction de chef de mission ne Audit : Rôle et missions (Sa)	• Ça peut être d'audit sur les fraudes, sur les check, sur la sécurité du système d'endogène. (S3.1) • J'étais intervenue également des audits sur le réseau multi marche donc audit d'agence. (S3.2) • Voilà, j'interviens en tant que chef des missions et du coup on doit élaborer un programme de travail qui identifie des risques préalables à mettre en place du contrôle.... (S3.3 et P3.2) • Mais nous on faisait plus des relations avec les auditée. (S6.5) • On fait un peu la bottelette, c'est eux qui faisaient l'investigation. (A6.3 et S6.6) • On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était une diversité de métier intéressant et une diversité d'opportunité également de carrière. (S8.1 et P8.1) • Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchies sur des améliorations sur le contrôle interne. (S11.1 et P11.1) • Donc c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque, c'est ce qui me valorise en gros. (S11.2 et P11.2) • Donc nous sur les audits bancaires, on se débrouille. (S17.2) • C'est à dire on a des compétences en interne pour faire nos audits surtout sur le domaine bancaire, protection	• En tant que chef de mission et du coup on doit élaborer un programme de travail qui identifie des risques préalables à mettre en place du contrôle pour valider le programme du travail…. (S3.3 et P3.2) • Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchies sur des améliorations sur le contrôle interne. (S11.1 et P11.1) • Donc c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque.... (S11.2 et P11.2)	• La rigueur, organisation, parce qu'il fait qualifié. (A5.1) • Empathie parce que il faut être d'ambiance comme même avec les auditée. (A5.2) • Capacité d'analyser des synthèses parce que il faut synthétise tous les travaux qui sont fait par les auditeurs donc il faut avoir une capacité pour synthétiser tous les problématiques relevés. (A5.3) • Prise de hauteur pour arriver à avoir prendre de la hauteur, prendre du reçus. En fait, on n'étudie pas point de taille mais avec ses points de taille il faut arrive à prendre de la hauteur pour synthétiser en fait pour voir les problèmes. (A5.4)

	clientèle, les contrats crédits, tout ce qui est risque bancaire. (S17.3)		
Cybersécurité : Contrainte et implication (Sb)	• Voilà ce genre des choses c'est vraiment la protection du système d'information pour éviter qu'il y a des intrusions. (P14.4 et S14.1) • Nous on n'intervient pas sur la sécurité de système d'information. (S6.1) • Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT. (P6.2 et S6.3) • En fait, on n'est des auditeurs généralistes de banque mais pas des auditeurs spécialisés des systèmes d'information, il y a des cabinée. (P6.3 et S6.4) • On n'a pas en interne donc on a fait appeler à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. (A7.1 et S7.2) • Tous ce qui développe des applications privatives dois prendre en compte cette impérative de sécurité quand il développe des applications privatives et faire une coordination avec le RSSI justement. (S19.1 et A19.2)	• Protection, contre des attaques externes sur le système d'information. (P14.1) • Protection des données également parce qu'on a des données des clients qui sont confidentielles, il faut qu'elles soient protégées. (P14.2) • Et également protection contre les attaques malveillantes et l'espionnage. (P14.3) • …la protection du système d'information pour éviter qu'il y a des intrusions. (P14.4 et S14.1) • Ce que je sais qu'avec le contrôle et les habilitations, c'est vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, qu'il avait regardé tous les dispositifs de contre de test d'intrusion pour voir si notre banque réalise bien de test d'intrusion. (S15.1 et P15.1) • On a les compétences en interne au niveau de la sécurité de système d'information qui est nouveau comme même une problématique intéressante on a pas d'auditeur spécialisé en ce système d'information. (S17.4 et P17.2)	• Là c'est le cabinet d'« ITEKIA » spécialisé en système d'information qui est venu chez nous, travailler en relation avec nous. (A6.2) • On fait un peu la bottelette, c'est eux qui faisaient l'investigation. (A6.3 et S6.6) • On n'a pas en interne donc on a fait appeler à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. (A7.1 et S7.2) • Qu'on a fait avec le cabinet « ITEKIA ». (A21.1 et P21.1)
Conséquence de la cybersécurité sur la banque (Sc)	• Oui effectivement il y a une deuxième personne et ça été une suite à notre mission qu'on a fait l'année dernière. (S18.1) • Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. (A18.2 et S18.2) • En fait c'est le résultat de l'audit qui a dit attention en demi et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevés c'est que justement le RSSI n'étais pas suffisamment proactif. (A18.3 et S18.3) • Et ça le cabine externe a trouvé que justement on ne prenait pas suffisamment compte la sécurité du système d'information pour développer des applications privatives. (A18.4 et S18.4) • C'est pourquoi la solution a été d'embauche un autre RSSI pour couvrir à temps complet. (A18.5 et S18.5)	• Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en termes de dispositif du contrôle de recrutement de RSSI. (S26.1 et P26.1) • Parce que c'est nouveau en fait la problématique de RSSI ce n'est pas tellement pris en compte jusqu'à présent mais il faut aller de plus en plus. (A26.2 et P26.3) • Nous on est en 3ième niveaux, nous ont vient vérifier. (P27.2) • C'est bien fait mais nous on intervient en 3ième rideau. (P27.3) • Donc, pour moi ce n'est pas notre rôle de maintenir tout seul la cybersécurité, c'est avec la direction des risques, c'est avec les autres services avec les services qui développe des applications, des services informatiques. (P27.4) • Donc il ne faut pas de collision entre guillemet, il faut qu'on soit disponible, professionnelle, à l'écoute il faut qu'on ne vaille pas trop parce qu'on vient déranger les gens dans le travail. (P29.2) • Oui, nous il nous manque les compétences internes parce que pour moi il faut des auditeurs spécialisés en système d'information. (P31.1 et S31.1) • Donc il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT. (P31.2)	• Mais pas dans notre service d'audit interne, je ne sais pas son poste mais ça peut être : RSSI responsable sécurité du système d'information. (A18.1 et P18.1) • En fait c'est le résultat de l'audit qui a dit attention en demi et parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevés c'est que justement le RSSI n'étais pas suffisamment proactif. (A18.3 et S18.3) • C'est le RSSI justement, et tous les services également en fait. (A19.1) • Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. (A18.2 et S18.2)

			• C'est pourquoi la solution a été d'embauche un autre RSSI pour couvrir à temps complet. (A18.5 et S18.5)
Travail relatif à la cybersécurité (Sd)	• Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI. (S26.1 et P26.1) • Et l'année prochaine, on fait des missions d'audit groupe donc qui vont être pilotée par des chefs de missions justement de l'informatique locale donc on va continuer à investiguer et faire des missions sur cette thématique pour la renforcer. (S26.2 et A26.1) • Parce que c'est nouveau en fait la problématique de RSSI ce n'est pas tellement pris en compte jusqu'à présent mais il faut aller de plus en plus. (A26.2 et P26.3) • Là justement On a demandé, il y a le rapport qu'on a fait l'année dernier avec les cabinets externes qu'il y a recrutement plus au niveau de RSSI. (S36.1) • Là c'est la direction des risques, elle est chargé de prendre à compte la recommandation sur le fait d'augmenter, les rejoint des moyennes allouer à la sécurité des systèmes d'information. (S37.1) • Donc ce qui affecte la direction des risques, c'est à eux de devoir mettre en œuvre les mesures, le plan d'action avec une date de séance. (S37.2)	• Chaque année on va avoir une mission à mener sur le système d'information je pense que ce n'est pas suffisant pour nécessiter. (P34.2) • Aujourd'hui en tous cas, ça ne semble pas suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission. (P34.3 et A34.1) • Je comprends il est en croissance mais le nécessaire chez nous est d'avoir un auditeur en temps plein c'est pour l'instant. (P35.1 et A35.1) • C'est ce que la banque est entraîné de faire de renforcer ses systèmes parce qu'il n'y a pas que des niveaux humains également contrer à la place. (P35.3 et S35.2) • Il faut que tous les services soient impliqués. (P35.3) • Mais déjà si en interne on arrive on a des failles, il faut les résoudre déjà avec les gens qu'on a remplacés et il n'y a pas de solutions qu'avec les recrutements externes pour régulariser ces problèmes. (S35.4 et P35.4) • Donc on est plutôt dans le sens il faut qu'on renforce, les moyens de sécurité à situer ont été plutôt dans l'aspect-là mais pas dans l'aspect des coûts. (P36.1) • Donc ils n'ont pas de liberté de prendre en compte la recommandation. (P37.1) • Il doit organiser sa journée, planifier ses rendez-vous, mener des entretiens, réaliser des tests pour vérifier tous ce qu'on lui a dit est correcte, synthétiser tous ce qu'on a dit pour rédiger un rapport. (A39.1 et P39.1) • Il ya des audités qui ont compris qu'on est là pour donner une valeur ajoutée et autre qui nous vois uniquement comme des gendarmes et qui ont peur. (A40.3 et P40.4)	• …c'est même le directeur général qu'à demander. (A23.1) • Mais ça dépend des audités. (A40.2) • Il y a des audités qui ont compris qu'on est là pour donner une valeur ajoutée et autre qui nous vois uniquement comme des gendarmes et qui ont peur. (A40.3 et P40.4) • Un programme de travail avec l'inspection générale de BPCE… (A38.1 et A38.2) • … faire attention à bien verrouiller nos ordinateurs etc. (A20.1 et S20.1) • Être vigilant sur nos codes, ne pas laisser trainer le mot de passe etc. (S24.3 et A24.1) • …l'auditeur adopte le comportement d'indépendance, pour moi c'est comme ça qu'on peut, il faut qu'on pas être en conflit interne. (A30.1 et P30.1) • Un auditeur généraliste aura du mal à évaluer la force, qualité de contrôle interne d'informatique s'il ne connait rien dans l'informatique. (A31.1

3. Production des catégories par l'analyse structurale

Notre travail présenté en ce qui précède était purement inductif. Nous allons maintenant dégager des unités de sens sur la base de notre description préalable et essentielle. Ces unités de sens sont appelées *« catégories sémiques »* selon Greimas qui sont constitutives de la logique sociale de l'entretien et de sa forme sémique.

Notre travail sera un travail démonstratif qui se reposera sur quelques principes de base qui constitueront une sorte de fonds communs de l'analyse structurelle. Conformément à notre projet de départ, nous sommes obligés de montrer la démarche en acte en introduisant des équivalents dans la littérature. Nous signalons les multiples choix sur lesquels repose la mise en œuvre de toute démarche d'inspiration structurale. Donc, notre mise en œuvre repose sur une intelligence préalable du discours que la partie précédente n'a que formaliser.

a. Disjonction et Conjonction

Nous allons considérer l'hypothèse de base de l'analyse est de traduire le schème précédent en une combinaison de catégories typiques constitutive du sens général de l'entretien.

Nous assumons que la révolution structurale consiste à analyser toute langue naturelle et tous ensemble signifiant comme un système d'opposition à l'intérieure d'une relation constitutive du sens. Nous s'occupons à des « éléments différentiels » ou des « traits distinctifs » qui assurent l'existence d'une langue. Donc, ce qui est vrai au sens lexical l'est aussi au sens sémantique.

Nous admettons que le sens linguistique d'un mot ne se comprend qu'en restituant la disjonction qui le spécifie et la conjonction qui lui assure son appartenance à une catégorie. La disjonction trouve son origine dans la chaine syntagmatique constitutive du signifiant et la conjonction de l'intégration paradigmatique définissant le signifié.

b. Application à l'entretien et à ses trois niveaux

i. La signification des séquences : l'opposition je sais/je ne sais pas

Thomas qualifie les expériences qu'elle a tiré des différentes phrases de son parcours au moyen d'expression souvent lapidaires :

(S1) : « Mes missions d'audit sont variées. » (§3)

(S2) : « on identifie des risques … » (§3)

(S3) : « Nous on n'intervient pas sur la sécurité de système d'information. » (§6)

(S4) : « Ce que je peux vous dire c'est qu'on a eu mission l'année dernière mais comme on n'est des auditeurs généralistes, on a dû faire appel à des cabinets externes. » (§6)

(S5) : « Parce qu'on n'a pas de compétence en informatique, notre service on n'a pas d'auditeur en IT. » (§6)

(S6) : « on est des auditeurs généralistes mais pas des auditeurs spécialisés des systèmes d'information... » (§6)

(S7) : « En interne chez nous, on n'a pas d'auditeur spécialisé en sécurité du système d'information. (§7)

(S8) : « On n'a pas d'auditeur qui soit spécialisé en informatique. » (§7)

(S9) : « pour voir si le système d'informatique est bien verrouillé, il faut certaine compétence d'informatique. » (§7)

(S10) : « On n'a pas en interne… on fait appel à des auditeurs spécialisés dans le système d'info pour nous aider à réaliser la mission. » (§7)

(S11) : « On a une diversité des missions intéressant à la fois sur commercial mais également plus de sécurité donc c'était une diversité de métier intéressant et une diversité d'opportunité également de carrière. » (§8)

(S12) : « Moi c'est plus qu'actuellement le fait de présenter nos travons à des directions et de les faire réfléchies sur des améliorations sur le contrôle interne. » (§11)

(S13) : « c'est pouvoir proposer des rapports avec des recommandations avec une valeur ajoutée pour la banque, c'est ce qui me valorise en gros. » (§11)

(S14) : « Ce que je sais qu'avec le contrôle et les habilitations, c'est vérifier qu'il y avait bien de système d'habilitation donnée au collaborateur de la banque, qu'il avait regardé tous les dispositifs de contre de test d'intrusion pour voir si notre banque réalise bien de test d'intrusion. » (§15)

(S15) : « C'est ce qui nous intéresse en fait c'est réussir à l'application privative parce qu'il y un système qui est développer par IBP. » (§15)

(S16) : « C'est l'application privative dans tous les services et ils ont fait des tests pour voir s'ils étaient bien verrouillés. » (§15)

(S17) : « Sur cette mission-là, la directrice de l'audit, l'ancienne directrice de l'audit qui est partie maintenant, elle avait choisi qu'on fait s'appelé à une cabine extérieure parce qu'elle considère qu'on a vais pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives. » (§17)
(S18) : « Et je pense qu'elle avait raison parce qu'on a vais pas tous les compétences requise pour par exemple faire des tests d'intrusion. » (§17)
(S19) : « On n'a pas les compétences en interne au niveau de la sécurité de système d'information qui est nouveau comme même une problématique intéressante on n'a pas d'auditeur spécialisé en ce système d'information. » (§17)
(S20) : « Ils ont pris la décision effectivement, ils ont considéré que, en fait G. intervenait en mi-temps sur ces parties là et ils ont trouvé que ce n'est pas suffisant. » (§18)
(S21) : « C'est le résultat de l'audit qui a dit attention parce que c'est aussi sur l'opérationnel, ce n'est pas suffisant pour couvrir tout cette partie-là parce que dans l'audit je ne l'avais pas dit qu'ils ont relevés c'est que justement le RSSI n'étais pas suffisamment proactif. » (§18)
(S22) : « C'est pourquoi la solution a été d'embauche un autre RSSI pour couvrir à temps complet. » (§18)
(S23) : « Tous ce qui développe des applications privatives dois prendre en compte cette impérative de sécurité quand il développe des applications privatives et faire une coordination avec le RSSI justement. » (§19)
(S24) : « Puis comme je vous l'avez dit tout à l'heure, dans la vie, tous les jours comme je vous l'ai dit, tout est concerner. » (§24)
(S25) : « Il y avait quelques points de faiblesse mais justement ce rapport a permis de commencer à améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI. » (§26)
(S26) : « pour moi ce n'est pas notre rôle de maintenir tout seul la cybersécurité, c'est avec la direction des risques, c'est avec les autres services avec les services qui développe des applications, des services informatiques. » (§27)
(S27) : « Oui, nous il nous manque les compétences internes parce que pour moi il faut des auditeurs spécialisés en système d'information. » (§31)
(S28) : « Un auditeur généraliste aura du mal à évaluer la force, qualité de contrôle interne d'informatique s'il ne connait rien dans l'informatique. » (§31)
(S29) : « il faut des auditeurs spécialisés, d'ailleurs si vous voyez dans les annonces souvent l'auditeur IT. » (§31)
(S30) : « Oui c'est ça, après il faut avoir des moyennes et puis il faut avoir l'envi de suffisamment mener une mission là-dessus vous savez c'est toujours l'histoire entre le besoin et le coût etc. » (§32)
(S31) : « Mais déjà si en interne on arrive on a des failles, il faut les résoudre déjà avec les gens qu'on a remplacés et il n'y a pas de solutions qu'avec les recrutements externes pour régulariser ces problèmes. » (§35)
Nous allons ici faire des hypothèses en restant le plus près possibles du texte retranscrit. Nous allons rétablir les oppositions entre unités de diverses séquences-types :

- Nos missions d'audit sont variées, On identifie tous les risques / Nous on n'intervient pas sur la sécurité de système d'information.
- Une diversité des missions, une diversité de métier intéressant et une diversité d'opportunité également de carrière / pour voir si le système d'informatique est bien verrouillé, il faut certaine compétence d'informatique qu'on n'a pas.
- On est des auditeurs généralistes/ pas des auditeurs spécialisés des systèmes d'information, on n'a pas d'auditeur en IT.
- Faire réfléchies sur des améliorations sur le contrôle interne, proposer des rapports avec des recommandations / Pas proposer des recommandations en sécurité informatique par manque de compétence.

- Réussir à l'application privative parce qu'il y un système qui est développer par IBP / on n'avait pas les compétences en interne pour vérifier qu'on n'a pas des failles au niveau des applications privatives, Pas de compétences requises pour par exemple faire des tests d'intrusion.
- Pas les compétences en interne au niveau de la sécurité de système d'information qui est nouveau comme même une problématique intéressante on n'a pas d'auditeur spécialisé en ce système d'information / le résultat de l'audit : d'embaucher un autre RSSI pour couvrir à temps complet.
- Rapport d'audit suggère d'améliorer des choses en terme de dis positive du contrôle de recrutement de RSSI et d'auditeurs spécialisés en sécurité informatique / Rapport pas totalement suivi contrainte de besoin et de coût.

L'opposition je sais/je ne sais pas concerne successivement ou simultanément toutes les catégories ou séquences citées (S0 à Sd). Thomas D. précise que le service d'audit interne est incompétent en cybersécurité. Il ajoute que le RSSI est responsable d'assurer la cybersécurité. Le résultat d'audit suggère l'embauche d'un deuxième RSSI pour couvrir tous les risques de la banque en sécurité informatique. Thomas insiste sur le recours au cabinet externe « ITEKIA » en cas de mission d'audit sur les services informatiques car il y a manque de compétences techniques et manque de compétence de réussir à l'application privative. Le service d'audit ne sait pas vérifier le système développé par l'I-BP. Enfin, le rapport d'audit n'a pas totalement été suivi pour embaucher des auditeurs internes spécialistes en IT par contrainte de besoin et de coûts.

ii. La signification des actants : pareils/pas pareils et mieux/pire

Nous allons procéder de la même façon pour les actants du récit de Thomas.
Nous résumons dans ce tableau ci-dessous les acteurs pareil et pas pareil à Thomas D.

Pareil	Pas Pareil
Chefs de missions (A2)	Cabinet extérieur « ITEKIA » (A4)
Auditeurs Internes (A3)	I-BP (A6)
BPVF (A5)	RSSI Didier G. (A8)
Agnès Bayard (A7)	Nouvelle RSSI embauché pour aider Didier G. (A9)
Directeur Général (A10)	La direction des risques (A14)
Les audités (A11)	
L'inspection générale (A12)	
Les employés (A13)	

Nous pouvons maintenant analyser le sens de l'opposition Pareil/Pas Pareil en retrouvant les catégories associant la conjonction de deux termes. Nous vérifions que pour Thomas D., sont pareils ceux qui n'ont pas les expertises et les connaissances techniques en cybersécurité, et pas pareils que lui, ceux qui ont les compétences techniques en cybersécurité. Pour Thomas le mieux sera que la cybersécurité soit une préoccupation de tous, que le RSSI coopère avec les autres employés pas seulement les experts et les cabinets externes, qu'il coopère aussi avec les auditeurs internes. Le pire c'est de laisser le RSSI seul responsable d'assurer la cybersécurité dans la banque. Thomas signale qu'il est nécessaire à tous les employés de protéger leurs données informatiques. (Mots de passes, ordinateurs…) Le pire c'est d'avoir un conflit interne entre les auditeurs internes et les employés en termes de sécurité informatique. Aussi, le pire est de ne pas exécuter les points d'amélioration du rapport d'audit comme l'embauche d'auditeurs

spécialisés à temps plein par contrainte de besoin et de coûts. Il faut en interne que l'auditeur interne spécialisé résous des failles en sécurité informatique pas avec des cabinets externes. De même, le pire c'est de ne pas avoir les compétences en interne pour appliquer les applications privatives développées par I-BP. Ces applications vérifier par le cabinet externe « ITEKIA » protègent la sécurité informatique de la banque.

iii. La signification des arguments : Facile/Pas facile

Thomas annonce qu'il y a un manque d'auditeur interne spécialisé dans le service d'audit. Ceci leur empêche de vérifier les applications privatives développées par I-BP et de ne pas intervenir sur les missions d'audit sur le département informatique.

Il assure que les auditeurs internes ne sont pas spécialistes en sécurité informatique, ils ont un manque de compétence en sécurité informatique. Mais, il oppose son discours en disant :

- Qu'il réalise des missions d'audits variés sur tous les services de la banque. Mais il ne réalise pas de mission sur le service d'informatique pour manque de compétences.
- En disant que la cybersécurité est la préoccupation de tous et il faut protéger nos données et nos informations mais en disant que c'est une responsabilité autonome du RSSI.
- En disant qu'il est généraliste et identifie tous les risques, mais dans le cas de la cybersécurité, un risque majeur, ce sont des expertises qu'il n'a pas, on n'intervient pas sur le service de sécurité informatique. La banque fait recours au cabinet externe « ITEKIA » expert en sécurité informatique.
- En disant qu'il y a besoin d'embaucher des auditeurs internes spécialisés en IT ou sécurité informatique. Mais, ce n'est pas possible par contrainte de besoin et de coût. (Il n'est pas suffisant d'avoir un auditeur à temps plein spécialisé pour une seule mission, c'est coûteux.)

Nous analysons ces oppositions pour trouver la totalité qui donne sens à ces couples, découvrir la conjonction qui englobe cette disjonction.

c. La structuration de l'univers sémantique et la logique du récit

Rappelons les résultats acquis à ce stade de l'analyse. Une première opposition je sais/je ne sais pas structure les séquences de Thomas. Nous l'avons décomposée selon trois propriétés combinées qui permettent de qualifier les renseignements de cybersécurité dans la banque :

- Je ne sais pas = Pas de compétence technique informatique + Pas réussir à l'application privative + recours à un cabinet externe « ITEKIA »
- Je sais = Compétence technique spécialisé en informatique + Auditeur interne spécialisé + Réussir à l'application privative + Assurer la cybersécurité

Une seconde opposition pareil/pas pareil structure les segments du récit qui mettent en scène des actants de la vie de Thomas D. Nous en avons trouvé deux propriétés principales qui permettent de qualifier les significations d'une autre « totalité » que l'on peut appeler statut :

- Pareil=Pas d'expertise+Pas de responsabilité + Pas d'ordonnance de recommandations
- Pas pareil= Expertise technique+Responsabilité de cybersécurité + Ordonnance de recommandations

Une autre opposition a été introduite pour rendre compte de la structuration du récit des actants : mieux/pire, qui renvoie à une autre « totalité » qu'il faut y avoir une collaboration pour réduire les failles et les cybers attaques.

Une troisième opposition nous a permis de structurer la narration de Thomas D. et de qualifier la relation précédente facile/pas facile. Nous allons extraire donc les propriétés suivantes :

- Facile=expertise technique+compétence technique en SI+recommandations
- Pas Facile=Incompétent domaine informatique+Contrainte du coût+Contrainte de Besoin

Nous allons terminer notre analyse par-là construction d'axes croisés permettant d'attribués des propriétés identiques à plusieurs significations dégagées antérieurement. Nous proposons pour l'entretien de Thomas D. les schémas suivants :

Tableau 1. Situation et perspectives professionnelles de Thomas

	Positives (Je sais)	Négatives (Je ne sais pas)
Possible (Facile)	Préoccupation de tous et du RSSI	Cabinet Externe « ITEKIA »
Impossible (Pas Facile)	Embauche des auditeurs internes spécialisés en sécurité informatique et coopération avec le RSSI (Réalisent des missions sur le SI et en donne des recommandations, réussir à l'application privative. développée par l'I-BP)	Ne pas suivre les recommandations du rapport d'audit par contrainte de besoin et de coût. Conflit entre le RSSI et les employés relatifs à la réussite de l'application privative.

Tableau 2. Personnages propre et perspectives professionnelles de Thomas

	Semblables (Pareil)	Différents (Pas Pareil)
Positives (Mieux)	Auditeurs internes, Directeur générale, Directeur de l'audit, Chefs de missions	Cabinet externe « ITEKIA », I-BP
Négatives (Pire)	Employés, clients, Audités	RSSI, seul responsabilité

B4. Méthodologie de codage du guide d'entretien du superviseur de l'audit interne à la BPVF

Le codage du Guide d'entretien du superviseur de l'audit interne

Nous commencerons l'analyse par un repérage des niveaux du discours considéré comme un récit. Selon Roland Barthes, tout récit peut être analysé selon trois niveaux correspondant à trois lectures différentes mais nécessairement articulées :

- Le niveau des fonctions est celui auquel se déploient les épisodes du récit que nous appellerons des séquences. Nous les numéroterons par (S). Ces séquences racontent le parcours d'Anne-Laure dans la banque.
- Le niveau des actions concerne les éléments du récit qui mettent en scène des « actants », c'est-à-dire des personnages qui agissent, interviennent, jouent un rôle dans le récit. Nous numéroterons tous les éléments de l'entretien comprenant de tels indices d'actant par (A).
- Le niveau de la narration se repère par la présence de thèses, d'arguments, de propositions destinées à nous convaincre, à défendre son point de vue. Nous noterons ces parties de l'entretien par (P).

Premier codage de l'entretien

35 questions = 35 séquences

Codage du Segment 1 (δ1) :

« Moi, j'ai fait des études, j'ai passé comptable, donc j'ai une formation comptable, je suis expertise comptable en fait. » (S1.1)

« Avant d'être expertise comptable, j'ai réalisé un Bac+4 en comptabilité. » (S1.2)

« Le travail actuel ? Je suis sortie de mes études, j'ai fait une mission d'intérim où je suis arrivé par hasard au milieu bancaire. » (S1.3 et P1.1)

« Ce n'était pas un choix de ma part, donc j'ai tombe dans une première banque mais pas la banque populaire. » (S1.4 et P1.2)

« Quand même pour vous préciser, j'ai 49 ans, ça fait 26 ans je travaille dans les banques. » (S1.5)

« C'est plusieurs banques dans mon passée, et donc la première banque je suis arrivée par hasard. » (S1.6 et P1.3)

« Et, donc, je suis arrivé dans une première banque qui s'appelait Fortis Banque, que vous ne connaissez peut-être pas, je suis resté une dizaine d'année. » (S1.7)

« Je suis arrivé dans le groupe BPCE en 2001, et après, à force de contacte et de réseau, j'ai commencé par un contrat BPCE S1. » (S1.8 et P1.4)

« Et je suis arrivé actuellement dans la BPVF, je suis arrivé, sans dire de bêtise, attendez, en 2003. Excusez-moi, en mai 2009. » (S1.9)

Codage du Segment 2 (δ2) :

« Actuellement, je travaille à l'audit. Je suis superviseur à l'audit. » (S2.1)

« Donc, vous avez eu faire ça avant avec mon directeur d'audit Monsieur Manuel Couillet. » (A2.1)

« Et donc, mon rôle en tant que superviseur, c'est de coordonner les équipes, donc, d'animer les missions d'audits que nous réalisons, de coordonner les équipes, de les animer, de les amener au niveau attendu. » (S2.2 et P2.1)

« C'est-à-dire, à l'audit, nous avons une méthodologie qui est très évidente, et des profondes d'habilitations qui sont déjà définis à l'avance, et qui nous demande, nous avons un minimum de cas inspecté. » (S2.3 et P2.2)

« Donc, mon rôle c'est d'animer cette équipe pour que les travaux soient accomplis avec la qualité attendue en quantité et en qualité je voudrai dire. » (S2.4)

« En fait, sur l'assurance que les missions sont bien prémunis dans la banque dans leur contenu et réaliser dans les délais qui nous sont donné. » (S2.5)

« Parce que nous avons à faire l'audit en 4 ans à réaliser et il faut que toutes les missions soient renouvelées. » (P2.3)

« C'est pour dire que cette mission qui était prévus en début d'année nous ne la faisons pas. » (P2.4)

« Et donc, mon rôle est de saturer que tout est fait en temps parfait. » (S2.6)

Codage du Segment 3 (δ3) :

« Alors j'ai bien commencé comme je vous l'ai dit en milieu comptable. » (S3.1)

« Donc, j'ai fait 25 ans tous les métiers comptables, possible imaginable au sein de la finance, et je suis arrivé à la banque populaire Val de France en tant que responsable de la révision comptable. » (S3.2)

« Et au bout de 5 an, j'ai évolué vers un poste de superviseur par hasard, on va dire c'est pareil, j'ai vu l'annonce proposé, et je me suis dit naturellement ce sont des métiers de contrôle, thématique indifférente, mais ce sont des métiers un peu près similaires, » (S3.3 et P3.1)

« Donc je me suis dit c'est le moment de changer, et puis élargir sa vision dans le sens de sortir de la comptabilité pour savoir tous les aspects de la banque. » (P3.2)

« Puisque dans l'audit, nos audits ils n'ont pas la comptabilité, mais nous auditons de toute façon toutes les services de la banque. » (P3.3)

« Je suis arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé. » (S3.4 et P3.4)

Codage du Segment 4 (§4) :

« Rigueur, agilité, beaucoup d'ouverture d'esprit. » (P4.1)

« Si on a un problème, on trouve une solution rapidement. » (P4.2)

« Et jamais ne se perdre non plus, il faut toujours garder l'esprit qu'on est là pour préserver les intérêts de la banque puisque nous nous sommes amenées à mettre à jour les risques et de découvrir les risques, et de détecter les risques pour le directeur général qui est notre principal client. » (A4.1 et P4.3)

« Il faut arriver à conserver l'esprit d'équipe parce qu'on est une équipe de plusieurs auditeurs. » (P4.4)

« Et il faut arriver à satisfaire tout le monde. » (P4.5)

« Il faut arriver à préserver les intérêts des auditeurs, et préserver les services que nous auditons. » (P4.6)

« C'est un rôle un peu diplomate entre guillemets. En France, il faut arriver à contenter les intérêts de tout le monde. » (P4.7)

Codage du Segment 5 (§5) :

« En termes de SSI, ce n'est pas notre confort, c'est vraiment un métier très spécifique. » (P5.1)

« Ce sont des expertises que nous n'avons pas forcement, donc, il y a rien à réaliser des missions sur les SSI. » (P5.2)

« Nous avons fait appel à un cabinet extérieur pour connaitre ses limites. » (A5.1)

« Nous, nous sommes des gens qui sont généralistes et la plupart des temps, on est curieux. » (P5.3)

« On a des méthodes pour apprendre des sujets qu'on ne connaît pas, les SSI par exemple, c'est un vrai métier. » (P5.4)

« Par contre, moi, j'ai une sensibilité sur tout ce qui est environnement informatique. » (P5.5)

« Donc, c'est en cas d'application que moi je n'ai pas mal de connaissances, sur toutes les applications, des différents métiers de la banque. » (P5.6)

« J'ai quand même cette sensibilité contre les sujets qui ne sont pas connus. » (P5.7)

« Je connais seulement l'importance de ces sujets, et je rappelle régulièrement tout le monde. » (S5.1)

« Et après, je suis moins expert en ce métier. » (P5.8)

« Je sais vous avez interviewé Didier G., ils ont embauché un expert là-dessus. » (A5.2)

« En tout cas, ce sont des problématiques que nous avons en tête, dont nous connaissons l'importance. » (P5.9)

Codage du Segment 6 (§6) :

« Par hasard au départ, c'est le hasard, l'opportunité. » (S6.1)

« Et, je vais dire que maintenant j'y reste parce que je trouve que c'est un milieu en mouvement, c'est un milieu qui évolue, qui va changer, donc il y a plein de métiers intéressants qui n'existent pas forcement encore, ça laisse beaucoup d'opportunités de carrière. » (S6.2 et P6.1)

« C'est un milieu que j'aime bien, je ne vois pas changer de milieu de travail. » (P6.2)

« Je resterai dans la banque le plus long possible. » (P6.3)

Codage du Segment 7 (§7) :

« Banque populaire Val de France. Moi, je suis attaché au milieu mutualiste. » (S7.1)

« Donc, c'est une banque qui me plait. » (P7.1)

« Ce sont les valeurs mutualistes qui me plaisent, et donc, je me n'en verrai pas allez dans une autre banque, société générale ou … » (P7.2)

« C'est à cause du côté mutualiste que je suis là, je reste attachée à la banque, je suis fidèle. » (P7.3)

« Donc, je suis une collaboratrice fidèle aux valeurs de la banque, et à la banque elle-même, je suis fidèle à mon employeur. » (P7.4)

« Donc, je ne me vois pas allez ailleurs dans une autre banque. » (P7.5)

Codage du Segment 8 (§8) :

« Oui, une banque, c'est-à-dire un client. » (A8.1)

« Toutes les banques ont des clients. » (A8.2)

« On a le même régulateur au-dessus qui gèrent les banques auxquels nous devront rendez compte. » (P8.1)

« Oui, ce que soit cette banque ou une autre, ce n'est pas par parce j'aime les valeurs mutualistes dans une banque que je ne vais pas allez dans une autre banque. » (P8.2)

Ça sera juste un choix de ma part de rester dans cette banque. » (P8.3)

« Ce qui pourra par ailleurs me bloquer, c'est que je ne pars pas assez couramment et qui pourrai me bloquer des perspectives en d'autres comptes qui seraient relation avec les banques. » (P8.4)

« Mais, sinon, le métier est le même d'une banque à l'autre. » (P8.5)

Codage du Segment 9 (§9) :

« Les deux. C'est l'ensemble des choses. » (P9.1)

« On va dire la passée c'est plutôt la rigueur, c'est dans ce cas où je me dis que mon passée me sert beaucoup. » (P9.2)

« Par contre il faut savoir inventer tous les jours, c'est plutôt le présent qui fait que je me contrôle moi-même chaque jour au quotidien. » (P9.3)

« Donc, il faut être curieux. » (P9.4)

« A l'audit, nous avons la chance de découvrir plein de sujets que nous ne sommes pas experts en au départ. Ça nous donne l'occasion d'appréhender de nouveaux sujets. » (P9.5)

Codage du Segment 10 (§10) :

« Ahhhhh ! C'est une bonne question. » (P10.1)

« Pourquoi je travaille ! Parce que j'aime bien travailler déjà, et j'aime bien découvrir de nouveaux choses, de nouveau challenges, apprendre à assez évoluer avec mon environnement. » (P10.2)

« Et, c'est déjà aussi avoir des relations humaines tous les jours. » (P10.3)

« Moi, j'ai une équipe à gérer. » (S10.1)

« C'est-à-dire avoir des relations avec mon équipe, avec les équipes extérieures auxquelles nous avons audités. » (S10.2)

« C'est recouru à l'argumentation, ça nous mettent en contact avec le monde extérieur. » (P10.3)

« Moi je suis active, et j'aime mon travail et je veux continuer à travailler, à progresser. » (P10.4)

Codage du Segment 11 (§11) :

« Oui, oui, on a plus de 2000 salariés. 2050 l'année dernière, oui. » (P11.1)

« Je ne sais pas combien il y a de services exactement, je peux vous dire qu'il y a un peu plus que 200 agences, mais au nombre de services, je ne peux pas vous dire exactement combien, mais je connais assez bien l'environnement de notre banque, en tout cas, ça nous fait exactement beaucoup de contacts avec énormément de mondes. » (P11.2)

« Ce qui importe c'est un sous-jacent qu'on connait bien la banque. » (P11.3)

« Nous ne sommes pas dans une tour d'histoire, on est en contact avec tout le monde, on est énormément de relation qui ne se passe pas forcement dans toutes les banques. » (S11.1)

« Dans ce cas, l'audit chez nous est en relation, on très bien enserré dans le dispositif de la banque. » (P11.4)

« Nous sommes au contacte, moi je communique énormément avec tout le monde, j'ai normalement de relations avec tout le monde, j'écoute les problématiques des uns les autres, ce qui peut nous aider aussi dans notre métier. » (S11.2)

Codage du Segment 12 (§12) :

« C'est le danger numéro 1 on va dire. » (P12.1)

« Pour moi, c'est le danger numéro 1 dans les entreprises actuellement. » (P12.2)

« Et puis, c'est un risque qui s'est largement sous-estimé parce que ça coûte cher. » (P12.3)

« Et que déjà, c'est un nouveau risque, et ça va mettre du temps à appréhender. » (P12.4)

« Et pour moi c'est un danger, un vrai danger, un danger qui doit être une préoccupation pour toutes les entreprises au-delà les banques. » (P12.5)

Codage du Segment 13 (§13) :

« Non, je n'ai pas les compétences. » (P13.1)

« C'est par contre en employant un cabinet, je pourrai faire des liens entre un cabinet, et lui apporté le lien entre les connaissances métier et les problématiques de cyber sécurité. » (P13.2 et A13.1)

« Mais, en tout cas, moi je n'ai pas les compétences à mon niveau. » (P13.3)

Codage du Segment 14 (§14) :

« Au sein de la banque, j'ai l'effet d'avoir des gens qui ont des connaissances et des préoccupations en informatique mais je dirai au sens large. » (S14.1 et P14.1)

« Et de mettre à jour le problème, ça veut dire qu'à l'instant, c'est un sujet, jusqu'à un an, qu'on ne se préoccupait pas du tout au sein de la banque. » (S14.2)

« Maintenant, depuis un an, les choses ont changé, ils ont embauché quelqu'un qui devra arriver. » (P14.2)

« Je pense qu'ils vont être amenés de plus en plus à contrecarrer, on va subir des attaques comme beaucoup d'établissements a d'autre. » (P14.3 et S14.3)

« Pour moi, c'est un nouveau sujet. » (P14.5)

« C'est un nouveau sujet pour nous, il faut savoir à mettre en compétences. » (P14.6)

« Il y a très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n'avons pas pour l'instant chez nous. » (P14.7)

« Ce qui sensibilise l'informatique, ce sont des profils très rares » (P14.8)

« Et dans les banques, ce ne sont pas les profils majoritaires pour l'instant. » (P14.9)

« Il y a très peu de gens qui connaissent ce sujet. » (P14.10)

Codage du Segment 15 (§15) :

« Je ne sais pas. » (P15.1)

« J'ai juste entendu qu'on allait renforcer le sujet. » (S15.1)

« Voilà, après son poste, je ne pourrai pas vous le dire. » (P15.2)

« La nouvelle personne va arriver chez Didier G. pour collaborer avec lui. » (A15.1 et P15.3)

« C'est un côté positive qu'on a clairement conscience qu'on a besoin d'une autre personne. » (S15.2)

« On ne peut pas être généraliste sur un sujet pareil. » (P15.4)

Codage du Segment 16 (§16) :

« Il faut qu'il y ait l'expert. » (A16.1)

« Mais, c'est l'affaire de tous, il faut que ce soit une préoccupation de tous. » (P16.1)
« Il faut changer la mentalité, il faut éviter les comportements à risque. » (P16.2)
« Pour moi, c'est une préoccupation de tous, parce qu'on peut tous se faire attaquer si on prend des risques. » (P16.3)
« On peut prendre des risques, et on peut laisser les portes ouvertes, pour s'attaquer. » (P16.4)
« Clairement, mais pour ça il faut animer le sujet, il faut que les gens prennent conscience que c'est un danger. » (P16.5 et S16.1)
« Et le danger peut venir de partout. » (P16.6)
« On est 2000 collaborateurs au sein de la banque, c'est facile d'y trouver une faille pour entrer dans la banque. » (S16.2)
« Voilà, pour moi, c'est l'affaire de tous. » (P16.7)
« Il faut du travail. » (P16.8)
Codage du Segment 17 (§17) :
« Oui, on a des formations, ce n'est pas en cyber sécurité exactement, c'est plus. » (S17.1)
« On sait que ça existe, on dit qu'il y a des risques, on a des animations, ce n'est pas au sens propre. » (S17.2 et P17.1)
« Ce ne sont pas des formations en cyber sécurité à mon sens. » (P17.2)
« Voilà, ça commence à monter que c'est un sujet qui porte des risques. » (S17.3)
« On part de loin. » (S17.4)
« On commence à faire prendre conscience aux gens que c'est un sujet qui a des risques informatiques, qu'il faut faire attention à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. » (S17.5)
« Pour moi, c'est bien ce qu'on fait. » (P17.3)
« Et que tout le monde soit expert sur le sujet. » (P17.4)
« On a la formation, on a forme, puisqu'on nous forme sur le sujet. » (S17.6 et P17.5)
« C'est de la formation, une prise de connaissances, on fait progresser les gens sur ce sujet. » (S17.7 et P17.6)
« La cybersécurité, c'est un vaste sujet, que personne, à l'instant, il y a peu de gens qui savent ce qui montre ce sujet. » (P17.7)
Codage du Segment 18 (§18) :
« Ahhhhh ! Oui. Oui. Ça c'est une vraie préoccupation maintenant. » (P18.1)
« Ils ont pris conscience. » (S18.1)
« Au niveau de la direction générale, il y a aucun sujet. » (S18.2)
« Moi, je crois qu'ils ont pris conscience du danger. » (P18.2)
« Après entre prendre conscience et trouver les bons moyens, trouver vite les moyens, ça va être plus compliqué de mettre en œuvre les moyens. » (S18.3)
« Ça coûte cher et ça prend du temps. » (P18.3)
« Mais, nous prenons conscience, ça fait sûre. » (S18.4)
Codage du Segment 19 (§19) :
« Dans nos audits, au quotidien, je veux dire en termes d'application interne, parce que le développement nous avons beaucoup d'assez questions informatiques. » (S19.1 et P19.1)
« Ils sont développés par notre prestataire informatique, et donc I-BP. » (A19.1)
« Et nous avons aussi beaucoup d'application informatique privative. » (S19.2)
« C'est comme ça. » (P19.2)

« Ces applications là nous donnent nos audits que nous allons auditer un procès ou un service, nous faisons la revue de toutes les applications. » (S19.3)

« Donc, quelque part, si on voit des failles en termes d'habilitation ou d'application qui sera un peu à la dérive ou isolé dans son coin. » (S19.4)

« Nous avons moyen d'attirer l'attention sur ces applications-là. » (S19.5)

« Il faut dire attention. » (P19.3)

« Il faut appeler un expert sur le sujet pour savoir s'il y a une faille ou pas. » (P19.4)

« En tout cas, une faille la répertorier rendent en procès quelle type d'application. » (P19.5)

« On peut avoir notre rôle à jouer en termes de détection d'application un peu orpheline dans certains services. » (P19.6)

Codage du Segment 20 (§20) :

« Oui. Pour moi, oui. » (P20.1)

« De toute façon, nous embauchons dans le monde de banque, il y a beaucoup de jeunes qui sont embauché, beaucoup de personnes qui partent en retraite. » (S20.1)

« Et de toute façon, il y a beaucoup de jeunes qui arrivent chaque année. » (S20.2)

« Pour tous ces nouveaux, il faut bien les former. » (P20.2)

« Et même, pour les anciens, il ne faut pas relâcher la caution. » (P20.3)

« Je pense qu'il faut y avoir… » (P20.4)

« C'est de tous les moments, il faut rappeler que c'est important, d'appréhender le risque. » (P20.5)

« Si on ne rappelle pas régulièrement, les hackers sont de plus en plus imaginatifs, pour faire du phishing et c'est la première faille. » (A20.1)

« Pour moi, les hackers sont toujours en avance de tout le monde. » (A20.2)

« Donc, il ne faut pas sous-estimer leurs forces. » (A20.3)

« Il faut y avoir une prise de conscience de ça. » (P20.6)

« Et plus on les informe rapidement, voilà, pour moi, il faut communiquer et être former. » (S20.3 et P20.7)

Codage du Segment 21 (§21) :

« Le seul fait était lorsqu'on fait la mission l'année dernière. » (S21.1)

« On a envisagé un expert métier, un cabinet spécialisé. » (A21.1)

« De toute façon, nous embauchons dans le monde de banque, il y a beaucoup de jeunes qui sont embauché, beaucoup de personnes qui partent en retraite. » (S21.2)

« Et de toute façon, il y a beaucoup de jeunes qui arrivent chaque année. » (S21.3)

« Et plus on les informe rapidement, voilà, pour moi, il faut communiquer et être former. » (S21.4 et P21.1)

« Le seul fait était lorsqu'on fait la mission l'année dernière. » (S21.4)

(A21.2)

« Donc, on les a assistés, on a participé avec eux dans leurs missions. » (A21.3 et S21.2)

« Après notre rôle était de coordonner, de sert en sorte d'interlocuteurs, pour faciliter leurs missions. » (S21.5)

« Après, en termes d'expertises, on n'a pas l'expertise, on les a laissés à leurs métiers et on a fait en sorte que les gens se comprennent. » (P21.2)

« La cyber sécurité, c'est un métier, une façon de se parler, de s'exprimer. » (P21.3)

« Mais l'informatique, nous avons essayé de mettre en correspondance les demandes des uns avec les réponses des autres, et de faire en sorte, que tout le monde se comprenne. » (P21.4)

Codage du Segment 22 (§22) :

« La démarche, c'est que nous avons un plan d'audit, sur 4 ans, ça fait partie des risques qu'on n'avait pas encore audité. » (S22.1)

« La démarche, c'est que nous avons un plan d'audit, sur 4 ans, ça fait partie des risques qu'on n'avait pas encore audité. » (S22.2 et P22.1)

« Et donc, on a amené ce cabinet. » (A22.1 et S22.3)

« Je pense, je ne peux pas vous dire, je n'ai pas participé au choix du cabinet, ma direction je pense qu'ils ont dû avoir un choix de plusieurs personnes, de plusieurs cabinets. » (S22.4 et P22.2)

« Et voilà, donc, s'il demande de la banque, et aussi par rapport au groupe, c'est-à-dire que ce cabinet-là, nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP. » (S22.5 et A22.2)

« Les prestataires informatiques, on sentait qu'on avait besoin, on les a fait venir. » (A22.3 et P22.3)

« Ils ont travaillé. » (A22.4)

« Et le but était que les failles qui étaient identifiées puissent être corrigées. » (S22.6)

« Et pour le compte de la communauté de la banque populaire, c'est-à-dire nous avons mis à jour des constats. » (S22.7)

« I-BP les a corrigés mais ne les a pas corrigées que dans notre établissement. » (A22.5)

« Il ne les a corrigés pour les autres banques populaires, c'est aussi la démarche. » (S22.8)

« Voilà, on a fait participer un cabinet au bénéfice du groupe. » (A22.6)

« Et c'était à notre demande en tout cas. » (S22.9)

Codage du Segment 23 (§23) :

« Non, pour moi non. » (P23.1)

« Parce que l'audit n'a pas de compétence métier. » (P23.2)

« On n'est pas expert. » (P23.3)

« Je disais tout à l'heure que les auditeurs sont généralistes et on n'a pas de compétence, il faut vraiment… » (P23.4)

« La cybersécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue. » (P23.5)

« Comme je vous le dit pour moi, les hackers entre guillemets, sont très inventifs, très très rapides, très très compétents. C'est un métier qu'on ne peut pas suivre. » (A23.1)

« Il faut quelqu'un qui soit dédié à ça. » (P23.6)

« Nous, on en peut pas suivre, on n'a pas les compétences en tout cas. » (P23.7)

« Par contre, on peut participer au processus d'alerte et de maintien. » (P23.8)

« Pour moi, le risque de cyber sécurité, c'est un risque qui est important. » (P23.9)

« Par contre il y a plein de risques dans la banque dont nous devons être prémunis aussi. » (P23.10)

« C'est un risque très très technique, compliquer à cerner. » (P23.11)

Codage du Segment 24 (§24) :

« Oui. Oui. » (P24.1)

« Selon moi, le RSSI c'est son travail. » (P24.2 et A24.1)

« Il est bien l'expert. » (A24.2)

« Comme je vous l'ai dit, il y a une nouvelle personne qui est venu qui a des compétences techniques en plus. » (P24.3)

« Donc, c'est clairement la position de la banque de ne pas laisser la faille arriver. » (S24.1)

« Moi, je pense que l'expertise doit rester là où elle est actuellement, il renforce le travail informatique. » (P24.4)
« C'est le meilleur endroit où ça peut être. » (P24.5)
« Et en plus dans la banque, il est au sein du service, il est en contact avec tout le monde. » (A24.3)
« Donc, il garde sa position pour animer le sujet, il faut qu'il puisse être en contact avec tout le monde. » (A24.4)
« Je pense que c'est la meilleure position, à mon sens, c'est très bien qu'il soit là-bas. » (A24.5 et P24.6)
Codage du Segment 25 (§25) :
« Pour moi de toute façon, au sens large, l'audit interne est réglementaire. » (P25.1)
« Donc, toutes les banques ont forcément… » (S25.1)
« Le régulateur c'est la BCE… » (A25.1)
« Vous aurez de l'audit interne dans toutes les banques. » (S25.2)
« Ça ce n'est pas négociable. » (P25.2)
« Par contre, pour la cybersécurité, toutes ces thématiques, nous avons au niveau de l'audit interne, un budget chaque année, que nous pouvons utiliser pour faire appel à des prestataires externes sur des spécificités ou expertises techniques que nous n'aurions pas dans notre collaborateur. » (S25.3)
« Voilà, typiquement, la cyber sécurité en fait partie. » (S25.4)
« Si nous n'avions pas de comptable, peut être que nous aurions faire appel à des prestataires pour nous faire des missions comptabilité. » (S25.5)
« Ça va dépendre des profils des collaborateurs de notre équipe d'audit. » (S25.6)
« Or je vais vous dire que si ça se trouve, certains établissements qui ont des compétences techniques informatiques dans la sécurité, ne font pas forcement appel à un prestataire externe, peut être qu'ils ont des compétences. » (S25.7)
« Après c'est compliqué… » (P25.3)
« Nous avons des budgets pour recourir à des prestataires externes. » (S25.8)
« Si on peut faire des missions en internes, on les fait. » (S25.9)
« Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes. » (S25.10 et A25.2)
Codage du Segment 26 (§26) :
« L'auditeur interne a toujours le même processus. » (A26.1)
« Avant d'entrer sur un sujet, je vous rappelle qu'il est généraliste. » (A26.2)
« Donc, c'est un sujet qu'il ne connait pas forcement. » (A26.3)
« Donc, on commence par faire un programme de travail, définissions toutes les thématiques que nous allons traiter. » (S26.1)
« Ça c'est l'auditeur qui va traiter. » (A26.4)
« Moi, en tant que superviseur, je valide avec lui, et nous faisons valider avec notre directeur d'audit. » (S26.2 et A26.5)
« Et après, nous définissons les questions et les thématiques, un peu comme vous. » (S26.3)
« Vous avez une prise de questions. » (S26.4)
« Donc, après, une fois qu'on a défini les questions et les thématiques que nous voulons avoir traité, nous allons faire des entretiens avec les audités. » (S26.5 et A26.6)
« Donc, évidement, ils ont plein de questions, et ils vont commencer à appréhender les autres risques. » (A26.7)
« Charge à nous après, de récupérer les documents pour valider et pour projet ce que les audites nous ont annoncé mais de façon orale. » (A26.8 et S26.6)
« Donc, on a toujours cette démarche d'aller vérifier et de garder preuve de ce qu'on nous dit. » (S26.7)

« Et donc, avec tout ça, avec ces documents, entre les questions, nous apportons des réponses à nos questions, et nous identifions les risques. » (S26.8)

« Donc, il est censé de ne pas avoir a priori l'auditeur. » (A26.8)

« L'auditeur est ponctuel. » (A26.9)

« Les constats que nous mettons à jour, on ne peut pas les opposés. » (P26.1)

« Ce sont des constats avec des preuves. » (S26.9)

« Ils ne sont pas opposables. » (S26.10)

« Et donc, nous allons en fin de mission, de toute façon, allez expliquer nos constats aux audités. » (S26.11 et A26.10)

« Nous allons leur faire adhérer à nos constats puisque c'est toujours la démarche de l'audit de faire adhérer les constats. » (S26.12)

« S'ils ne sont pas d'accord, ils ont le droit de le reprendre. » (S26.13)

« On trouve toujours un accord en fin. » (P26.2)

« Et après, si nous identifions un risque, nous émettons des recommandations et donc cette recommandation permet de couvrir le risque. » (S26.14)

« Donc, le service qui récupère une recommandation, est chargé de trouver une solution pour couvrir les risques identifiés sur le sujet. » (S26.15)

« Donc, enfin, l'auditeur, nous suivons ces recommandations qui sont suivies toute l'année pour qu'elles soient mise en œuvre. » (A26.11 et S26.16)

Codage du Segment 27 (§27) :

« Objectivité parce que nous sommes attachés au Directeur Général. » (P27.1 et A27.1)

« Nous sommes indépendants vis-à-vis de tous les autres services du groupe. » (P27.2)

« Nous avons tout pouvoir entre guillemets, nous avons accès à tous les éléments, les informations. » (P27.3)

« On ne peut pas nous faire de rétention d'informations, et d'autre façon, notre premier client est notre directeur général. » (A27.2)

« Evidemment, nous sommes au service de nos clients. Nous sommes là pour protéger la banque et protéger aussi nos clients. » (A27.3 et S27.1)

« Néanmoins, nous n'avons pas de pressions. » (P27.4)

« Si nous avons quelques choses à dire, nous le disons. » (S27.2)

« Et comme nous avons de toute façon toujours des constats, qui ne peuvent pas être mise en cause, nous avons pouvoir de le dire. » (S27.3)

« Après l'établissement choisit de couvrir ou pas les risques, ce n'est pas notre problème. » (S27.4)

« Si le directeur général ne souhaite pas recouvrir un risque, ce de sa responsabilité. » (A27.4)

« Notre travail est de mettre à jour les risques, de les identifier. » (S27.5)

« Et donc s'il vient à arriver qu'il n'accepte pas à couvrir un risque majeur ou grave. » (A27.7)

« Donc, on est indépendant, clairement indépendant. » (P27.5)

Codage du Segment 28 (§28) :

« Alors oui. Agile ça c'est le propos de la banque populaire » (P28.1)

« Notre service aussi. Il est agile. » (P28.2)

« Puisque je vous disais, on peut avoir accès à toutes les informations. » (S28.1)

« Mais, il y a beaucoup d'informations qui ne sont pas disponibles. » (P28.3)

« Il y a un manque d'information. » (P28.4)

« Donc, on n'a pas toujours tout ce qu'on veut. » (P28.5)

« Donc, on est toujours très très agile. » (P28.6 et S28.2)

« On essaye de trouver toujours des solutions. » (S28.3)

« Ça demande beaucoup d'énergie, mais ça on sait faire. » (S28.4)

« En termes de cyber sécurité, je vais vous dire que ce n'est pas le sujet à l'audit actuel. » (P28.7)

« A l'audit actuellement, ce n'est pas le sujet principal la cyber sécurité. » (P28.8)

« C'est un sujet niveau banque. » (P28.9)

« A l'audit, c'est un sujet parmi tant d'autres. » (P28.10)

« Notre rôle au quotidien est la protection de la clientèle. » (P28.11)

« En termes de régulateur, ce n'est pas la cyber sécurité. » (P28.12)

« Nous, on rendait compte, il faut que nos clients soient bien traités, qu'ils aient toutes les informations nécessaires utiles contre leurs ennemies. » (A28.1)

« Ça c'est notre occupation comme régulateurs. » (P28.13)

« En termes de sécurité, on se protège. » (P28.14)

« Mais nous, notre ennemie est notre problème si on ne se protège pas. » (P28.15)

« Le régulateur ne demande pas de se protéger. » (P28.16)

« Donc, ce n'est pas notre mission principale au niveau de l'audit. » (P28.17)

Codage du Segment 29 (§29) :

« Oui, si on a besoin, bien sûr. » (P29.1)

« Si ça va servir la mission et pour réduire les attaques, et pour des risques qu'on ne peut pas identifier, on fera bien intervenir des prestataires. » (A29.1 et P29.2)

« Je pense là que le directeur général devrait être conscient du sujet. » (A29.2 et P29.3)

Codage du Segment 30 (§30) :

« Pour les constats, tous les constats qui sortent de nos missions, moi personnellement je les verrouille, entre guillemets au sens interne. » (S30.1)

« Je les verrouille c'est-à-dire que je vérifie effectivement les constats, les constats remis en cause. » (P30.1)

« Donc, je vérifie d'ailleurs, ce qu'on appelle la piste d'audit. » (S30.2)

« Donc, dès que nous avons un constat, nous avons la preuve de ce que nous avançons et nous n'allons pas les présenter à la direction générale et aux audités quand nous ne sommes pas sûr de nos constats. » (S30.3)

« Tous les constats que nous présentons ont été vérifiés, ils sont verrouillés, il n'y a aucun souci. » (S30.4 et P30.2)

« Après donc les fautes que nous avons émis les recommandations, pour qu'on puisse les identifier. » (S30.5)

« Moi, à mon niveau, je suis tous les trimestres. » (S30.6)

« On a ce qu'on appelle un suivi de recommandations. » (S30.7)

« Et donc, je suis dans l'avancement des recommandations que les services ont souffrance pour y trouver des solutions. » (S30.8)

« Je peux les accompagner à trouver des solutions malgré tout avec les connaissances que j'ai. » (S30.9)

« Et de toute façon, pour les recommandations, chaque recommandation a une durée de mise en œuvre, c'est-à-dire si vous avez identifié un problème sur un sujet dans un service, on va lui donner un an pour trouver une solution pour couvrir le service. » (S30.10)

« Pendant cette année, tous les trimestres, je relance ce service pour dire est ce que cette recommandation est en avance. » (S30.11)

« Est ce que vous êtes bloqué ? » (S30.12)

« Est-ce que vous avez un souci ? » (S30.13)

« Mon rôle est de faire un reporting auprès du directeur général, pour faire attention dans ce service-là, c'est que ce sujet, ils ont un peu mal à le gérer, il faut le faire avancer. » (A30.1 et S30.14)

« En toute façon, moi j'alerte. » (S30.15)

« J'alerte la direction générale. » (A30.2)

« Et je reste en fonction d'accompagnement au niveau du service. » (S30.16)

« En toute façon derrière, nous avons un vrai suivi des constats que nous avons, que nous avons vu. » (S30.17)

« Nous avons mis là-dessus, et une fois que le conseil mis en œuvre, je vérifie parce qu'il m'apporte la preuve, que la recommandation était mise en œuvre, moi je vérifie que la preuve, ils ont toujours un support écrit qui atteste que la recommandation est traitée. » (S30.18)

Codage du Segment 31 (§31) :

« En général, je ne sais pas répondre à seuil du coup. » (P31.1)

« Ma mission, est que je coordonne beaucoup, j'essaye de voir toutes les problématiques de la banque, de faire le lien entre toutes les sujets de la banque. » (S31.1)

« Au-delà de ça, on a tous les intérêts de se préserver aux intérêts de la banque. » (S31.2)

« Si je peux avoir une information d'un côté, puis transmettre une fois à l'autre. » (S31.3)

« Voilà, mon rôle je suis à l'écoute. » (S31.4)

« Après, je n'ai pas un rôle non plus. » (S31.5)

« Moi, je suis à l'écoute. » (S31.6)

Codage du Segment 32 (§32) :

« Euhhhh ! Là comment dire. » (P32.1)

« Lorsqu'il vient faire son travail ! » (A32.1)

« Le matin, il avance tous les jours sur ces questions, il a des questions à qui il faut répondre. » (A32.2)

« Tous les matins, il est ouvert, il fait plutôt des propositions, il est à l'écoute de ses audités quand il pose des questions s'il n'a pas la réponse. » (A32.3)

« C'est des gens contentieux, des gens contentieux, qui cherchent à savoir la part des choses lorsqu'ils mettent des constats. » (P32.2)

« Après au quotidien, il arrive le matin à son poste, il fait ses contrôles, il a éventuellement des entretiens à réaliser avec les audités. » (A32.4)

« Au quotidien, moi, je ne suis pas régulièrement avec eux. » (S32.1)

« On reste au quotidien à l'écoute. » (S32.2)

« S'ils ont des problèmes, moi, je suis là pour les écouter, pour trouver des solutions. » (S32.3)

« Donc, c'est un auditeur, qui va communiquer dans la banque, avec son directeur, ou avec moi-même. » (P32.3 et A32.5)

« Ils communiquent énormément avec les audités, avec ses co-équipiers aussi. » (A32.6)

« Et c'est quelqu'un qui ne reste pas tout seul. » (A32.7)

« S'il a un problème, il va en parler tout de suite. » (A32.8)

« En tout cas, c'est quelqu'un qui est agile, autant que moi. » (A32.9 et P32.4)

« Une personne qui n'a pas de luxe d'avoir du temps à perdre. » (A32.10)

« On a plein d'audits. » (S32.4)

« On a une liste de mission à réaliser pendant l'année. » (S32.5)

« Ainsi, il faut allez vite. » (P32.5)

« Il faut allez vite. » (P32.6)

« L'agilité donc est au quotidien. » (P32.7)

« Il faut être inventif. » (P32.8)

« Et puis, il faut avoir de l'énergie en revanche, beaucoup d'énergie et trouver des solutions rapidement à ces problèmes. » (P32.9)

« Il faut que les auditeurs soient bien faits et comprendre les sujets rapidement. » (A32.11 et P32.10)

Codage du Segment 33 (§33) :

« Oui, c'est sûr. » (P33.1)

« Pour le passée, l'audit était plutôt. » (P33.2)

« En fait, le positionnement de l'audit et ses missions ont changé depuis quelques années. » (P33.3)

« Avant, c'était sanctions, il y avait des procédures qu'on ne respecte pas, ce n'est pas bien. » (P33.4)

« Depuis quelques années, peut-être 4 ou 5 ans, l'audit est plus dans un rôle d'audit conseil. » (P33.5)

« Donc, on va leur rapporter des solutions, on voit des problèmes et on les aide à trouver des solutions, on est plus dans le conseil. » (P33.6)

« Maintenant les gens ont peur, ils ont peur de ce qu'ils ne connaissent pas. » (P33.7)

« Donc, ils pensent qu'on va les… » (P33.8)

« On va mettre en cause leur travail au quotidien. » (P33.9)

« Non, évidement, lorsqu'on trouve une faille, forcément, il faut directement là conserver. » (S33.1)

« On va les identifier la cause, des défaillances que nous trouvons. » (S33.2)

« C'est-à-dire c'est un problème, si dans un service, ils nous ont dit que personnes de mes collègues font ça, forcément, le travail serait moins bien fait. » (A33.1 et S33.3)

« Donc, nous, nous allons mettre en cause de dire : Bien non, vous avez un problème, ce n'est pas que le travail est mal fait, ce qui vous demande c'est l'effectif. » (P33.10)

« Enfin, ils ont peur de l'inconnu, ils ont peur de se sanctionner, de mettre en cause leur travail. » (A33.2)

« Alors qu'en fait, ce que nous regardons ce n'est pas leur travail mais le processus. » (S33.4)

« Ça va du mal à leur faire comprendre, que ce ne sont pas les personnes que nous auditons mais les processus au sens large. » (P33.11)

Codage du Segment 34 (§34) :

« Dans l'équipe d'audit, moi, dans mon quotidien, c'est de l'écoute. » (P34.1)

« C'est de l'écoute au quotidien. » (P34.2)

« C'est beaucoup de ressenti. » (P34.3)

« Il y en a un qui n'est pas bien, qui est fatigué, qui est énervé. » (P34.4 et A34.1)

« Voilà, c'est bien une motivation, trouver de l'intérêt, trouver des solutions lorsqu'ils ont des problèmes. » (P34.5 et A34.2)

« C'est de l'écoute, de l'accompagnement, de l'accompagnement au quotidien. » (P34.6)

« Donc, au sein de l'équipe, effectivement, mon rôle est assez central pour animer, pour réduire les détentions entre les équipes ça arrive. » (S34.1)

« C'est un risque comme un autre. » (S34.2)

« Donc, moi je suis à l'écoute et la surveillance, comme je l'ai dit, même si je suis là pour que le travail soit fait. » (S34.3)

« Et mon rôle est que le travail soit fini en fin d'année. » (S34.4)

« Et cette double casquette, où il fait qu'ils s'apprennent non plus, que la situation est variante et qu'il faut trouver la solution par n'importe quelle manière possible. » (P34.7 et A34.3)

Codage du Segment 35 (§35) :

« Dans les autres services, on va dire en externe, c'est pareil. » (A35.1)

« Je suis en audit pour rappeler les tensions si les services sont en souffrance, même quand nous les auditons de toute façon. » (A35.2 et S35.1)

« Je suis là quand il y a moins de compréhension, ou un manque de disponibilité, je suis là pour trouver des solutions. » (S35.2)

« Pour moi mon rôle, c'est vraiment, de plaisir tout le monde, et de leur prouver que l'audit peut trouver des solutions, et qu'on n'est pas là juste pour travailler. » (P35.1)

« Notre rôle est d'identifier un problème et d'y trouver des solutions qui pourront les aider de toute façon. » (A35.3 et S35.3)

« Donc, voilà, je n'ai pas trop de souci au sein de la banque, j'ai de bonnes relations avec tout le monde, je n'ai pas de problèmes et au sein de l'équipe, c'est pareil. » (P35.2)

Et voilà, c'est aussi, de faire que tout ça passe bien, et faire attention aux tensions au sein des équipes, de phase de transparence, être à l'écoute de tous, et donner des informations aux autres quand ils le veulent, et d'être à l'écoute de prendre les informations qui sont à prendre à l'extérieur du service. (S35.4 et P35.3)

4. Classement des unités codées : Recodage

M. Les séquences-types de l'entretien d'Anne-Laure

Nous allons maintenant regrouper et ordonner les séquences dans l'ordre chronologique depuis le départ (S0) jusqu'à la fin de l'entretien (S+). Nous allons joindre toutes les unités concernées (tous les S) en leur donnant un titre résumant leur contenu.

Nous avons divisés l'entretien d'Anne-Laure en quatre séquences respectives selon l'ordre chronologique.

15. Niveau de formation et progression de la carrière

S0=S1+S1.2+...+S1.9+ S3.1+S3.2+S3.3+S3.4+S6.1+S6.2+S7.1

16. Fonction de superviseur en audit : Rôle et missions

Sa=S2.1+...+S2.6+S3.3+S3.4+S5.1+S10.1+S10.2+S11.1+S11.2

17. Cybersécurité : contrainte et implication

Sb=S14.1+S14.2+S14.3+S14.4+S15.1+S15.2+S16.1+S18.3

18. Conséquence de la cybersécurité sur la banque

Sc=S19.1+S19.2+S19.3+…+S21.5+S22.1+S24.1….S25.5

19. Travail relatif à la cybersécurité

Sd=S25.6+S25.7+S25.8+…+S35.4

Nous allons maintenant proposer un premier résumé des séquences-types de l'entretien d'Anne-Laure après avoir effectué le regroupement selon un ordre chronologique.

Résumé des séquences-types de l'entretien d'Anne-Laure

Au début de l'entretien, Anne-Laure nous explique son parcours professionnel puis son insertion professionnelle dans la BPVF. Elle commence par obtenir un Bac+4 en comptabilité, puis devenu expertise comptable grâce à des formations comptables. Elle a réalisé une mission d'intérim pour entrer après par hasard dans la banque. Elle a progressé durant 25 ans pour devenir enfin un superviseur d'audit dans la BPVF.

Elle a expliqué après son rôle et ses missions comme superviseur d'audit dans la banque. Elle coordonne les équipes, les animent et les amènent au niveau attendu. Aussi, elle gère son équipe et communique avec tout le monde.

Elle a explicité le problème de la cybersécurité en disant que c'était un sujet récent qu'aucun ne se préoccupait pas du tout au sein de la banque. Elle a incité sur le risk et le danger que peut produire la cybersécurité sans pilotage et surveillance. Elle justifie l'embauche d'un personnel qualifié de sécurité informatique qui sera spécialisé dans ce secteur de cybersécurité. Par un manque de compétences en informatiques. Elle insiste aussi sur la formation continue des employés en cybersécurité et l'importance de sa prise de conscience.

Elle aborde l'appel à un cabinet ou prestataire externe pour prévenir les failles en cybersécurité. Elle confirme ce choix parce que ce cabinet leur a permis de mettre à jour certaines défaillances et de détecter et identifier les failles à corriger.

Elle insiste sur l'appel d'un prestataire externe sur des spécificités ou expertises techniques qu'elle n'aura pas dans son équipe.

Dans le cas de cybersécurité, elle confirme l'usage des budgets pour recourir à des prestataires externes qui ont des compétences en sécurité informatique. Enfin, elle réexplique son rôle d'écoute et de supervision sur les missions qu'elle effectue. En cas de détection d'anomalie, elle alerte. Elle est présente pour trouver des solutions à ces problèmes.

N. Les actants du récit d'Anne-Laure

Nous allons ici identifies les personnages dans le récit d'Anne-Laure. Nous allons inclure Anne-Laure elle-même lorsqu'elle se dédouble (« moi, je…). Nous notons respectivement les acteurs de A1 jusqu'à An. Le premier actant du récit est Anne-Laure elle-même puisqu'elle a utilisé le « moi » 39 fois. Le second actant est le directeur de l'audit interne Monsieur « Manuel Couillet ».

A2= A2.1+A26.5

Le troisième actant est le directeur général de la banque.

A3=A4.1+A27.2+A27.4+A27.7+A29.2+A30.1+A30.2

Le quatrième actant est le cabinet extérieur embauche par la banque.

A4=A5.1+A13.1+A21.1+A21.3+A22.1+A22.2+A22.6

Le cinquième actant est le responsable de sécurité et système informatique (RSSI) Monsieur « Didier G. ».

A5=A5.2+A24.1+A24.2+A24.3+A24.4+A24.5

Le sixième actant est les clients de la banque.

A6=A8.2+A27.3+A28.1

Le septième actant est la nouvelle personne embauché pour aider le RSSI

A7=A15.1+A16.1

Le huitième actant est les prestataires externes informatiques.

A8=A22.3+A22.4+A25.2+A29.1

Le neuvième actant est l'i-BP.

A9=A22.5

Le dixième actant est la BPCE.

A10=A25.1

Le onzième actant est l'auditeur interne.

A11=A23.1+A26.2+A26.3+A26.4+A26.5+A26.8+A26.9+A26.11+A32.1+A32.2+A32.3+A32.4+A32.5+A32.6+A32.7+A32.8+A32.9+A32.10+A32.11+A33.1

Le douzième actant est l'audités.

A12=A6.6+A26.7+A26.8+A26.10+A35.2+A35.3

Le treizième actant est l'employé.

A13=A33.2+A34.1+A34.2

Le quatorzième actant est les Hackers.

A14=A20.1+A20.2+A20.3+A23.1

Les actants du récit d'Anne-Laure

Le premier actant est Anne-Laure elle-même. Nous remarquons qu'elle a fréquemment utilisé le « moi » dans son récit pour donner son avis ou son opinion.

Le deuxième actant est le directeur de l'audit « Manuel Couillet ». Il est le superviseur d'Anne-laure. Elle valide avec lui tous les rapports d'audit.

Le troisième actant est le directeur général de la banque. Elle le considère comme le premier client de la banque. Il a une grande importance puisque tous les risques doivent être détectés pour lui.

Le quatrième actant est le cabinet externe embauché par la direction générale. Il intervient par manque de compétence technique informatique à la place de l'audit interne. Anne-Laure appuie sur le rôle du cabinet embauché en cybersécurité. Son rôle est d'assister et de participer avec le cabinet dans leurs missions de cybersécurité. Elle justifie son rôle en répétant qu'elle n'a pas l'expertise. Elle les a laissés à leurs métiers. Ce cabinet a permis de mettre à jour certaines défaillances que l'audit interne incompétent n'a pas pu déceler.

Le cinquième actant est le RSSI « Didier G. » qui est responsable selon Anne-laure de maintenir la cybersécurité dans la banque. Elle le qualifie comme expert en cybersécurité. Elle est rassurée que son positionnement comme RSSI va renforcer la cybersécurité dans la banque car il est expert.

Le sixième actant est les clients de la banque. Le rôle principal d'Anne-Laure est de servir les clients, de les protéger contre les cybers attaques. Les clients doivent être bien traités et bien informés contre tous les attaques et les ennemies.

Le septième actant est la nouvelle personne embauchée comme RSSI. Anne-laure Elle justifie son emploi en disant qu'elle venait renforcer le travail du RSSI. Didier manquait de l'expertise technique en cybersécurité. Cette personne vient renforcer le travail de Didier en sécurité informatique.

Elle défend cette embauche en disant qu'il y a un manque de compétences en cybersécurité dans la banque.

Le huitième actant est les prestataires externes. Elle prouve leur emploi dans sa banque en cas de manques de compétences. Ils ont venu travailler en réduisant les attaques et parfois en détectant des risques indentifiables.

Le neuvième actant est la banque I-BP. C'est une banque relie à la BPVF et qui est en charge de tous ce qui est informatique. Son rôle est de corriger avec le cabinet les observations et les détections des failles informatiques.

Le dixième actant est la BPCE. C'est la banque ou travaille Anne-Laure. Elle est très fidèle et impliquée à travailler dans cette banque.

Le onzième actant est l'auditeur interne. Elle le décrit comme généraliste et faible en cybersécurité. Il est ponctuel aussi et ouvert à faire des propositions et être à l'écoute de ses audites. Il n'a pas les compétences techniques en cybersécurité.

Il est énergétique et agile et n'a pas de temps à perdre. Il est bien informé sur tous les sujets.

Le douzième actant est les audités. Ils font partie des missions d'audit.

Le treizième actant est les employés de la BPVF. Ils ont peur de l'audit car ils ont peur de l'inconnu, de se sanctionner, de mettre en cause leur travail.

Le quatorzième actant est les hackers. Ils sont de plus en plus imaginatifs pour faire des attaques, et ils sont toujours en avance de tout le monde. Ils sont très inventifs, très rapides, très compétents.

O. Les classes d'arguments

Ce niveau d'analyse concerne l'ensemble des arguments, démonstrations et propositions d'Anne-Laure destinés à nous convaincre. Nous allons regroupés l'ensemble des unités codées en P selon des « classes d'arguments » dont chacune représente une étape logique dans un raisonnement.

Nous allons classer les arguments le type de raisonnement qu'Anne-Laure présente dans ces réponses. Nous en avons repéré six qui font l'objet d'arguments explicites qui sont à la base de ce classement.

Nous avons noté (P1) les propositions d'Anne-Laure associé à son travail dans la banque. Elle a expliqué plusieurs fois que c'est le hasard et l'opportunité qui l'ont amené dans la BPVF et son présent poste.

- « Le travail actuel ? Je suis sortie de mes études, j'ai fait une mission d'intérim où je suis arrivé **par hasard** au milieu bancaire. » (S1.3 et P1.1)
- « **Ce n'était pas un choix de ma part**, donc j'ai tombé dans une première banque mais pas la banque populaire. » (S1.4 et P1.2)
- « C'est plusieurs banques dans mon passée, et donc la première banque je suis arrivée **par hasard**. » (S1.6 et P1.3)
- « Et au bout de 5 an, j'ai évolué vers un poste de superviseur **par hasard**, on va dire c'est pareil, j'ai vu l'annonce proposé, et je me suis dit naturellement ce sont des métiers de contrôle, thématique indifférente, mais ce sont des métiers un peu près similaires, » (S3.3 et P3.1)
- « Donc je me suis dit **c'est le moment de changer**, et puis élargir sa vision dans le sens de sortir de la comptabilité pour savoir tous les aspects de la banque. » (P3.2)
- « **Je suis arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé**. » (S3.4 et P3.4)

Nous résumons cet ensemble ainsi : *« Le travail par hasard et par opportunité dans le secteur bancaire ».*

Nous avons noté (P2) les expressions d'Anne-Laure associés aux exigences de l'auditeur interne dans la banque. Elle a les mêmes exigences que ceux des auditeurs internes :

- « **Rigueur, agilité, beaucoup d'ouverture d'esprit**. » (P4.1)
- « **Si on a un problème, on trouve une solution rapidement**. » (P4.2)
- « Il faut arriver à **conserver l'esprit d'équipe** parce qu'on est une équipe de plusieurs auditeurs. » (P4.4)
- « Et il faut arriver à **satisfaire tout le monde**. » (P4.5)
- « Il faut arriver à **préserver les intérêts des auditeurs**, et **préserver les services que nous auditons.** » (P4.6)
- « C'est **un rôle un peu diplomate** entre guillemets. En France, il faut arriver à contenter les intérêts de tout le monde. » (P4.7)
- « Nous, nous sommes des gens qui sont **généralistes** et la plupart des temps, on est **curieux.** » (P5.3)
- « Par contre il faut **savoir inventer tous les jours**, c'est plutôt le présent qui fait que je me contrôle moi-même chaque jour au quotidien. » (P9.3)
- « Donc, **il faut être curieux**. » (P9.4)

- « A l'audit, nous avons la chance de découvrir plein de sujets que nous ne sommes pas experts en au départ. Ça nous donne l'occasion d'appréhender de nouveaux sujets. » (P9.5)
- « **En tout cas, c'est quelqu'un qui est agile, autant que moi.** » (A32.9 et P32.4)
- « **L'agilité** donc est au quotidien. » (P32.7)
- « Il faut être **inventif.** » (P32.8)
- « **Il faut que les auditeurs soient bien faits et comprendre les sujets rapidement**. » (A32.11 et P32.10)
- « Dans l'équipe d'audit, moi, dans mon quotidien, c'est de l'écoute. » (P34.1)
- « C'est de l'écoute au quotidien. » (P34.2)
- « C'est beaucoup de ressenti. » (P34.3)

Cet ensemble se résume ainsi : *« Travail semblable, profil très proche que celui des auditeurs internes ».*
Nous avons noté (P3) toutes les formules associées à la zone de confort d'Anne-Laure dans son travail et ses avantages positifs.

- « Pourquoi je travaille ! Parce que **j'aime bien travailler déjà**, et **j'aime bien découvrir de nouveaux choses**, **de nouveau challenges**, apprendre à assez évoluer avec mon environnement. » (P10.2)
- « Moi je suis active, et **j'aime mon travail** et **je veux continuer à travailler, à progresser.** » (P10.4)
- « C'est **un milieu que j'aime bien**, je ne vois pas changer de milieu de travail. » (P6.2)
- « Je **resterai dans la banque** le plus long possible. » (P6.3)
- « Donc, c'est **une banque qui me plait**. » (P7.1)
- « Ce sont **les valeurs mutualistes qui me plaisent**, et donc, je me n'en verrai pas allez dans une autre banque, société générale ou … » (P7.2)
- « C'est à cause du côté mutualiste que je suis là, je reste **attachée à la banque, je suis <u>fidèle</u>**. » (P7.3)
- « Donc, je suis une collaboratrice **<u>fidèle</u>** aux valeurs de la banque, et à la banque elle-même, je suis **<u>fidèle</u>** à mon employeur. » (P7.4)
- « Donc, je ne me vois pas allez ailleurs dans une autre banque. » (P7.5)
- Ça sera juste **un choix de ma part de rester** dans cette banque. » (P8.3)
- « Ce qui importe c'est un sous-jacent qu'on **connait** bien la banque. » (P11.3)

Cet ensemble se résume ainsi : *« Impliquée dans sa banque : Bonne connaissance, rattachée et fidèle. »*
Nous avons noté (P4) les faiblesses et désavantages du métier d'Anne-Laure en cybersécurité :

- « En termes de SSI, **ce n'est pas notre confort**, c'est vraiment un métier très spécifique. » (P5.1)
- « **Ce sont <u>des expertises</u> que nous n'avons pas forcement**, donc, il y a rien à réaliser des missions sur les SSI. » (P5.2)
- « Par contre, moi, j'ai **une sensibilité sur tout ce qui est environnement informatique.** » (P5.5)
- « Et après, je suis **<u>moins expert</u>** en ce métier. » (P5.8)
- « « Non, je **<u>n'ai pas les compétences</u>**. » (P13.1)
- « Mais, en tout cas, **<u>moi je n'ai pas les compétences à mon niveau</u>**. » (P13.3)
- « Pour moi, c'est **un nouveau sujet.** » (P14.5)
- « C'est **un nouveau sujet pour nous**, il faut savoir à mettre en compétences. » (P14.6)
- « Il y a très peu de gens qui sont sensibles à ce sujet et ce sont **des vraies compétences que nous n'avons pas pour l'instant chez nous.** » (P14.7)

- « **Je ne sais pas**. » (P15.1)
- « On ne peut pas **être généraliste sur un sujet pareil**. » (P15.4)
- « Il faut appeler **un expert** sur le sujet pour savoir s'il y a une faille ou pas. » (P19.4)

Nous résumons cet ensemble : *« L'audit interne est faible en compétence technique, il n'a pas les expertises spécifiques dans ce domaine de cybersécurité. »*

Nous avons noté (P5) les expressions et les formules relatives à la cybersécurité :

- « C'est le **danger numéro 1** on va dire. » (P12.1)
- « Pour moi, c'est **le danger numéro 1** dans les entreprises actuellement. » (P12.2)
- « Et puis, c'est **un risque qui s'est largement sous-estimé** parce que **ça coûte cher.** » (P12.3)
- « Et que déjà, c'est un **nouveau risque**, et ça va mettre du temps à appréhender. » (P12.4)
- « Et pour moi c'est **un danger, un vrai danger, un danger** qui doit être une préoccupation pour toutes les entreprises au-delà les banques. » (P12.5)
- « Pour moi, c'est une préoccupation de tous, parce qu'on peut tous se faire attaquer si on prend des risques. » (P16.3)
- « Mais, c'est l'affaire de tous, il faut que ce soit une préoccupation de tous. » (P16.1)
- « Clairement, mais pour ça il faut animer le sujet, il faut que les gens **prennent conscience** que **c'est un danger**. » (P16.5 et S16.1)
- « Et le danger peut venir de partout. » (P16.6)
- « Voilà, pour moi, c'est l'affaire de tous. » (P16.7)
- « On commence à faire **prendre conscience au gens** que c'est un sujet qui a des risques informatiques, qu'il **faut faire attention** à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. » (S17.5)
- « Pour moi, **c'est bien ce qu'on fait.** » (P17.3)
- « Et que tout le monde soit expert sur le sujet. » (P17.4)
- « Moi, je crois qu'ils ont pris conscience du danger. » (P18.2)
- « Ça coûte cher et ça prend du temps. » (P18.3)
- « Il faut dire attention. » (P19.3)
- « C'est **un risque très très technique**, compliquer à cerner. » (P23.12)

Nous résumons cet ensemble par le raisonnement d'Anne-Laure. *Elle explique que la cybersécurité doit être un problème de tous les employés dans la banque car c'est le danger numéro 1. Il faut sensibiliser tous les employés et prendre conscience du danger de ce risque. C'est un danger qui coûte cher et qui va prendre du temps à appréhender. Elle argumente qu'elle fait jusqu'à maintenant un bon travail de formation et de sensibilisation à ce risque, mais ce n'est pas suffisent, il faut plus de travail.*

Nous avons noté (P6) les expressions et les formules associés à qui est responsable d'assurer la cybersécurité :

- « La cyber sécurité**, c'est un métier**, une façon de se parler, de s'exprimer. » (P21.3)
- « La cybersécurité, **c'est un vaste sujet**, que personne, à l'instant, il y a peu de gens qui savent ce qui montre ce sujet. » (P17.7)
- « On peut avoir notre rôle à jouer en termes de détection d'application un **peu orpheline** dans certains services. » (P19.6)

- « La cybersécurité, pour moi, **c'est un métier**, aussi vrai, **le responsable de cyber sécurité est un <u>métier</u> qui évolue**. » (P23.5)
- « Selon moi, **le RSSI** c'est son travail. » (P24.2 et A24.1)
- « Il **<u>est bien l'expert.</u>** (RSSI) » (A24.2)
- « Comme je vous l'ai dit, il y a **une nouvelle personne** qui est venu qui a **des compétences techniques en plus.** » (P24.3)
- « Moi, je pense que **l'expertise** doit rester là où elle est actuellement, il renforce le travail informatique. » (P24.4)
- « C'est le **meilleur endroit** où ça peut être. » (P24.5)

Anne-Laure a expliqué que c'est le rôle d'une part de tous d'assurer la cybersécurité. L'audit interne est faible en compétence et expertise technique dans ce domaine. Elle admet que la cybersécurité est un métier qui doit être indépendant. Le RSSI et la nouvelle personne embauchée qui vient l'assister ont les expertises et compétences spécifiques pour appréhender les risques de la cybersécurité.

P. <u>Le schème provisoire de l'entretien</u>

Nous allons tout d'abord restituer le schème en situant les arguments dans leur ordre d'intervention dans le récit et en les mettant en relation « spatiale » avec les deux autres classes d'unités précédemment recodées : les séquences et les actants. Nous allons les présenter dans ce tableau qui constituera un schème provisoire de l'entretien.

Séquences (Sn)		Arguments (Pn)	Actant (An)
Niveau de formation et progression de la carrière (S_0)	• Je suis expertise comptable en fait. (S1.1) • J'ai réalisé un Bac+4 en comptabilité. (S1.2) • Je suis arrivé par hasard au milieu bancaire. (S1.3) • Je suis arrivée par hasard. (S1.6) • Actuellement, je travaille à l'audit. Je suis superviseur à l'audit. (S2.1) • Et au bout de 5 an, j'ai évolué vers un poste de superviseur par hasard, • Arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé. (S3.4)	• Je suis arrivé par hasard au milieu bancaire. (P1.1) • Ce n'était pas un choix de ma part (P1.2) • Je suis arrivée par hasard. (P1.3) • Un poste de superviseur par hasard, (P3.1) • C'est le moment de changer, (P3.2) • Je suis arrivé par opportunité, ce n'est pas un choix, je n'avais pas anticipé. (P3.4) • J'aime bien travailler déjà, et j'aime bien découvrir de nouvelles choses (P10.2) • J'aime mon travail et je veux continuer à travailler, à progresser. (P10.4) • Je ne vois pas changer de milieu de travail. (P6.2) • Je resterai dans la banque le plus long possible. (P6.3) • C'est une banque qui me plait. (P7.1) • C'est à cause du côté mutualiste que je suis là, je reste attachée à la banque, je suis fidèle. (P7.3) • Collaboratrice fidèle aux valeurs de la banque, et à la banque elle-même, je suis fidèle à mon employeur. (P7.4)	• Le Moi.(répété plusieurs fois).
Fonction de superviseur en Audit : Rôle et missions (Sa)	• Je suis superviseur à l'audit. (S2.1) • Mon rôle c'est de coordonner les équipes, de les animer, de les amener au niveau attendu. » (S2.2) • Et donc, mon rôle est de saturer que tout est fait en temps parfait. (S2.6) • Je rappelle régulièrement tout le monde sur la cybersécurité. (S5.1) • Moi, j'ai une équipe à gérer. (S10.1) • Moi je communique énormément avec tout le monde. (S11.2)	• Rigueur, agilité, beaucoup d'ouverture d'esprit. (P4.1) • Si on a un problème, on trouve une solution rapidement. (P4.2) • Conserver l'esprit d'équipe parce qu'on est une équipe de plusieurs auditeurs. (P4.4) • Satisfaire tout le monde. (P4.5) • Préserver les intérêts des auditeurs, et préserver les services que nous auditons. (P4.6) • Diplomate (P4.7) • Généralistes, curieux. (P5.3) • Être curieux. (P9.4) • L'agilité donc est au quotidien. (P32.7) • Il faut être inventif. (P32.8) • C'est de l'écoute au quotidien. (P34.2) • C'est beaucoup de ressenti. (P34.3)	• Moi, en tant que superviseur, je valide avec lui, et nous faisons valider avec notre directeur d'audit. (A26.5) • Préserver les intérêts de la banque, découvrir les risques, et de détecter les risques pour le directeur général qui est notre principal client. (A4.1) • Notre premier client est notre directeur général. (A27.2) • Si le directeur général ne souhaite pas recouvrir un risque, ce de sa responsabilité. (A27.4) • Le directeur général devrait être conscient du sujet. (A29.2) • Reporting auprès du directeur général, pour faire attention dans ce service-là, c'est que ce sujet, ils ont un peu mal à le gérer, il faut le faire avancer. (A30.1) • J'alerte la direction générale. (A30.2)

Cybersécurité : Contrainte et implication (Sb)	• C'est un sujet, jusqu'à un an, qu'on ne se préoccupait pas du tout au sein de la banque. (S14.2) • Les choses ont changé, ils ont embauché quelqu'un qui devra arriver. (S14.3) • J'ai juste entendu qu'on allait renforcer le sujet. (S15.1) • C'est un côté positive qu'on a clairement conscience qu'on a besoin d'une autre personne. (S15.2) • Clairement, mais pour ça il faut animer le sujet, il faut que les gens prennent conscience que c'est un danger. (S16.1) • On est 2000 collaborateurs au sein de la banque, c'est facile d'y trouver une faille pour entrer dans la banque. (S16.2) • Oui, on a des formations, ce n'est pas en cyber sécurité exactement, c'est plus. (S17.1) • On commence à faire prendre conscience aux gens que c'est un sujet qui a des risques informatiques, qu'il faut faire attention à ce qu'on fait dans notre mode de fonctionnement au quotidien, et donc il faut aller plus loin. (S17.5)	• En termes de SSI, ce n'est pas notre confort, c'est vraiment un métier très spécifique. (P5.1) • Ce sont des expertises que nous n'avons pas forcement, donc, il y a rien à réaliser des missions sur les SSI. (P5.2) • J'ai une sensibilité sur tout ce qui est environnement informatique. (P5.5) • Je suis moins expert en ce métier. (P5.8) • Je n'ai pas les compétences. (P13.1) • Je n'ai pas les compétences à mon niveau. (P13.3) • Nouveau sujet. (P14.5) • Nouveau sujet pour nous, il faut savoir à mettre en compétences. (P14.6) • On ne peut pas être généraliste sur un sujet pareil. (P15.4)	• Il est généraliste. (A26.2) • Un sujet qu'il ne connait pas forcement. (A26.3) • C'est l'auditeur qui va traiter. (A26.4) • L'auditeur est ponctuel. » (A26.9) • Il faut que les auditeurs soient bien faits et comprendre les sujets rapidement. » (A32.11) • C'est un problème, si dans un service, ils nous ont dit que personnes de mes collègues font ça, forcément, le travail serait moins bien fait. » (A33.1)
Conséquence de la cybersécurité sur la banque (Sc)	• Donc, quelque part, si on voit des failles en termes d'habilitation ou d'application qui sera un peu à la dérive ou isolé dans son coin. (S19.4) • De toute façon, nous embauchons dans le monde de banque, il y a beaucoup de jeunes qui sont embauché, beaucoup de personnes qui partent en retraite. (S20.1) • Et plus on les informe rapidement, voilà, pour moi, il faut communiquer et être former. (S20.3 et P20.10) • Donc, on les a assistés, on a participé avec eux dans leurs missions. (A21.3 et S21.2) • Après notre rôle était de coordonner, de sert en sorte d'interlocuteurs, pour faciliter leurs missions. (S21.5) • Et donc, on a amené ce cabinet. (S22.3) • Je pense, je ne peux pas vous dire, je n'ai pas participé au choix du cabinet (S22.4) • ce cabinet-là, nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP. (S22.5) • Et le but était que les failles qui étaient identifiées puissent être corrigées. (S22.6) • Faire appel à des prestataires externes sur des spécificités ou expertises techniques que nous n'aurions pas dans notre collaborateur. (S25.3)	• Danger numéro 1 on va dire. (P12.1) • Danger numéro 1 dans les entreprises actuellement. (P12.2) • Risque qui s'est largement sous-estimé parce que ça coûte cher. (P12.3) • Nouveau risque, et ça va mettre du temps à appréhender. (P12.4) • Danger, un vrai danger, un danger qui doit être une préoccupation pour toutes les entreprises au-delà les banques. (P12.5) • Ça coûte cher et ça prend du temps. (P18.3) • Il faut dire attention. (P19.3) • C'est un risque très très technique, compliquer à cerner. » (P23.12)	• Les hackers sont de plus en plus imaginatifs, et c'est la première faille. (A20.1) • Les hackers sont toujours en avance de tout le monde. (A20.2) • Il ne faut pas sous-estimer leurs forces. (A20.3) • Les hackers sont très inventifs, très rapides, très compétents. C'est un métier qu'on ne peut pas suivre. (A23.1) • Nous avons fait appel à un cabinet extérieur. (A5.1) • En employant un cabinet, je pourrai faire des liens entre un cabinet, et lui apporté le lien entre les connaissances métier et les problématiques de cyber sécurité. » (A13.1) • On a envisagé un expert métier, un cabinet spécialisé. » (A21.1) • Ce cabinet nous a permis de mettre à jour certains défaillances, qu'après nous avons fait en coordination avec l'I-BP. (A22.2) • Participer un cabinet au bénéfice du groupe. (A22.6)

			• Les prestataires informatiques, on sentait qu'on avait besoin, on les a fait venir. (A22.3) • Pas les compétences, appel à ces prestataires externes. (A25.2) • Servir la mission et réduire les attaques, et des risques qu'on ne peut pas identifier, intervenir des prestataires. (A29.1)
Travail relatif à la cybersécurité (Sd)	• Ça va dépendre des profils des collaborateurs de notre équipe d'audit. (S25.6) • Ont des compétences techniques informatiques dans la sécurité, ne font pas forcement appel à un prestataire externe, peut-être qu'ils ont des compétences. (S25.7) • Budgets pour recourir à des prestataires externes. (S25.8) • Si on peut faire des missions en internes, on les fait. (S25.9) • Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes. (S25.10) • L'auditeur, nous suivons ces recommandations qui sont suivies toute l'année pour qu'elles soient mise en œuvre. (S26.16) • Nous sommes là pour protéger la banque et protéger aussi nos clients. (S27.1) • Mettre à jour les risques, de les identifier. (S27.5) • Accès à toutes les informations. (S28.1) • Moi j'alerte. (S30.15) • je suis à l'écoute. (S31.4)	• Très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n'avons pas pour l'instant chez nous. (P14.7) • Appeler un expert sur le sujet pour savoir s'il y a une faille ou pas. (P19.4) • Préoccupation de tous, parce qu'on peut tous se faire attaquer si on prend des risques. (P16.3) • L'affaire de tous, il faut que ce soit une préoccupation de tous. (P16.1) • Il faut que les gens prennent conscience que c'est un danger. (P16.5) • C'est l'affaire de tous. (P16.7) • Le monde soit expert sur le sujet. (P17.4) • La cyber sécurité, c'est un métier, une façon de se parler, de s'exprimer. (P21.3) • On peut avoir notre rôle à jouer en termes de détection d'application un peu orpheline dans certains services. (P19.6) • La cybersécurité, pour moi, c'est un métier, aussi vrai, le responsable de cyber sécurité est un métier qui évolue. (P23.5) • Le RSSI c'est son travail. (A24.1) • Il est bien l'expert. (RSSI) (A24.2) • Nouvelle personne qui est venu qui a des compétences techniques en plus. (P24.3) • L'expertise doit rester là où elle est actuellement, il renforce le travail informatique. (P24.4)	• Je sais vous avez interviewé Didier G., ils ont embauché un expert là-dessus. (A5.2) • Le RSSI c'est son travail. (A24.1) • Il est bien l'expert. (A24.2) • Et en plus dans la banque, il est au sein du service, il est en contact avec tout le monde. (A24.3) • Il garde sa position pour animer le sujet, il faut qu'il puisse être en contact avec tout le monde. (A24.4) • Je pense que c'est la meilleure position, à mon sens, c'est très bien qu'il soit là-bas. (A24.5) • La nouvelle personne va arriver chez Didier G. pour collaborer avec lui. (A15.1) • Il faut qu'il y ait l'expert. (A16.1)

5. Production des catégories par l'analyse structurale

Notre travail présenté en ce qui précède était purement inductif. Nous allons maintenant dégager des unités de sens sur la base de notre description préalable et essentielle. Ces unités de sens sont appelées *« catégories sémiques »* selon Greimas (1986) qui sont constitutives de la logique sociale de l'entretien et de sa forme sémique.

Notre travail sera un travail démonstratif qui se reposera sur quelques principes de base qui constitueront une sorte de fonds communs de l'analyse structurelle. Conformément à notre projet de départ, nous sommes obligés de montrer la démarche en acte en introduisant des équivalents dans la littérature. Nous signalons les multiples choix sur lesquels repose la mise en œuvre de toute démarche d'inspiration structurale. Donc, notre mise en œuvre repose sur une intelligence préalable du discours que la partie précédente n'a que formaliser.

a. Disjonction et Conjonction

Nous allons considérer l'hypothèse de base de l'analyse est de traduire le schème précédent en une combinaison de catégories typiques constitutive du sens général de l'entretien.

Nous assumons que la révolution structurale consiste à analyser toute langue naturelle et tous ensemble signifiant comme un système d'opposition à l'intérieure d'une relation constitutive du sens. Nous s'occupons à des « éléments différentiels » ou des « traits distinctifs » qui assurent l'existence d'une langue. Donc, ce qui est vrai au sens lexical l'est aussi au sens sémantique.

Nous admettons que le sens linguistique d'un mot ne se comprend qu'en restituant la disjonction qui le spécifie et la conjonction qui lui assure son appartenance à une catégorie. La disjonction trouve son origine dans la chaine syntagmatique constitutive du signifiant et la conjonction de l'intégration paradigmatique définissant le signifié.

b. Application à l'entretien et à ses trois niveaux

i. La signification des séquences : l'opposition je sais/je ne sais pas

Anne-Laure qualifie les expériences qu'elle a tiré des différentes phrases de son parcours au moyen d'expression souvent lapidaires :

(S1) : « Si on a un problème, on trouve une solution rapidement. » (§4)

(S2) : « En termes de SSI, ce n'est pas notre confort, c'est vraiment un métier très spécifique. » (§5)

(S3) : « Ce sont des expertises que nous n'avons pas forcement, il y a rien à réaliser des missions sur les SSI. » (§5)

(S4) : « Par contre, moi, j'ai une sensibilité sur tout ce qui est environnement informatique. » (§5)

(S5) : « J'ai quand même cette sensibilité contre les sujets qui ne sont pas connus. » (§5)

(S6) : « Et après, je suis moins expert en ce métier. » (§5)

(S7) : « Et puis, c'est un risque qui s'est largement sous-estimé parce que ça coûte cher. » (§6)

(S8) : « Et que déjà, c'est un nouveau risque, et ça va mettre du temps à appréhender. » (§6)

(S9) : « Non, je n'ai pas les compétences. » (§13)

(S10) : « Mais, en tout cas, moi je n'ai pas les compétences à mon niveau. » (§13)

(S14) : « Pour moi, c'est un nouveau sujet. » (§14)

(S15) : « C'est un nouveau sujet pour nous, il faut savoir à mettre en compétences. » (§14)

(S16) : « Il y a très peu de gens qui sont sensibles à ce sujet et ce sont des vraies compétences que nous n'avons pas pour l'instant chez nous. » (§14)

(S17) : « Ce qui sensibilise l'informatique, ce sont des profils très rares » (§14)

(S18) : « Je ne sais pas. » (§14)

(S19) : « C'est un côté positive qu'on a clairement conscience qu'on a besoin d'une autre personne. » (§15)

(S20) : « On ne peut pas être généraliste sur un sujet pareil. » (§15)

(S21) : « Il faut qu'il y ait l'expert. » (§16)

(S22) : « Mais, c'est l'affaire de tous, il faut que ce soit une préoccupation de tous. » (§16)

(S23) : « Pour moi, c'est une préoccupation de tous... » (§16)

(S24) : « Voilà, pour moi, c'est l'affaire de tous. » (§16)

(S25) : « Non, pour moi non. » (§16)

(S26) : « Parce que l'audit n'a pas de compétence métier. » (§16)

(S27) : « On n'est pas expert. » (§16)

(S28) : « Je disais tout à l'heure que les auditeurs sont généralistes et on n'a pas de compétence… » (§16)

(S29) : « Il faut quelqu'un qui soit dédié à ça. » (§17)

(S30) : « Nous, on en peut pas suivre, on n'a pas les compétences en tout cas. » (§17)

(S31) : « C'est un risque très très technique, compliquer à cerner. » (§17)

(S32) : « Selon moi, le RSSI c'est son travail. » (§18)

(S33) : « Il est bien l'expert. » (§18)

(S34) : « Comme je vous l'ai dit, il y a une nouvelle personne qui est venu qui a des compétences techniques en plus. » (§18)

(S35) : « Moi, je pense que l'expertise doit rester là où elle est actuellement... » (§18)

« C'est le meilleur endroit où ça peut être. » (§18)

(S36) : « Si on n'a pas les compétences, on a la possibilité de faire appel à ces prestataires externes. » (§18)

(S37) : « des compétences techniques informatiques dans la sécurité… » (§25)

Nous allons ici faire des hypothèses en restant le plus près possibles du texte retranscrit. Nous allons rétablir les oppositions entre unités de diverses séquences-types :

- Si on a un problème, on trouve une solution rapidement/ En termes de SSI, ce n'est pas notre confort, Ce sont des expertises que nous n'avons pas forcement ;
- On n'est pas expert / Il est bien l'expert ;
- Une nouvelle personne qui est venu qui a des compétences techniques en plus / je n'ai pas les compétences ;
- On ne peut pas être généraliste sur un sujet pareil / On est curieux et généraliste dans notre travail.

L'opposition je sais/je ne sais pas concerne successivement ou simultanément trois catégories : Niveau de formation et progression de la carrière, fonction de superviseur en audit et conséquence de la cybersécurité sur la banque. Ce qu'Anne-Laure précise ici clairement est qu'elle n'a pas les compétences spécifiques en cybersécurité. Il existe un poste de RSSI et une personne qui est venue l'aider spécialiste et expertise dans ce métier. Elle ajoute que dans le cas de mission d'audit sur les services informatiques, et car il y a manque de compétences techniques, il y a appel à un cabinet externe pour réaliser cette mission.

ii. La signification des actants : pareils/pas pareils et mieux/pire

Nous allons procéder de la même façon pour les actants du récit d'Anne-Laure.

Nous résumons dans ce tableau ci-dessous les acteurs pareil et pas pareil à Anne-Laure.

Pareil	Pas Pareil
Directeur de l'audit Interne (A2)	Cabinet extérieur embauché (A4)
Directeur générale (A3)	RSSI Didier (A5)
Clients de la banque (A6)	Nouvelle personne embauché pour aider le RSSI (A7)
Auditeur interne (A11)	Prestataires externes informatiques (A8)
Les audités (A12)	Hackers (A14)
Les employés (A13)	

Nous pouvons maintenant analyser le sens de l'opposition Pareil/Pas Pareil en retrouvant les catégories associant la conjonction de deux termes. Nous vérifions que pour Anne-Laure, sont pareils ceux qui n'ont pas les expertises et les connaissances techniques en cybersécurité, et pas pareils qu'elle, ceux qui ont les compétences techniques en cybersécurité. Pour Anne-laure le mieux sera que la cybersécurité soit une préoccupation de tous, pas seulement les experts et les RSSI. Le pire c'est de laisser les spécialistes seuls manager la cybersécurité dans la banque en formant plus les hauts employés dans les zones d'informatique et de cybersécurité. Elle signale que le danger vient de partout en disant que c'est facile de trouver une faille pour entrer dans la banque. Le pire sera plus d'attaque et de failles en

cybersécurité si elle est laissée seulement à RSSI sans une coopération avec l'audit interne. Le pire c'est de se déceler de la responsabilité de la cybersécurité en justifiant que c'est hors de son expertise et champ d'application.

iii. La signification des arguments : Facile/Pas facile

Anne-Laure précise dans son discours qu'elle n'a pas les compétences en informatique et en cybersécurité. Elle dit je ne sais pas et ce n'est pas dans mon champ d'expertise, elle a une sensibilité sur tout ce qui est environnement informatique. Mais elle oppose son discours en disant :

- Qu'elle a de bonnes connaissances sur toutes les applications et les différents métiers de la banque. Mais, Elle n'a pas les compétences dans ce niveau d'informatique.
- En disant que la cybersécurité est un risque très majeur et important mais elle ne sait rien sur le sujet, elle a une sensibilité contre les sujets qui ne sont pas connus.
- En disant qu'elle est curieuse, généraliste et réalise des missions d'audit sur tous les départements, mais dans le cas de la cybersécurité, ce sont des expertises qu'elle n'a pas forcement, donc, il y a rien à réaliser des missions sur les SSI. (La banque fait recours à un cabinet externe expert en sécurité informatique)
- En disant qu'elle connait seulement l'importance de ces sujets, et rappelle régulièrement tout le monde mais elle ne se contente pas d'apprendre sur le sujet en tant que superviseur d'équipe d'audit
- En disant qu'elle est fidèle et attachée à la banque, mais elle ne préserve pas les intérêts des auditeurs, ni des clients ni du directeur général en limitant sa collaboration comme superviseur à la prévention sur la cybersécurité.

Nous analysons ces oppositions pour trouver la totalité qui donne sens à ces couples, découvrir la conjonction qui englobe cette disjonction.

c. La structuration de l'univers sémantique et la logique du récit

Rappelons les résultats acquis à ce stade de l'analyse. Une première opposition je sais/je ne sais pas structure les séquences d'Anne-Laure. Nous l'avons décomposée selon trois propriétés combinées qui permettent de qualifier les renseignements de cybersécurité dans la banque :

- Je ne sais pas = Pas de compétence technique informatique + Pas d'expertise + recours à un cabinet externe ou prestataires externes
- Je sais = Compétence technique spécialisé en informatique + Expertise technique + assurer la cybersécurité

Une seconde opposition pareil/pas pareil structure les segments du récit qui mettent en scène des actants de la vie d'Anne-Laure. Nous en avons trouvé deux propriétés principales qui permettent de qualifier les significations d'une autre « totalité » que l'on peut appeler statut :

- Pareil=Pas d'expertise+Pas de responsabilité
- Pas pareil= Expertise technique+Responsabilité de cybersécurité

Une autre opposition a été introduite pour rendre compte de la structuration du récit des actants : mieux/pire, qui renvoie à une autre « totalité » qu'il faut y avoir une collaboration pour réduire les failles et les cybers attaques.
Une troisième opposition nous a permis de structurer la narration d'Anne-Laure et de qualifier la relation précédente facile/pas facile. Nous allons extraire donc les propriétés suivantes :

- Facile=expertise technique acquise+compétence technique+connaissance
- Pas Facile=Incompétent domaine informatique+coûte cher+Prend du temps

Nous allons terminer notre analyse par-là construction d'axes croisés permettant d'attribués des propriétés identiques à plusieurs significations dégagées antérieurement. Nous proposons pour l'entretien d'Anne-Laure les schémas suivants :

Tableau 1. Situation et perspectives professionnelles d'Anne-Laure

	Positives (Je sais)	Négatives (Je ne sais pas)
Possible (Facile)	J'alerte tout le monde	Cabinet Externe et Coopération
Impossible (Pas Facile)	Prestataire externe expert et spécialiste	Préoccupation de tous, il faut du travail.

Tableau 2. Personnages propre et perspectives professionnelles d'Anne-Laure

	Semblables (Pareil)	Différents (Pas Pareil)
Positives (Mieux)	Auditeurs internes, Directeur générale, Directeur de l'audit	Cabinet externe spécialiste, Prestataire externe expert
Négatives (Pire)	Employés, clients, Audités	RSSI seul responsabilité

B5. Méthodologie de codage du guide d'entretien du RSSI à la BPVF

Le Codage du Guide d'entretien du RSSI

Nous commencerons l'analyse par un repérage des niveaux du discours considéré comme un récit. Selon Roland Barthes, tout récit peut être analysé selon trois niveaux correspondant à trois lectures différentes mais nécessairement articulées :

- Le niveau des fonctions est celui auquel se déploient les épisodes du récit que nous appellerons des séquences. Nous les numéroterons par (S). Ces séquences racontent le parcours de Didier dans la banque.
- Le niveau des actions concerne les éléments du récit qui mettent en scène des « actants », c'est-à-dire des personnages qui agissent, interviennent, jouent un rôle dans le récit. Nous numéroterons tous les éléments de l'entretien comprenant de tels indices d'actant par (A).
- Le niveau de la narration se repère par la présence de thèses, d'arguments, de propositions destinées à nous convaincre, à défendre son point de vue. Nous noterons ces parties de l'entretien par (P).

Premier codage de l'entretien

51 questions = 51 séquences

Codage du Segment 1 (§1) :

J'ai passé un baccalauréat en France. (S1.1)

Et après, j'ai passé des examens bancaires. (S1.2)

Le Certificat d'aptitude professionnelle à la profession des banques et un brevet professionnel de banque de trois ans et j'ai fait la première année de l'Institut technique bancaire ITB. (S1.3)

Codage du Segment 2 (§2) :

J'ai trouvé ce travail, en envoyant des CV dans plusieurs banques, et j'ai été retenu dans la banque populaire. (S2.1)

Codage du Segment 3 (§3) :

Alors je suis responsable des risques opérationnels, au sein de la direction des risques et du contrôle permanent et de la conformité de la BPVF. (S3.1)

J'ai également en charge les plans d'urgence et de poursuite d'activité et la sécurité des systèmes d'information. (S3.2)

Codage du Segment 4 (§4) :

Mon parcours, ça a été un parcours à la profession bancaire pendant une trentaine d'année. (S4.1)

Donc, j'étais responsable du traitement des chèques au moyen de paiement. (S4.2)

Ensuite, j'étais responsable de la monnaie c'est-à-dire tout ce qui tourne autour des cartes bancaires. (S4.3)

Ensuite, j'étais responsable de l'ensemble des moyens de paiement, les chèques, les virements, les traitements, les cartes bancaires, les moyens de paiement internationaux. (S4.4)

Et on m'a fait opposition compte tenu de mes connaissances de production bancaire. (S4.5)

On m'a fait la proposition de m'occuper de risques opérationnels. (S4.6)

C'est une suite un peu logique. (P4.1)

Codage du Segment 5 (§5) :

Les qualités requises c'est une bonne connaissance des métiers bancaires, et en particulier des métiers qui tournent autour des moyens de paiements, c'est un bon relationnel avec les métiers, puisqu'en fait, les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire, comme la « BPVF », nous ne sommes pas des experts en sécurité informatique. (P5.1 et S5.1)

Les experts en sécurité informatique sont chez les opérateurs informatiques et ne sont pas dans les établissements comme une banque populaire. (A5.1)

Je ne sais pas si je vous ai décrit notre organisation, du groupe « BPCE », parce que ça peut avoir un intérêt pour vous. (P5.2)

Donc, les banques populaires font partie du groupe « BPCE », qui est le deuxième groupe français que vous connaissez certainement qui comprend les banques populaires, les caisses d'épargnes et un certain nombre de filiales. (A5.2)

Et donc, la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique par des opérateurs informatiques. (S5.2 et A5.3)

Dans la banque populaire, on a une petite structure qui fait seulement des développements internes. (S5.3)

Et travailler en mode transversale, travailler en équipe. (P5.3)

Et d'avoir une bonne communication. (P5.4)

Et de soigner le relationnel, les relations avec des gens, être rigoureux, organiser. (P5.5)

Codage du Segment 6 (§6) :

En effet, les autres métiers de la banque. (S6.1)

Codage du Segment 7 (§7) :

Il y a le responsable des moyens de paiement, les responsables des crédits, les responsables d'épargne, les responsables d'assurance, les responsables ressources humaines, les responsables communication, les responsables immeubles sécurités, ce sont des banques plus que dans le réseau d'agence. (S7.1 et A+)

Codage du Segment 8 (§8) :

Parce que quand j'étais jeune, la banque avait bonne réputation et c'était un peu la sécurité dans travailler dans une banque. (P8.1)

Codage du Segment 9 (§9) :

Parce que c'est une banque à taille humaine. (P9.1)

Il y a des valeurs coopératives qui me correspondent bien. (P9.2)

En plus, c'est à proximité de mon domicile. (P9.3)

Codage du Segment 10 (§10) :

Oui, je pense. (P10.1)

Codage du Segment 11 (§11) :

Oui, je crois mon expérience d'après, enrichit par la profession bancaire. (P11.1)

Codage du Segment 12 (§12) :

Pourquoi je travail ? (P12.1)

Je travaille pour gagner ma vie, pour élever ma famille d'une part, et parce que j'ai envie de travailler sur ces domaines-là, parce que ça m'intéresse, d'autre part. (P12.2)

Mais bon, je travaille parce que j'ai besoin de travailler pour gagner ma vie comme tout le monde. (P12.3)

Codage du Segment 13 (§13) :

Justement ? Euhhhh, je n'en sais rien. (P13.1)

Il pourrait y avoir une dizaine de directions. (P13.2)

Codage du Segment 14 (§14) :

Sécurité internet, risque de fraude, risque d'attaques, risque de fuites de données, risque d'arrêt d'activité, risque de cyber malveillant, risque cyber fraude. (S14.1)

Je pense au risque, mais je pense aussi à autre mesure pour réduire ce risque. (S14.2 et P14.1)

On pense aussi déjà à des menaces. (P14.2)

Il y a plusieurs types de menaces sur la cybersécurité. (P14.3)

Et comme ça, il y a spontanément, la cyber criminalité, tout ce qui tourne des escrocs. (P14.4)

On a aussi ce qu'on appelle le cyber activisme, c'est-à-dire des gens qui veulent nuire fortement à l'image de l'entreprise. (S14.3 et P14.5)

Et pourquoi pas, ça c'est une autre catégorie une peut plus rare, en tant que petit établissement qu'on soit menacé, on a le cyber terrorisme qui se développe aussi avec l'aide éventuellement de cyber mercenaire. (S14.4 et P14.6)

Je pense à des menaces lorsque vous me posez cette question. (P14.7)

Je pense aussi à la nécessité de préserver notre patrimoine informationnel, nos systèmes d'informations. (P14.8)

Aussi, je pense à 4 piliers que sont :

- La disponibilité des systèmes d'informations
- L'intégrité de nos systèmes d'informations c'est ce que nos données ne soient pas détournées ou modifiées.
- La confidentialité c'est tout ce qui tourne autour du risque de fuite de données.
- La preuve c'est à dire obtenir des traces qui nous permettent de répondre à nos clients, si jamais ne on avait des soucis sur nos systèmes d'informations. (S14.5)

La cyber sécurité, pour moi, c'est un sous-ensemble de ce qu'on appelle la sécurité des systèmes d'informations au sens large, la « SSI ». (P14.9)

La cyber sécurité est un élément à l'intérieur de la sécurité des systèmes d'informations et un élément très important, un enjeu majeur en termes de risque, pas seulement pour la banque populaire « Val de France », mais pour tous les établissements bancaires. (S14.6 et P14.10)

C'est un risque majeur identifié par la « BCE », c'est-à-dire la banque centrale européenne. (A14.1)

Codage du Segment 15 (§15) :

Ouais, déjà, je vous rappelle un peu de notre propre organisation dans le groupe BPCE. (A15.1)

Oui, oui, il y a un opérateur informatique qui est IBP, Vous avez eu l'occasion de discuter avec le responsable de l'audit IBP. (A15.2)

Et il y a BPCIT l'opérateur informatique pour la profession informatique, donc les alertes, des cybers attaques viennent d'eux, de ces opérateurs. (A15.3)

Et dans la banque, on se met en cas d'attaque, on se met en mode de gestion de crise avec tous métiers qui sont concernés dans la banque pour faire face à l'attaque et pour appliquer des mesures, des contres mesures qui vont nous être demandées par les opérateurs informatiques d'une part, et dans la pilule de crise, on a aussi le métier de communication qui communiquera si nécessaire aux collaborateurs de la banque et ou aux clients, s'il y a des attaques sur les clients. (S15.1)

Codage du Segment 16 (§16) :

Moi, personnellement, en tant que responsable de la sécurité des systèmes d'information en cas de crise et moi qui réunirait la cellule de crise avec tous les métiers dont je vous ai parlé tout à l'heure. (S16.1)

Et c'est moi qui fais l'interface entre ces métiers et les opérateurs informatiques. (S16.2 et A16.1)

Codage du Segment 17 (§17) :

Oui selon un protocole. (S17.1)

Alors, normalement, il y a un protocole de gestion de crise au niveau des opérateurs informatiques qui lorsqu'ils sont avertis d'une cyberattaque importante. (S17.2 et A17.1)

Ils réuniraient les RSSI des établissements rattachés à ces opérateurs. (S17.3)

En cellule de crise, charge après au responsable de la sécurité des systèmes d'information d'établissements de réunir sa propre cellule de crise dans l'établissement. (S17.4)

Codage du Segment 18 (§18) :

Les difficultés. (S18.1)

La difficulté est bien et de bien analyser les impacts que ce soit pour les collaborateurs ou les clients. (S18.2)

De bien analyser les risques, de bien soigner sa communication, la communication, c'est important que ce soit vers les collaborateurs pour qu'ils ne fassent pas des choses qui aggraverait la situation ou vis à vis des clients, surtout si l'indisponibilité du service consécutif à cette cyber attaque. (P18.1 et A18.1)

Codage du Segment 19 (§19) :

C'est ce que je vous ai expliqué plutôt le travail des opérateurs informatiques. (A19.1)

On confit notre informatique à un opérateur et c'est eux qui sont en charge de mettre en place des contres mesures pour éviter le risque de cyber attaque. (P19.1 et A19.2)

Codage du Segment 20 (§20) :

Oui, Pascal Gombert a raison. (A20.1)

Dans chaque établissement, on a nommé un responsable de la sécurité des informations pour la BPVF : c'est moi. (S20.1)

La banque populaire, c'est-à-dire le groupe « BPCE », organise la filière sécurité des systèmes d'information, et parmi la politique de sécurité des systèmes d'information, chaque établissement doit désigner un responsable de la sécurité des systèmes d'information, un « RSSI ». (P20.1 et A20.2)

Et c'est à moi de mettre en place, de faire appliquer la politique de sécurité des systèmes d'information par les collaborateurs, car c'est à moi de faire la sensibilisation des collaborateurs aux comités des risques qui nous passent sur des liens. (S20.1 et A20.2)

Mais quand vous me posez la question qui est responsable de la cyber sécurité sur nos infrastructures informatiques, ce sont les opérateurs informatiques. (A20.3)

Codage du Segment 21 (§21) :

Non, quand je vous parle des opérateurs informatiques, ce sont les collaborateurs du groupe BPCE-IT. (A20.1 et S20.1)

C'est une structure à part entière responsable du service informatique de toutes les banques populaires et de toutes les caisses d'épargnes qui font partie du groupe BPCE. (S20.2)

Codage du Segment 22 (§22) :

Oui, on a des modules de formation que les collaborateurs suivent. (S22.1)

On a dispositif de sensibilisation des collaborateurs, parce qu'on sait très bien en termes de cybersécurité, l'une des vulnérabilités la plus importante c'est l'humain. (P22.1)

C'est les hommes plus que les machines. (P22.2)

Donc, on a un programme de sensibilisation des collaborateurs qui est assez important, avec qui est baser avec des « E-Learning », des formations, ou qui est baser sur des campagnes de sensibilisation, et il y a aussi au niveau national, des campagnes de sensibilisation qui sont réaliser. (S22.3 et A22.1)

Il y a des petits films qui sont faits, des petites vidéos qui sont construites au niveau national, puisqu'il y a une organisation en France, avec ce qu'on appelle l'ANSSI, l'agence nationale de la sécurité des systèmes d'informations qui met à dispositions aussi des guides de sensibilisations. (A22.2)

Oui, on a une formation parmi toutes les autres formations, à la banque, surtout à la sensibilisation pour dire à nos collaborateurs, ne cliquer pas sur les liens de suspects, comme on dit pour le client le reste… (S22.4)

Codage du Segment 23 (§23) :

Oui, on a mis en place un comité interne de sécurité. (S23.1)

On prépare les incidents et on intervient sur ce domaine. (S23.2)

Codage du Segment 24 (§24) :

Surtout par la sensibilisation des collaborateurs à mon niveau. (P24.1 et A24.1)

C'est Surtout par la sensibilisation des collaborateurs, pour appliquer des règles de sécurité, et pour ne pas se faire piéger par des attaques de phishing, à vocation… (P24.2 et A24.2)

C'est aussi participer à mener des plans d'action pour réduire ce risque de cyber sécurité. (P24.3)

Codage du Segment 25 (§25) :

Oui. Il faut répéter, répéter, répéter. (P25.1)

Codage du Segment 26 (§26) :

Oui. Elle est assurée par BPCE-IT. (A26.1)

Oui. Elle est assurée au niveau des opérateurs informatiques. (A26.2)

Codage du Segment 27 (§27) :

On travaille ensemble à deux niveaux. (S27.1)

Premier niveau, on a le groupe BPCE, admit la filière des RSSI avec des comités de suivi réguliers trimestriels et réellement où les plans d'action des actualités nous sont donnés. (S27.2 et A27.1)

Ça c'est au niveau de l'animation par BPCE de la filière des RSSI. (S27.3 et A27.2)

Et du temps. (P27.1)

Et donc, parmi cette animation, il y a tous les RSSI, bien réfléchi les opérateurs, des débiteurs logiciels. (S27.4)

Et en deuxième niveau, au niveau quotidien, nous recevons ces informations, par mail, du groupe BPCE sur ces questions de sécurité, dès lors des alertes, dès lors des clients qui s'ont piégé... (S27.5 et A27.3)

Codage du Segment 28 (§28) :

Les auditeurs peuvent mener des missions d'audit sur la cybersécurité, et m'interviewé comme ils interviewent les autres départements de banque. (A28.1)

Dans un autre sens, moi je n'ai pas de relation avec l'audit. (S28.1)

Codage du Segment 29 (§29) :

Là ce n'est pas le choix qui a été fait par le groupe BPCE parce que l'audit est un contrôle périodique dans le dispositif de contrôle permanent qui s'applique en France. (A29.1 et S29.1)

L'audit est une structure qui fait du contrôle périodique et non pas du contrôle en permanence. (A29.2)

Donc je ne pense pas qu'il doit adapter le fait que l'audit est confié à maintenir la cyber sécurité. (P29.1)

L'audit peut faire des missions périodiques sur les apparts de la cyber sécurité mais ne pas la maintenir en totale. (29.3 et P29.2)

Je pense que le traitement opérationnel de la sécurité des systèmes d'information doit être au plus près des métiers. (P29.4)

Il faut que ce soit très opérationnel par des gens qui ont des expertises et une connaissance de la sécurité des systèmes d'information. (P29.5)

Le « RSSI », lui il intervient en deuxième niveau sachant que les opérationnels de la sécurité interviennent en premier niveau. Le « RSSI » doit réaliser un certain niveau de contrôle pour s'assurer que le premier niveau est bien réalisé. (P29.6)

L'audit, de mon point de vue, c'est la règlementation des contrôles qui, en France et en Europe, comme je vous l'ai dit intervient en troisième niveau, et effectue des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. (A29.3 Et S29.1)

Donc, l'audit n'est pas dans un rôle opérationnel, mais effectue des missions en troisième niveau qui peuvent être beaucoup plus longues et plus approfondies mais ne sont pas dans le traitement opérationnel. (A29.4)

Ils vont s'assurer que les dispositifs fonctionnent, qu'il n'y a pas de failles ou s'il y a des failles, ils vont émettre des recommandations. (A29.5)

Mais ils ne sont pas dans le quotidien de la cyber sécurité. (A29.6)

Ce n'est pas l'organisation du contrôle qui existe chez nous en France, où l'audit est en troisième niveau, il n'est pas en opérationnel sur la sécurité des systèmes d'information. (P29.7 et A29.7)

Codage du Segment 30 (§30) :

On l'appréhende très au sérieux justement par une organisation qu'on espère est efficace, où on a mis en place au niveau « BPCE », encore une fois une politique de sécurité des systèmes d'information, c'est-à-dire une politique à plusieurs niveaux au moins à deux niveaux. (S30.1)

Le premier niveau, c'est une charte ou un cadre de fonctionnement de la sécurité des informations qui dit comment on doit être organisé : (S30.2)

Quel est le rôle du « BPCE » ? (A30.1)

Quel est le rôle des opérateurs informatiques ? (A30.2)

Quel est le rôle des établissements bancaires ? (A30.3)

A l'intérieur de chacune de ces structures, comment on doit être organisé ? (S30.2)

Comment on doit échanger ? (S30.3)

Quels outils on doit mettre en place ? (S30.4)

C'est le premier niveau et c'est la charte de fonctionnement, le cadre d'application pour dire que tous les établissements doivent respecter de manière homogène pour lutter contre la cybersécurité. (S30.5)

Le deuxième niveau de la politique, c'est un référentiel de règles de la sécurité des systèmes d'informations qui s'appliquent à tous les établissements du groupe « BPCE » et un certain nombre de règles que je ne peux pas tous les citer. (S30.6 et A30.4)

Évidemment, il y a plusieurs centaines qui vont vous dire par exemple : (S30.7)

- Qu'un mot de passe doit faire tant de caractères pour être suffisamment robuste dans tous les établissements du groupe. (S30.8)
- Que les proxys doivent être installés là où c'est nécessaire. (S30.9)
- Que les messageries doivent être sécurisées. (S30.10)
- Que dans tous les domaines de l'informatique, des règles de sécurité doivent être appliqués, c'est-à-dire c'est le deuxième niveau de la politique de sécurité des systèmes d'information, au-dessous du cadre qui fixe le fonctionnement. (S30.11)

Donc, on appréhende ce risque surtout, par une politique d'une part, on appréhende aussi ce risque par … (S30.12)

Codage du Segment 31 (§31) :

Avec les règles de sécurité qui doivent être appliqués et les normes en place, et justement dans ces règles de fonctionnement, il y a aussi des structures qui s'occupent de lutter au quotidien contre la cybersécurité, avec ce qu'on appelle des « SOC », centre opérationnel de sécurité qui font de la veille sur tout ce qui est menace, tout ce qui vulnérabilité, et qui mènent des actions de réduction des risques au quotidien. (S31.1 et A31.1)

Codage du Segment 32 (§32) :

En établissement bancaire, « BPVF », non. (P32.1)

Au niveau du groupe au des autres banques, il y a des attaques comme dans toutes les entreprises. (S32.1)

On a cité « WannaCry » en 2007 qui a touché toutes les entreprises, mais ces attaques, n'ont pas eu d'impact important, en tout cas, au niveau du groupe « BPCE ». (A32.1 et S32.2)

Mais il a fallu bien y répondre, mettre les patches nécessaires, mettre les correctifs de sécurité nécessaires. (S32.3)

Donc, il y a des attaques. (S32.4)

Il en y a régulièrement en ransomware. (S32.5)

Mais, il y en n'a pas eu pour le groupe « BPCE » d'impacts importants jusqu'à présent. (S32.6 et A32.2)

Codage du Segment 33 (§33) :

Oui, c'est comme la sécurité est un métier d'expert, les auditeurs internes dans une banque sont généralistes dans les effets bancaires. (A33.1)

Dans notre banque, il y a un audit interne à la banque qui intervient pour tous les domaines de la banque. (A33.2)

Mais sur ces sujets-là de cyber sécurité, on peut faire appel à des auditeurs externes qui ont une compétence technique particulière qu'on n'aurait pas forcement dans nos établissements sur ces sujets-là. (A33.3 et S33.1)

Aujourd'hui, si on veut faire des tests d'intrusion sur des systèmes d'informations, on fait des appels à des auditeurs externes. (S33.2 et A33.4)

Codage du Segment 34 (§34) :

Si on décide, ou lorsque les opérateurs décident de faire des tests d'intrusion sur les systèmes, et qu'ils choisissent un auditeur externe. (S34.1 et A34.1)

Ils vont bien sûr travailler avec cet auditeur externe. (A34.2)
Ils vont définir ensemble le périmètre de ce qu'ils souhaitent auditer. (A34.3)
Ils vont définir ensemble les modalités, le planning, ce qu'ils attendent. (A34.4)
Codage du Segment 35 (§35) :
A ma connaissance, dans nos établissements, les décisions menées des audits sur les systèmes d'information sont faites par l'audit interne ou l'inspection générale du groupe « BPCE ». (S35.1 et A35.1)
Or au niveau de groupe « BPCE », l'audit interne est appelé l'inspection générale. (A35.2)
Elle peut décider de faire appel à des auditeurs externes. (A35.3 et S35.2)
Mais en règle générale, la décision de faire un audit sur ces sujets-là, elle est confiée à l'inspection générale qui peut alors faire appel à un auditeur externe ou inspection externe. (S35.3 et A35.4)
En revanche, ce qui peut être demandé par l'administration, mais ce qui sera chez nous, le régulateur, la « BCE » banque centrale européenne, elle pourrait exiger qu'on effectue des tests d'intrusion par exemple selon certaines conditions. (S35.4)
Elle peut fixer les conditions de l'audit ce que doit contenir l'audit, quelle est le résultat attendu de l'audit. (S35.5)
Mais sur le choix de l'auditeur, je ne pense pas. (S35.6)
Codage du Segment 36 (§36) :
Très peu de relation. (S36.1)
Quand il y a des missions d'audit de nos domaines, ils viennent nous interviewés. (S36.2)
Mais si non, il y a très peu de relation. (S36.3)
Codage du Segment 37 (§37) :
Je les vois une fois par an, mais c'est tout à fait ça. (S37.1)
Codage du Segment 38 (§38) :
Pas de relation. (P38.1)
Codage du Segment 39 (§39) :
Oui, sur le domaine de la sécurité des systèmes d'information, on a des interlocuteurs dans les différents métiers de l'informatique plutôt, puisqu'on a des relations régulières avec les gens qui s'occupent des habilitations, les contrôles d'accès par exemple, on a des relations régulières avec les gens qui s'occupent des développements privatifs. (S39.1)
On a des accès réguliers avec les gens qui s'occupent de l'informationnel c'est-à-dire les entrepôts de données, tout ce qui peut générer des programmes particuliers. (S39.2)
Enfin, le RSSI que je suis, à des relations avec les différents métiers qui s'occupe de l'informatique dans la banque. (S39.3)
Codage du Segment 40 (§40) :
Vous devez demander cette question à l'audit. (P40.1)
Pas vraiment d'avis sur la question. (P40.2)
Codage du Segment 41 (§41) :
Oui, c'est une question de domaine, ou ça évolue assez vite, il faut s'adapter en permanence. (P41.1)
Codage du Segment 42 (§42) :
En se formant déjà, en faisant de la veille, savoir ce qui se passe, en identifiant régulièrement les nouveaux risques, avec encore une fois des opérateurs informatiques, bien sûr. (P42.1)
Et en sensibilisant en fait sur l'audit. (P42.2)
Codage du Segment 43 (§43) :

Moi, je n'ai pas connaissance d'expert d'orange cyber défense qui viennent à la banque faire une formation. (A43.1)
Mais, peut être chez les opérateurs informatiques et pas à la BPVF. (A43.2)

Codage du Segment 44 (§44) :

Oui, on peut envisager de ce qu'on discute tout à l'heure, de faire intervenir des sociétés spécialisées en sécurité informatique pour faire par exemple des tests d'intrusion, sur notre périmètre relatif. (S44.1)
Pas au niveau de la banque populaire « Val de France », mais au niveau encore une fois du groupe « BPCE », ils font intervenir des experts puisqu'on travaille avec des prestataires de services qui sont experts en sécurité informatique. (A44.1 et S44.2)
Les entreprises, pas seulement les banques, s'entourent des prestataires de services, spécialisés dans la cybersécurité, pour travailler justement à réduire ces risques. (S44.3)

Codage du Segment 45 (§45) :

En règle générale, c'est quelqu'un sérieux qui vient et qui a bien préparer son entretien. (A45.1)
C'est-à-dire il arrive avec un certain nombre de questions, ils viennent toujours par deux, une équipe de deux auditeurs. (A45.2)
Mais, les relations avec les auditeurs sont bonnes en général, je crois qu'il n'y a pas de pièges. (A45.3)
Sur une mission d'audit, soit sur une cyber sécurité ou pas, il y a deux auditeurs qui demandent un certain nombre de questions et qui suivent un guide d'audit et qui viennent nous interviewés en nous posant un certain nombre de questions, pour écrire après les réponses, pour se faire une idée des risques et des éventuelles recommandations à formuler. (A45.3 et S45.1)
Ensuite, on se met d'accord avec les auditeurs sur les recommandations, qui nous sont affecter et après on met en œuvre les recommandations, il y a un suivi de recommandation qui est fait par les auditeurs. (A45.4 et S45.2)

Codage du Segment 46 (§46) :

Ce sont des gens avec de général connaissances des processus à faire. (A46.1)
Ce ne sont pas des spécialistes, une bonne connaissance des métiers bancaires, et ils ont des attitudes à bien communiquer, ils ont des attitudes à bien analyser, à bien identifier les risques. (A46.2)

Codage du Segment 47 (§47) :

Alors ils ne sont pas forcément peur ou intimidés, mais en règle générale, les collaborateurs ont crainte d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre, et ces recommandations à mettre en œuvre sont des moyens à engager qu'on n'a pas forcement tout le temps. (S47.1 et A47.1)

Codage du Segment 48 (§48) :

Il faut avoir un bon relationnel, se respecter. (P48.1)

Codage du Segment 49 (§49) :

Pour les autres les métiers autre que l'audit, on a mis en place des lieux d'échange trimestrielle, qu'on appelle des comités de sécurité des systèmes d'information, où on échange sur les différents sujets d'actualités, sur les différentes actions à mener. (S49.1)
Donc, on a des lieux d'échange avec les différents métiers. (S49.2)

Codage du Segment 50 (§50) :

Pour qu'ils s'approprient des enjeux, il faut qu'ils soient sensibilisés bien sûr, il faut les éclairer sur les risques, sur ce qui pourrait arriver si jamais on ne mettait pas en œuvre les politiques et les moyens pour réduire les risques de cyber sécurité. (A50.1 et S50.1)
Donc, il faut éclairer les dirigeants pour qu'ils dégagent les moyens nécessaires. (A50.2)

Codage du Segment 51 (§51) :

Il y a des contrôles qui sont faits, il y a des formations qui sont réalisés. (S51.1)

Or les contrôles sont faits par des équipes de contrôle permanent de deuxième niveau. (S51.2)

En France, comme je vous l'ai dit, il y a trois niveaux : (S51.3)

Il y a les métiers qui réalisent des contrôles de premier niveau. (S51.4)

Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits. (S51.5)

Et puis, il y a l'audit en troisième niveau, comme on disait tout à l'heure, qui effectue des missions ponctuelles, périodiques. (S51.6 et A51.1)

Classement des unités codées : Recodage

Q. Les séquences-types de l'entretien de Didier G.

Nous allons maintenant regrouper et ordonner les séquences dans l'ordre chronologique depuis le départ (S0) jusqu'à la fin de l'entretien (S+). Nous allons joindre toutes les unités concernées (tous les S) en leur donnant un titre résumant leur contenu.

Nous avons divisé l'entretien de Didier G. en six séquences respectives selon l'ordre chronologique.

20. Niveau de formation et progression de la carrière

S0=S1.1+S1.2+S1.3+S2.1+S4.1+…+S4.6

21. Fonction de RSSI : Rôle et missions en sécurité informatique

Sa=S3.1+S3.2+S5.1+S5.3+S6.1+S20.1+S35.4+S39.3+S49.1+S49.2

22. Cybersécurité : contrainte et implication

Sb=S14.1+…+S14.6+S17.2+S18.1+S18.2

23. Responsabilité en cybersécurité et par rapport aux cyberattaques

Sc=S5.2+S15.1+S16.1+S16.2+S17.3+S17.4+S20.1+S20.2+S24.1+S27.4+S32.1+…+S32.6+S35.1+S35.2+S39.1+S39.2+S44.1+S44.2+S44.3

24. Politiques et actions pour essayer de maintenir la cybersécurité

Sd=S22.1+S22.3+S22.4+S23.1+S23.2+S27.1+S27.2+S27.3+S27.5+S30.1+S30.2+…+S30.12+S31.1+S33.1+S33.2+S34.1+S50.1+S51.1+…+S51.6

25. Audit interne : Définition et relation avec la cybersécurité

Se=S28.1+S29.1+S29.3+S35.6+S36.1+S36.2+S36.3+S37.1+S45.1+S45.2+S47.1

Nous allons maintenant proposer un premier résumé des séquences-types de l'entretien de Didier G. après avoir effectué le regroupement selon un ordre chronologique.

Résumé des séquences-types de l'entretien de Didier G.

Didier G. nous explique son parcours professionnel puis sa progression de carrière dans la BPVF. Il a commencé par obtenir un baccalauréat en France puis il a passé les examens bancaires. Il est arrivé à la BPVF par opportunité. Son parcours s'étend sur 30 ans dans le secteur bancaire où il a progressé chronologiquement du responsable du traitement des chèques au moyen de paiement, au responsable de la monnaie, au responsable de l'ensemble des moyens de paiement jusqu'à s'occuper de risques opérationnels pour être enfin installé dans le poste de RSSI.

En tant que RSSI, Didier explique qu'il est responsable des risques opérationnels et ceux de la sécurité des systèmes d'information. Il annonce que le RSSI doit avoir de bonne connaissance des métiers bancaires. Il doit avoir un bon relationnel avec les métiers. Didier attire l'attention que le RSSI n'est pas expert en sécurité informatique au sein de la BPVF. Il limite son rôle à réaliser des développements internes et à sensibiliser tous les collaborateurs aux comités des risques. Didier affirme qu'il n'a pas de relation avec les auditeurs internes. Mais, il assiste à des lieux d'échange avec les différents métiers comme le comité de sécurité des systèmes d'information, où il échange sur les différents sujets d'actualités, sur les différentes actions à mener.

Didier explique que la cybersécurité englobe la sécurité internet, risque de fraude, risque d'attaques, risque de fuites de données, risque d'arrêt d'activité, risque de cyber malveillant, risque cyber fraude. Son rôle est de chercher à comment réduire ce risque qui est un élément essentiel relatif à la sécurité des systèmes d'informations. Il essaye d'agir contre la cybersécurité selon un protocole de gestion de crise au niveau des opérateurs informatiques qui lorsqu'ils sont avertis d'une cyberattaque importante.

G. affirme que la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique par des opérateurs informatiques. En cas d'attaque, il parle d'une cellule de crise guidée par les opérateurs informatiques qui va se réunir et qui contient tous les métiers concernés **(L'audit interne n'est pas un métier concerne selon lui)** pour faire face à l'attaque. Il limite sa responsabilité à réunir la cellule de crise et faire l'interface avec les opérateurs informatiques. G. explique qu'il y a toujours des attaques mais qui n'ont pas eux d'impacts importants jusqu'à présent.

Il éclaircit que l'inspection générale est en charge de choisir si l'audit interne doit mener un audit sur les systèmes d'information. Sur les missions d'audit sur la sécurité informatique, il approuve le recours à des sociétés spécialisées en sécurité informatique, des experts, des prestataires de services qui sont experts en sécurité informatique, pour faire pour travailler justement à réduire ces risques et par exemple faire des tests d'intrusion.

Pour faire face à la cybersécurité, Didier approuve un programme de sensibilisation des collaborateurs qui est assez important, avec des « E-Learning », des formations, et qui est baser sur des campagnes de sensibilisation. Il annonce l'existence d'un comité interne de sécurité qui se prépare contre les incidents et qui intervient sur la cybersécurité. Il introduit deux niveaux :

- Le premier contenant le groupe BPCE, la filière des RSSI, le comité de suivi.
- Le deuxième contenant le RSSI qui agit sur des missions de sécurité quotidienne relative à la sécurité des clients qui ont été piégé.

Pour être efficace contre la cybersécurité, Il parle aussi d'une politique de sécurité des systèmes d'information, qui se constitue d'une charte de fonctionnement de la sécurité des informations qui dit comment on doit être organisé, et d'un référentiel de règles de la sécurité des systèmes d'informations qui s'appliquent à tous les établissements du groupe « BPCE ».

G. introduit aussi le centre opérationnel de sécurité « COC » qui font de la veille sur tout ce qui est menace, tout ce qui vulnérabilité, et qui mènent des actions de réduction des risques au quotidien.

Il insiste sur son rôle de sensibilisation pour réduire les risques de cybersécurité.

Il termine en expliquant les trois niveaux présents en France :

- Les métiers de contrôle de premier niveau.
- Les structures de contrôle permanent qui réalisent des contrôles de deuxième niveau.
- L'audit interne qui effectue des missions ponctuelles et périodiques en troisième niveau.

En ce qui concerne l'audit interne, Didier confirme le rôle de l'audit en troisième niveau en effectuant des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. Il les décrits comme des personnes sérieuses et qui ont bien préparer leur entretien. Ils ont de général connaissances des processus à faire. Ils ne sont pas des spécialistes, mais ils ont une bonne connaissance des métiers bancaires, et ils ont des attitudes à bien communiquer, ils ont des attitudes à bien analyser, à bien identifier les risques. Il termine en disant que les collaborateurs ont crainte des auditeurs internes parce qu'il s'agit de recommandations à mettre en œuvre.

R. <u>Les actants du récit de Didier G.</u>

Nous allons ici identifies les personnages dans le récit de Didier G. Nous allons inclure Didier lui-même lorsqu'il se dédouble (« moi, je…).

Nous notons respectivement les acteurs de A1 jusqu'à An.

Le premier actant du récit est Didier lui-même puisqu'il a utilisé le « moi » 9 fois.

Le second actant sont les opérateurs informatiques de l'I-BP.

A2=A5.1+A5.3+A15.2+A15.3+A16.1+A17.1+A19.1+A19.2+A20.3+A21.3+A26.2+A30.2+A34.1+A34.2+A34.3+A36.4+A43.2

Le troisième actant est le groupe BPCE.

A3=A5.2+A15.1+A20.2+A26.1+A27.1+A27.2+A29.1+A30.1+A30.3+A30.4+A33.2+A44.1

Le quatrième actant est la BCE.

A4=A14.1

Le cinquième actant est le poste de RSSI

A5=A18.1+A20.2+A22.1+A24.1+A24.2+A27.3+A43.1+A45.3+A50.2

Le sixième actant est Monsieur Pascal GOMBERT qui est directeur des risques conformité et contrôle permanent dans la BPVF.

A6=A20.1

Le septième actant est l'ANSSI.

A7=A22.2

Le huitième actant est les auditeurs internes.

A8=A28.1+A29.2+A29.3+A29.4+A29.5+A29.6+A29.7+A33.1+A33.2+A35.1+A35.2+A35.3+A35.4+A45.1+A45.2+A45.3+A45.4+A46.1+A46.2+A50.1+A51.1

Le neuvième actant est le centre opérationnel de sécurité.

A9=A31.1

Le dixième actant est la cyberattaque WannaCry.

A10=A32.1

Le onzième actant est l'auditeur interne.

A11=A23.1+A26.2+A26.3+A26.4+A26.5+A26.8+A26.9+A26.11+A32.1+A32.2+A32.3+A32.4+A32.5+A32.6+A32.7+A32.8+A32.9+A32.10+A32.11+A33.1

Le douzième actant est l'audités.

A12=A47.1

<u>Les actants du récit de Didier G.</u>

Le premier actant est G. lui-même. Nous remarquons qu'il a fréquemment utilisé le « moi » dans son récit pour donner son avis ou son opinion puisqu'il est directement lié à la cybersécurité grâce à son travail.

Le deuxième actant sont les opérateurs informatiques de l'I-BP. Selon G., ils pilotent la sécurité des systèmes d'information et ils sont experts en sécurité informatiques et lui transmettent les alertes de cyberattaques. G. explique que c'est eux qui sont responsable d'assurer la cybersécurité dans la BPVF en mettant des contres mesures pour éviter le risque de cyber attaque. Ces opérateurs appellent des auditeurs externes pour faire des tests d'intrusion sur les systèmes informatiques qui sont plus experts que les auditeurs internes sur ces domaines-là.

Le troisième actant est la BPCE qui a une politique interne de désigner un RSSI pour chaque établissement comme la BPVF. La BPCE joint une filière des RSSI avec des comités de suivi réguliers pour surveiller la cybersécurité. Elle a fait intervenir des experts, des prestataires de service qui sont experts en sécurité informatique au niveau de la cybersécurité.

Le quatrième actant est la banque centrale européenne BCE. Elle identifie la cybersécurité comme un risque majeur à identifier.

Le cinquième actant est le poste de RSSI qui est responsable selon Mr. Gombert de maintenir la cybersécurité dans la banque. Didier quant à lui, il limite son rôle à la sensibilisation des collaborateurs en cybersécurité, et à la mise en place et l'application des politiques de sécurité des systèmes d'information par les collaborateurs. Il n'a pas de relation avec les auditeurs internes ni avec les experts qui viennent à la banque pour intervenir en cybersécurité. Sa relation se limite aussi aux opérateurs informatiques qui lui transmets des alertes et des informations pour agir en cas de cyber attaque.

Le sixième actant est Mr Gombert qui insiste que Didier G. doive être responsable de maintenir la cybersécurité dans la banque. Et Didier agrée de ce que Pascal a affirmé.

Le septième actant est l'agence nationale de la sécurité des systèmes d'information. G. annonce qu'elle joue un rôle important au niveau national à la sensibilisation à la cybersécurité grâce à des petits films, petits vidéos et des guides de sensibilisation à la cybersécurité.

Le huitième actant sont les auditeurs internes. Didier explique que l'audit est un contrôle périodique qui peut faire des missions périodiques sur les apparts de la cyber sécurité mais ne pas la maintenir en totale. Il qualifie l'interférence de l'audit en troisième niveau y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. G. assure que l'audit n'est pas opérationnel et plus spécifiquement sur la cybersécurité car les auditeurs sont généralistes et ne sont pas experts en cybersécurité.

G. ajoute que l'audit interne peut décider de faire appel à des auditeurs externes sur des sujets techniques de cybersécurité et qui ont besoin d'une certaine expertise que l'audit n'a pas. Didier décrit l'auditeur interne comme quelqu'un sérieux et qui à bien préparer son entretien, qui a des général connaissance des processus à faire. Lui, il collabore avec les auditeurs internes lors des missions d'audit et lors de la mise en œuvre des recommandations. Il réexplique qu'ils ne sont pas spécialistes mais ont une bonne connaissance des métiers bancaires, et ils ont des attitudes à bien communiquer, ils ont des attitudes à bien analyser, à bien identifier les risques.

Le neuvième actant est le centre opérationnel de sécurité « COS » qui lutte au quotidien contre la cybersécurité, en veillant sur tout ce qui est menace, tout ce qui vulnérabilité, et en menant des actions de réduction des risques au quotidien.

Le dixième actant est la cyberattaque *« Wanna Cry »* qui a touché la BPVF mais selon Didier elle n'a pas aucun impact important sur elle.

Le onzième actant sont des auditeurs externes qui sont appelés pour intervenir en cybersécurité parce qu'ils ont des compétences techniques particulières qui ne sont pas disponible à la BPVF chez les auditeurs internes.

Le douzième actant sont les collaborateurs ou les audités. G. affirme qu'ils ont crainte d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre et c'est comme un examen du travail des collaborateurs.

S. Les classes d'arguments

Ce niveau d'analyse concerne l'ensemble des arguments, démonstrations et propositions de Didier G. destinés à nous convaincre. Nous allons regroupés l'ensemble des unités codées en P selon des « classes d'arguments » dont chacune représente une étape logique dans un raisonnement.

Nous allons classer les arguments le type de raisonnement que Didier présente dans ces réponses. Nous en avons repéré cinq qui font l'objet d'arguments explicites qui sont à la base de ce classement.

Nous avons noté (P1) les propositions de Didier associé à son travail dans la banque jusqu'à être le RSSI. Il a expliqué son trajet comme étant une suite logique pour arriver dans son présent poste et que c'était une bonne banque à valeur humaine et à proximité de son domicile et c'est pourquoi il l'a choisi.

- Parce que quand j'étais jeune, la banque **avait bonne réputation** et c'était un peu **la sécurité** dans travailler dans une banque. (P8.1)
- Parce que c'est une banque à taille humaine. (P9.1)
- Il y a des valeurs coopératives qui me correspondent bien. (P9.2)
- En plus, c'est à proximité de mon domicile. (P9.3)
- Oui, je pense. (P10.1)
- Oui, je crois mon expérience d'après, enrichit par la profession bancaire. (P11.1)
- Pourquoi je travail ? (P12.1)
- Je travaille pour gagner ma vie, pour élever ma famille d'une part, et parce que j'ai envie de travailler sur **ces domaines-là**, parce que **ça m'intéresse**, d'autre part. (P12.2)
- Mais bon, je travaille parce que j'ai besoin de travailler pour gagner ma vie comme tout le monde. (P12.3)
- Justement ? Euhhh, je n'en sais rien. (P13.1)
- Il pourrait y avoir une dizaine de directions. (P13.2)
- C'est une **suite un peu logique**. (P4.1)
- Je ne sais pas si je vous ai décrit notre organisation, du groupe « BPCE », parce que ça peut avoir un intérêt pour vous. (P5.2)
- Et d'avoir une bonne communication. (P5.4)
- Et de soigner le relationnel, les relations avec des gens, être rigoureux, organiser. (P5.5)

Nous résumons cet ensemble ainsi : *« La sécurité et les valeurs humaines du travail à la BPVF et l'envie d'avoir une carrière en informatique »*.

Nous avons noté (P2) les expressions et les formules associés à Didier G. RSSI en termes de cybersécurité. C'est-à-dire son rôle dans la BPVF et en relation avec la cybersécurité.

- « Dans la banque populaire, on a une petite structure qui fait **seulement** des développements internes. (S5.3) »
- « Et travailler en mode transversale, travailler en équipe. (P5.3) »
- « Les qualités requises c'est une bonne connaissance des métiers bancaires, et en particulier des métiers qui tournent autour des moyens de paiements, c'est un bon relationnel avec les métiers, puisqu'en fait, les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire, comme la BPVF, nous ***ne sommes pas des experts en sécurité informatique*** ». (P5.1 et S5.1)

- « De bien analyser les risques, de bien soigner sa communication, la communication, c'est important que ce soit vers les collaborateurs pour qu'ils ne fassent pas des choses qui aggraverait la situation ou vis à vis des clients, surtout si l'indisponibilité du service consécutif à cette cyber attaque. » (P18.1 et A18.1)
- Le « RSSI », lui il intervient en deuxième niveau sachant que **les opérationnels de la sécurité interviennent en premier niveau**. Le « RSSI » doit réaliser un certain niveau de contrôle pour s'assurer que le premier niveau est bien réalisé. (P29.6)
- Donc, on a un programme de sensibilisation des collaborateurs qui est assez important, avec qui est baser avec **des « E-Learning »**, **des formations**, ou qui est baser sur **des campagnes de sensibilisation**, et il y a aussi au niveau national, des campagnes de sensibilisation qui sont réaliser. (S22.3 et A22.1)
- Il y a des **petits films** qui sont faits, des petites vidéos qui sont construites au niveau national, puisqu'il y a une organisation en France, avec ce qu'on appelle **l'ANSSI**, l'agence nationale de la sécurité des systèmes d'informations qui met à dispositions aussi des guides de sensibilisations. (A22.2)
- Surtout par **la sensibilisation des collaborateurs à mon niveau**. (P24.1 et A24.1)
- C'est Surtout par **la sensibilisation des collaborateurs**, pour appliquer des règles de sécurité, et pour ne pas se faire piéger par des attaques de phishing, à vocation… (P24.2 et A24.2)
- C'est aussi participer à mener des plans d'action pour réduire ce risque de cyber sécurité. (P24.3)
- En se formant déjà, en faisant **de la veille**, savoir ce qui se passe, en identifiant régulièrement les nouveaux risques, avec encore une fois des opérateurs informatiques, bien sûr. (P42.1)
- Et **en sensibilisant** en fait sur l'audit. (P42.2)
- Oui. Il faut répéter, **répéter**, répéter. (P25.1)

Nous résumons cet ensemble ainsi : *« Le RSSI limite son travail en cybersécurité à la sensibilisation seulement en se basant sur le fait que sa fonction intervient en deuxième niveau en contrôle et surveillance »*.
Nous avons noté (P3) les expressions et les formules associés à qui est responsable d'assurer la cybersécurité selon Didier G. Il considère que l'humain est le maillon le plus faible dans la cybersécurité et qu'il n'a pas les compétences techniques en sécurité informatique.

- « Les qualités requises c'est une bonne connaissance des métiers bancaires, et en particulier des métiers qui tournent autour des moyens de paiements, c'est un bon relationnel avec les métiers, puisqu'en fait, les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire, comme la BPVF, nous ***ne sommes pas des experts en sécurité informatique*** ». (P5.1 et S5.1)
- On a dispositif de sensibilisation des collaborateurs, parce qu'on sait très bien en termes de cybersécurité, **l'une des vulnérabilités la plus importante c'est l'humain**. (P22.1)
- C'est **les hommes plus que les machines.** (P22.2)
- **Les experts en sécurité informatique** sont chez **les opérateurs informatiques** et ne sont pas dans les établissements comme une banque populaire. (A5.1)
- Et donc, la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique **par des opérateurs informatiques.** (S5.2 et A5.3)
- Je pense au risque, mais je pense aussi à autre mesure pour réduire ce risque. (S14.2 et P14.1)
- On pense aussi déjà à **des menaces**. (P14.2)
- Je pense à des menaces lorsque vous me posez cette question. (P14.7)
- Je pense aussi à la nécessité de préserver notre patrimoine informationnel, nos systèmes d'informations. (P14.8)

- On **confit <u>notre informatique à un opérateur</u>** et c'est eux qui sont ***<u>en charge</u>*** de mettre en place des contres mesures pour éviter le risque de cyber attaque. (P19.1 et A19.2)
- La banque populaire, c'est-à-dire le groupe « BPCE », organise la filière sécurité des systèmes d'information, et parmi la politique de sécurité des systèmes d'information, chaque établissement doit désigner <u>un responsable de la sécurité des systèmes d'information, un « RSSI »</u>. (P20.1 et A20.2)

Nous résumons cet ensemble ainsi : *« La cybersécurité est une menace humaine qui doit être assurée au niveau des opérateurs informatiques car le RSSI n'est pas expert en sécurité informatique, malgré que la BPVF l'a mis en charge pour cette mission dans sa politique de sécurité ».*

Nous avons noté (P4) les expressions et les formules relatives à la cybersécurité :

- « Il y a plusieurs types de **<u>menaces</u>** sur la cybersécurité. » (P14.3)
- « Et comme ça, il y a spontanément, la **<u>cyber criminalité</u>**, tout ce qui tourne **<u>des escrocs</u>**. » (P14.4)
- On a aussi ce qu'on appelle le **<u>cyber activisme</u>**, c'est-à-dire des gens qui veulent **<u>nuire</u>** fortement à l'image de l'entreprise. (S14.3 et P14.5)
- Et pourquoi pas, ça c'est une autre catégorie une peut plus rare, en tant que petit établissement qu'on soit menacé, on a le cyber terrorisme qui se développe aussi avec l'aide éventuellement de cyber mercenaire. (S14.4 et P14.6)
- La **<u>cyber sécurité</u>**, pour moi, c'est un sous-ensemble de ce qu'on appelle la sécurité des systèmes d'informations au sens large, la **<u>« SSI »</u>**. (P14.9)
- La **cyber sécurité** est un élément *<u>à l'intérieur de la sécurité des systèmes d'informations et un élément très important</u>*, <u>un enjeu majeur en termes de risque</u>, pas seulement pour la banque populaire « Val de France », mais pour tous les établissements bancaires. (S14.6 et P14.10)

Cet ensemble se résume ainsi : *« La cybersécurité est définie comme la sécurité des systèmes d'informations. Elle est liée à la cybercriminalité et aux cyberattaques qui créent des menaces et des escrocs au sein de l'entreprise ».*

Nous avons noté (P5) les expressions et les formules associés à la fonction d'audit interne.

- **L'audit** est une structure qui fait du <u>contrôle périodique</u> et non pas du contrôle en permanence. (A29.2)
- Donc je **ne** pense **pas** qu'il doit adapter le fait que **l'audit** est confié à <u>maintenir la cyber sécurité</u>. (P29.1)
- **L'audit** peut faire des <u>missions périodiques</u> sur les apparts de la cyber sécurité <u>mais ne pas la maintenir en totale</u>. (29.3 et P29.2)
- Je pense que le <u>traitement opérationnel</u> de <u>la sécurité des systèmes d'information</u> doit être au <u>plus près des métiers</u>. (Métiers d'informatique) (P29.4)
- Il faut que ce <u>soit très opérationnel</u> par des gens qui ont **<u>des expertises</u>** et une **<u>connaissance de la sécurité des systèmes d'information</u>**. (P29.5)
- **L'audit**, de mon point de vue, c'est <u>la règlementation des contrôles</u> qui, en France et en Europe, comme je vous l'ai dit intervient en troisième niveau, et effectue des missions thématiques sur un certain nombre de domaines, y compris dans **la cybersécurité**, puisqu'il y a <u>des audits sur la sécurité des serveurs</u>, <u>des audits sur la sécurité des infrastructures en générale</u>. (A29.3 Et S29.1)
- Ce n'est pas l'organisation du contrôle qui existe chez nous en France, où l'audit est en troisième niveau, il **n'**est **pas** en <u>opérationnel sur la sécurité des systèmes d'information</u>. (P29.7 et A29.7)
- En établissement bancaire, « BPVF », non. (P32.1)
- Au niveau du groupe au des autres banques, il y a des attaques comme dans toutes les entreprises. (S32.1)

- On a cité « WannaCry » en 2007 qui a touché toutes les entreprises, mais ces attaques, n'ont pas eu d'impact important, en tout cas, au niveau du groupe « BPCE ». (A32.1 et S32.2)
- **Pas de relation.** (P38.1)
- Vous devez demander cette question à l'audit. (P40.1)
- Pas vraiment d'avis sur la question. (P40.2)
- Oui, c'est une question de domaine, ou ça évolue assez vite, il faut s'adapter en permanence. (P41.1)
- Il faut avoir un bon relationnel, se respecter. (P48.1)
- Il y a les métiers qui réalisent des contrôles de premier niveau. (S51.4)
- Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits. (S51.5)
- Et puis, il y a **l'audit** en troisième niveau, comme on disait tout à l'heure, qui effectue **des missions ponctuelles**, **périodiques**. (S51.6 et A51.1)

Cet ensemble se résume ainsi : *« L'audit interne est une règlementation de troisième niveau qui réalise des missions périodiques sur tous les départements de la banque y inclus la cybersécurité. Mais l'audit ne peut pas assurer la cybersécurité puisqu'il n'est pas opérationnel ni il a les compétences et les expertises en sécurité informatique ».*
G. a mandaté le rôle d'assurance de la cybersécurité dans la banque aux opérateurs informatiques. Il explique que l'audit interne est faible en compétence et expertise technique dans ce domaine. Il admet que la cybersécurité est un métier qui a besoin de quelqu'un très opérationnel et qui de bonnes connaissances et expertises en sécurité informatique. Il admet aussi que son rôle en tant que RSSI se limite à la sensibilisation et à la réunion de la cellule de crise en cas d'attaque parce qu'il n'est de même pas experts en sécurité informatique.

T. Le schème provisoire de l'entretien

Nous allons tout d'abord restituer le schème en situant les arguments dans leur ordre d'intervention dans le récit et en les mettant en relation « spatiale » avec les deux autres classes d'unités précédemment recodées : les séquences et les actants. Nous allons les présenter dans ce tableau qui constituera un schème provisoire de l'entretien.

Séquences (Sn)		Arguments (Pn)	Actant (An)
Niveau de formation et progression de la carrière (S_0)	• J'ai passé un baccalauréat en France. (S1.1) • Et après, j'ai passé des examens bancaires. (S1.2) • Le Certificat d'aptitude professionnelle à la profession des banques et un brevet professionnel de banque de trois ans et j'ai fait la première année de l'Institut technique bancaire ITB. (S1.3) • J'ai trouvé ce travail, Euhhhh, en envoyant des CV dans plusieurs banques, et j'ai été retenu dans la banque populaire. (S2.1) • Mon parcours, ça a été un parcours à la profession bancaire pendant une trentaine d'année. (S4.1) • Donc, j'étais responsable du traitement des chèques au moyen de paiement. (S4.2) • Ensuite, j'étais responsable de la monnaie c'est-à-dire tout ce qui tourne autour des cartes bancaires. (S4.3) • Ensuite, j'étais responsable de l'ensemble des moyens de paiement, les chèques, les virements, les traitements, les cartes bancaires, les moyens de paiement internationaux. (S4.4) • Et on m'a fait opposition compte tenu de mes connaissances de production bancaire. (S4.5) • On m'a fait la proposition de m'occuper de risques opérationnels. (S4.6)	• Parce que quand j'étais jeune, la banque avait bonne réputation et c'était un peu la sécurité dans travailler dans une banque. (P8.1) • Parce que c'est une banque à taille humaine. (P9.1) • Il y a des valeurs coopératives qui me correspondent bien. (P9.2) • En plus, c'est à proximité de mon domicile. (P9.3) • Oui, je crois mon expérience d'après, enrichit par la profession bancaire. (P11.1) • Je travaille pour gagner ma vie, pour élever ma famille d'une part, et parce que j'ai envie de travailler sur ces domaines-là, parce que ça m'intéresse, d'autre part. (P12.2) • Mais bon, je travaille parce que j'ai besoin de travailler pour gagner ma vie comme tout le monde. (P12.3) • Il pourrait y avoir une dizaine de directions. (P13.2) • C'est une suite un peu logique. (P4.1)	• Le Moi. (Répété plusieurs fois).
Fonction de RSSI Rôle et missions en sécurité informatique (Sa)	• Alors je suis responsable des risques opérationnels, au sein de la direction des risques et du contrôle permanent et de la conformité de la BPVF. (S3.1) • J'ai également en charge les plans d'urgence et de poursuite d'activité et la sécurité des systèmes d'information. (S3.2) • Dans la banque populaire, on a une petite structure qui fait seulement des développements internes. (S5.3) • En effet, les autres métiers de la banque. (S6.1) • Dans chaque établissement, on a nommé un responsable de la sécurité des informations pour la BPVF : c'est moi. (S20.1) • En revanche, ce qui peut être demandé par l'administration, mais ce qui sera chez nous, le régulateur, la « BCE » banque centrale européenne, elle pourrait exiger qu'on effectue des tests d'intrusion par exemple selon certaines conditions. (S35.4) • Enfin, le RSSI que je suis, à des relations avec les différents métiers qui s'occupe de l'informatique dans la banque. (S39.3) • Pour les autres les métiers autre que l'audit, on a mis en place des lieux d'échange trimestrielle, qu'on appelle des comités de sécurité des systèmes d'information, où on échange sur les différents sujets d'actualités, sur les différentes actions à mener. (S49.1) • Donc, on a des lieux d'échange avec les différents métiers. (S49.2)	• Les qualités requises c'est une bonne connaissance des métiers bancaires, et en particulier des métiers qui tournent autour des moyens de paiements, c'est un bon relationnel avec les métiers, puisqu'en fait, les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire, comme la « BPVF », nous ne sommes pas des experts en sécurité informatique. (P5.1 et S5.1) • Le « RSSI », lui il intervient en deuxième niveau sachant que les opérationnels de la sécurité interviennent en premier niveau. Le « RSSI » doit réaliser un certain niveau de contrôle pour s'assurer que le premier niveau est bien réalisé. (P29.6) • On a dispositif de sensibilisation des collaborateurs, parce qu'on sait très bien en termes de cybersécurité, l'une des vulnérabilités la plus importante c'est l'humain. (P22.1) • C'est les hommes plus que les machines. (P22.2) • C'est Surtout par la sensibilisation des collaborateurs, pour appliquer des règles de sécurité, et pour ne pas se faire piéger par des attaques de phishing, à vocation… (P24.2 et A24.2) • C'est aussi participer à mener des plans d'action pour réduire ce risque de cyber sécurité. (P24.3) • En se formant déjà, en faisant de la veille, savoir ce qui se passe, en identifiant régulièrement les nouveaux risques, avec encore une fois des opérateurs informatiques, bien sûr. (P42.1) • Et en sensibilisant en fait sur l'audit. (P42.2) • Oui. Il faut répéter, répéter, répéter. (P25.1)	• Et c'est à moi de mettre en place, de faire appliquer la politique de sécurité des systèmes d'information par les collaborateurs, car c'est à moi de faire la **sensibilisation des collaborateurs** aux comités des risques qui nous passent sur des liens. (S20.1 et A20.2) • De bien analyser les risques, de bien soigner sa communication, la communication, c'est important que ce soit vers les collaborateurs pour qu'ils ne fassent pas des choses qui aggraverait la situation ou vis à vis des clients, surtout si l'indisponibilité du service consécutif à cette cyber attaque. (P18.1 et A18.1) • Donc, on a un programme de **sensibilisation des collaborateurs** qui est assez important, avec qui est baser avec des « E-Learning », des formations, ou qui est baser sur des campagnes de sensibilisation, et il y a aussi au niveau national, des campagnes de sensibilisation qui sont réaliser. (S22.3 et A22.1) • …des petits films qui sont construites au niveau national, **l'ANSSI**, qui met à dispositions aussi des guides de sensibilisations. (A22.2) • Surtout par la **sensibilisation des collaborateurs** à mon niveau. (P24.1 et A24.1)

Cybersécurité : Contrainte et implication (Sb)	• Sécurité internet, risque de fraude, risque d'attaques, risque de fuites de données, risque d'arrêt d'activité, risque de cyber malveillant, risque cyber fraude. (S14.1) • Aussi, je pense à 4 piliers que sont : • La disponibilité des systèmes d'informations • L'intégrité de nos systèmes d'informations c'est ce que nos données ne soient pas détournées ou modifiées. • La confidentialité c'est tout ce qui tourne autour du risque de fuite de données. • La preuve c'est à dire obtenir des traces qui nous permettent de répondre à nos clients, si jamais ne on avait des soucis sur nos systèmes d'informations. (S14.5) • Oui selon un protocole. (S17.1) • Les difficultés. (S18.1) • La difficulté est bien et de bien analyser les impacts que ce soit pour les collaborateurs ou les clients. (S18.2)	• Il y a plusieurs types de menaces sur la cybersécurité. (P14.3) • Et comme ça, il y a spontanément, la cyber criminalité, tout ce qui tourne des escrocs. (P14.4) • On a aussi ce qu'on appelle le cyber activisme, c'est-à-dire des gens qui veulent nuire fortement à l'image de l'entreprise. (S14.3 et P14.5) • Et pourquoi pas, ça c'est une autre catégorie une peut plus rare, en tant que petit établissement qu'on soit menacé, on a le cyber terrorisme qui se développe aussi avec l'aide éventuellement de cyber mercenaire. (S14.4 et P14.6) • La cyber sécurité, pour moi, c'est un sous-ensemble de ce qu'on **appelle la sécurité des systèmes d'informations** au sens large, la **« SSI »**. (P14.9) • La cyber sécurité est un élément à l'intérieur de la sécurité des systèmes d'informations et un élément très important, un enjeu majeur en termes de risque, pas seulement pour la banque populaire « Val de France », mais pour tous les établissements bancaires. (S14.6 et P14.10)	• Alors, normalement, il y a un protocole de gestion de crise au niveau **des opérateurs informatiques** qui lorsqu'ils sont avertis d'une cyberattaque importante. (S17.2 et A17.1) • C'est un risque majeur identifié par la « BCE », c'est-à-dire **la banque centrale européenne**. (A14.1) • Oui, **Pascal Gombert** a raison. (A20.1)
Responsabilité en cybersécurité et par rapport aux cyberattaques (Sc)	• Et donc, la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique par des opérateurs informatiques. (S5.2 et A5.3) • Et dans la banque, on se met en cas d'attaque, on se met en mode de gestion de crise avec tous métiers qui sont concernés dans la banque pour faire face à l'attaque et pour appliquer des mesures, des contres mesures qui vont nous être demandées par les opérateurs informatiques d'une part, et dans la pilule de crise, on a aussi le métier de communication qui communiquera si nécessaire aux collaborateurs de la banque et ou aux clients, s'il y a des attaques sur les clients. (S15.1) • Moi, personnellement, en tant que responsable de la sécurité des systèmes d'information en cas de crise et moi qui réunirait la cellule de crise avec tous les métiers dont je vous ai parlé tout à l'heure. (S16.1) • Et c'est moi qui fais l'interface entre ces métiers et les opérateurs informatiques. (S16.2 et A16.1) • Ils réuniraient les RSSI des établissements rattachés à ces opérateurs. (S17.3) • En cellule de crise, charge après au responsable de la sécurité des systèmes d'information d'établissements de réunir sa propre cellule de crise dans l'établissement. (S17.4) • Non, quand je vous parle des opérateurs informatiques, ce sont les collaborateurs du groupe BPCE-IT. (A20.1 et S20.1) • C'est une structure à part entière responsable du service informatique de toutes les banques populaires et de toutes les caisses d'épargnes qui font partie du groupe BPCE. (S20.2) • Et donc, parmi cette animation, il y a tous les RSSI, bien réfléchi les opérateurs, des débiteurs logiciels. (S27.4) • Au niveau du groupe au des autres banques, il y a des attaques comme dans toutes les entreprises. (S32.1) • Mais il a fallu bien y répondre, mettre les patches nécessaires, mettre les correctifs de sécurité nécessaires. (S32.3) • Donc, il y a des attaques. (S32.4) • Il en y a régulièrement en ransomware. (S32.5)	• Je pense **au risque**, mais je pense aussi à autre mesure pour **réduire ce risque**. (S14.2 et P14.1) • On pense aussi déjà à **des menaces**. (P14.2) • Je pense à des menaces lorsque vous me posez cette question. (P14.7) • Je pense aussi à la nécessité de **préserver notre patrimoine informationnel**, nos systèmes d'informations. (P14.8) • La banque populaire, c'est-à-dire le groupe « BPCE », organise la filière sécurité des systèmes d'information, et parmi la politique de **sécurité des systèmes d'information**, chaque établissement doit désigner un responsable de la sécurité des systèmes d'information, **un « RSSI »**. (P20.1 et A20.2)	• Les **experts en sécurité informatique** sont chez les **opérateurs informatiques** et ne sont pas dans les établissements comme une banque populaire. (A5.1) • Et donc, la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique par **des opérateurs informatiques**. (S5.2 et A5.3) • On confit notre informatique à **un opérateur** et c'est eux qui sont en charge de mettre en place des contres mesures pour éviter le risque de cyber attaque. (P19.1 et A19.2) • Surtout par **la sensibilisation des collaborateurs à mon niveau**. (P24.1 et A24.1) • Mais en règle générale, la décision de faire un audit sur ces sujets-là, elle est confiée à l'inspection générale qui peut alors faire appel à un **auditeur externe ou inspection externe**. (S35.3 et A35.4) • Elle peut décider de faire appel à **des auditeurs externes.** (A35.3 et S35.2) • Pas au niveau de la banque populaire « Val de France », mais au niveau encore une fois du groupe « BPCE », ils font intervenir **des experts** puisqu'on

	• A ma connaissance, dans nos établissements, les décisions menées des audits sur les systèmes d'information sont faites par l'audit interne ou l'inspection générale du groupe « BPCE ». (S35.1 et A35.1) • Oui, sur le domaine de la sécurité des systèmes d'information, on a des interlocuteurs dans les différents métiers de l'informatique plutôt, puisqu'on a des relations régulières avec les gens qui s'occupent des habilitations, les contrôles d'accès par exemple, on a des relations régulières avec les gens qui s'occupent des développements privatifs. (S39.1) • On a des accès réguliers avec les gens qui s'occupent de l'informationnel c'est-à-dire les entrepôts de données, tout ce qui peut générer des programmes particuliers. (S39.2) • Oui, on peut envisager de ce qu'on discute tout à l'heure, de faire intervenir des sociétés spécialisées en sécurité informatique pour faire par exemple des tests d'intrusion, sur notre périmètre relatif. (S44.1) • Les entreprises, pas seulement les banques, s'entourent des prestataires de services, spécialisés dans la cybersécurité, pour travailler justement à réduire ces risques. (S44.3)		travaille avec **des prestataires de services qui sont experts en sécurité informatique**. (A44.1 et S44.2) • Donc, on a un **programme de sensibilisation des collaborateurs** qui est assez important, avec qui est baser avec des « E-Learning », des formations, ou qui est baser sur des campagnes de sensibilisation, et il y a aussi au niveau national, des campagnes de sensibilisation qui sont réaliser. (S22.3 et A22.1) • …il y a aussi des structures qui s'occupent de lutter au quotidien contre la cybersécurité, avec ce qu'on appelle des « COS », **centre opérationnel de sécurité** qui font de la veille sur tout ce qui est menace, tout ce qui vulnérabilité, et qui mènent des actions de réduction des risques au quotidien. (S31.1 et A31.1)
Politiques et actions pour essayer de maintenir la cybersécurité (Sd)	• Oui, on a des modules de formation que les collaborateurs suivent. (S22.1) • Oui, on a une formation parmi toutes les autres formations, à la banque, surtout à la sensibilisation pour dire à nos collaborateurs, ne cliquer pas sur les liens de suspects, comme on dit pour le client le reste… (S22.4) • Oui, on a mis en place un comité interne de sécurité. (S23.1) • On prépare les incidents et on intervient sur ce domaine. (S23.2) • On travaille ensemble à deux niveaux. (S27.1) • Le premier niveau, c'est une charte ou un cadre de fonctionnement de la sécurité des informations qui dit comment on doit être organisé : (S30.2) • A l'intérieur de chacune de ces structures, comment on doit être organisé ? (S30.2) • Comment on doit échanger ? (S30.3) • Quels outils on doit mettre en place ? (S30.4) • C'est le premier niveau et c'est la charte de fonctionnement, le cadre d'application pour dire que tous les établissements doivent respecter de manière homogène pour lutter contre la cybersécurité. (S30.5) • Évidemment, il y a plusieurs centaines qui vont vous dire par exemple : (S30.7) • Qu'un mot de passe doit faire tant de caractères pour être suffisamment robuste dans tous les établissements du groupe. (S30.8) • Que les proxys doivent être installés là où c'est nécessaire. (S30.9) • Que les messageries doivent être sécurisées. (S30.10) • Donc, on appréhende ce risque surtout, par une politique d'une part, on appréhende aussi ce risque par … (S30.12) • Pour qu'ils s'approprient des enjeux, il faut qu'ils soient sensibilisés bien sûr, il faut les éclairer sur les risques, sur ce qui pourrait arriver si jamais on ne mettait pas en œuvre les politiques et les moyens pour réduire les risques de cyber sécurité. (A50.1 et S50.1) • Il y a des contrôles qui sont faits, il y a des formations qui sont réalisés. (S51.1)	• On l'appréhende très au sérieux justement par une organisation qu'on espère est efficace, où on a mis en place au niveau « BPCE », encore une fois une politique de sécurité des systèmes d'information, c'est-à-dire une politique à plusieurs niveaux au moins à deux niveaux. (S30.1 et P30.1) • Que dans tous les domaines de l'informatique, des règles de sécurité doivent être appliqués, c'est-à-dire c'est le deuxième niveau de la politique de sécurité des systèmes d'information, au-dessous du cadre qui fixe le fonctionnement. (S30.11 et P30.2)	• Premier niveau, on a le groupe BPCE, admit la filière des RSSI avec des comités de suivi réguliers trimestriels et réellement où les plans d'action des actualités nous sont donnés. (S27.2 et A27.1) • Ça c'est au niveau de l'animation par BPCE de la filière des RSSI. (S27.3 et A27.2) • Et en deuxième niveau, nous recevons ces informations, **par mail**, du groupe **BPCE** sur ces questions de sécurité, dès lors des alertes, dès lors des clients qui s'ont piégé... (S27.5 et A27.3) • Le deuxième niveau de la politique, c'est un référentiel de **règles de la sécurité des systèmes d'informations** qui s'appliquent à tous les établissements du groupe « BPCE ». (S30.6 et A30.4) • Mais sur ces sujets-là de cyber sécurité, on peut faire appel à **des auditeurs externes qui ont une compétence technique particulière** qu'on n'aurait pas forcement dans nos établissements sur ces sujets-là. (A33.3 et S33.1) • Aujourd'hui, si on veut faire des tests d'intrusion sur des systèmes d'informations, on fait des appels

	• Or les contrôles sont faits par des équipes de contrôle permanent de deuxième niveau. (S51.2) • En France, comme je vous l'ai dit, il y a trois niveaux : (S51.3) • Il y a les métiers qui réalisent des contrôles de premier niveau. (S51.4) • Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits. (S51.5) • Et puis, il y a l'audit en troisième niveau, comme on disait tout à l'heure, qui effectue des missions ponctuelles, périodiques. (S51.6 et A51.1)		**à des auditeurs externes.** (S33.2 et A33.4) • Si on décide, ou lorsque les opérateurs décident de faire des tests d'intrusion sur les systèmes, et qu'ils choisissent **un auditeur externe**. (S34.1 et A34.1)
Audit interne : Définition et relation avec la cybersécurité (Se)	• Dans un autre sens, moi je n'ai **pas de relation** avec l'audit. (S28.1) • Elle peut fixer les conditions de l'audit ce que doit contenir l'audit, quelle est le résultat attendu de l'audit. (S35.5) • Mais sur le choix de l'auditeur, je ne pense pas. (S35.6) • Très peu de relation. (S36.1) • Quand il y a des missions d'audit de nos domaines, ils viennent nous interviewés. (S36.2) • Mais si non, il y a **très peu de relation**. (S36.3) • Sur une mission d'audit, soit sur une cyber sécurité ou pas, il y a deux auditeurs qui demandent un certain nombre de questions et qui suivent un guide d'audit et qui viennent nous interviewés en nous posant un certain nombre de questions, pour écrire après les réponses, pour se faire une idée des risques et des éventuelles recommandations à formuler. (A45.3 et S45.1) • Ensuite, on se met d'accord avec les auditeurs sur les recommandations, qui nous sont affecter et après on met en œuvre les recommandations, il y a un suivi de recommandation qui est fait par les auditeurs. (A45.4 et S45.2) • Alors ils ne sont pas forcément peur ou intimidés, mais en règle générale, les collaborateurs ont crainte d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre, et ces recommandations à mettre en œuvre sont des moyens à engager qu'on n'a pas forcement tout le temps. (S47.1 et A47.1)	• Donc je **ne pense pas** qu'il doit adapter le fait que **l'audit** est confié à **maintenir la cyber sécurité**. (P29.1) • L'audit peut faire des missions périodiques sur les apparts de la cyber sécurité mais **ne pas la maintenir** en totale. (A29.3 et P29.2) • Je pense que le traitement opérationnel de la sécurité des systèmes d'information doit être au plus près des métiers. (P29.4) • Il faut que ce soit très opérationnel par des gens qui ont des expertises et une connaissance de la sécurité des systèmes d'information. (P29.5) • En établissement bancaire, « BPVF », non. (P32.1) • Au niveau du groupe au des autres banques, il y a des attaques comme dans toutes les entreprises. (S32.1) • On a cité « WannaCry » en 2007 qui a touché toutes les entreprises, mais ces attaques, n'ont pas eu d'impact important, en tout cas, au niveau du groupe « BPCE ». (A32.1 et S32.2) • Pas de relation. (P38.1) • Vous devez demander cette question à l'audit. (P40.1) • Pas vraiment d'avis sur la question. (P40.2) • Oui, c'est une question de domaine, ou ça évolue assez vite, il faut s'adapter en permanence. (P41.1) • Il faut avoir un bon relationnel, se respecter. (P48.1)	• Là ce n'est pas le choix qui a été fait par le groupe BPCE parce que l'audit est un contrôle périodique dans le dispositif de contrôle permanent qui s'applique en France. (A29.1 et S29.1) • **L'audit,** de mon point de vue, c'est **la règlementation des contrôles** qui, en **troisième niveau**, et effectue des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. (A29.3 Et S29.1) • Ce n'est pas l'organisation du contrôle qui existe chez nous en France, où l'audit est en troisième niveau, il n'est pas en opérationnel sur la sécurité des systèmes d'information. (P29.7 et A29.7) • …mais en règle générale, les collaborateurs **ont crainte** d'un audit car lorsqu'il y a des audits, il y a des recommandations à mettre en œuvre, et ces recommandations à mettre en œuvre sont des moyens à engager qu'on n'a pas forcement tout le temps. (S47.1 et A47.1) • Mais ils **ne sont pas** dans le quotidien de **la cyber sécurité**. (A29.6)

6. Production des catégories par l'analyse structurale

Notre travail présenté en ce qui précède était purement inductif. Nous allons maintenant dégager des unités de sens sur la base de notre description préalable et essentielle. Ces unités de sens sont appelées *« catégories sémiques »* selon Greimas (1986) qui sont constitutives de la logique sociale de l'entretien et de sa forme sémique.

Notre travail sera un travail démonstratif qui se reposera sur quelques principes de base qui constitueront une sorte de fonds communs de l'analyse structurelle. Conformément à notre projet de départ, nous sommes obligés de montrer

la démarche en acte en introduisant des équivalents dans la littérature. Nous signalons les multiples choix sur lesquels repose la mise en œuvre de toute démarche d'inspiration structurale. Donc, notre mise en œuvre repose sur une intelligence préalable du discours que la partie précédente n'a que formaliser.

a. Disjonction et Conjonction

Nous allons considérer l'hypothèse de base de l'analyse est de traduire le schème précédent en une combinaison de catégories typiques constitutive du sens général de l'entretien.

Nous assumons que la révolution structurale consiste à analyser toute langue naturelle et tous ensemble signifiant comme un système d'opposition à l'intérieure d'une relation constitutive du sens. Nous s'occupons à des « éléments différentiels » ou des « traits distinctifs » qui assurent l'existence d'une langue. Donc, ce qui est vrai au sens lexical l'est aussi au sens sémantique.

Nous admettons que le sens linguistique d'un mot ne se comprend qu'en restituant la disjonction qui le spécifie et la conjonction qui lui assure son appartenance à une catégorie. La disjonction trouve son origine dans la chaine syntagmatique constitutive du signifiant et la conjonction de l'intégration paradigmatique définissant le signifié.

b. Application à l'entretien et à ses trois niveaux

i. La signification des séquences : l'opposition je sais/je ne sais pas

Didier qualifie les expériences qu'il a tiré des différentes phrases de son parcours au moyen d'expression souvent lapidaires :

(S1) : « je suis responsable des risques opérationnels, en charge et de poursuite d'activité et la sécurité des systèmes d'information. » (§3)

(S2) : « parcours pendant une trentaine d'année, responsable de la monnaie et responsable de l'ensemble des moyens de paiement. » (§2)

(S3) : « …**les qualités de responsable de la sécurité des systèmes d'informations dans l'établissement bancaire**, comme la « BPVF », **nous ne sommes pas des experts en sécurité informatique**. (§5)

(S4) : « Les experts en sécurité informatique sont chez les opérateurs informatiques et ne sont pas dans les établissements comme une banque populaire. » (§5)

(S5) : « Et donc, la sécurité des systèmes d'informations est pilotée au niveau du groupe « BPCE » en spécifique par des opérateurs informatiques. (§5)

(S6) : « Je pense au risque, mais je pense aussi à autre mesure pour réduire ce risque. » (§14)

(S7) : « Je pense aussi à la nécessité de préserver notre patrimoine informationnel, nos systèmes d'informations. (§14)

(S8) : « La preuve c'est à dire obtenir des traces qui nous permettent de répondre à nos clients, si jamais ne on avait des soucis sur nos systèmes d'informations. » (§14)

(S9) : « La cyber sécurité, pour moi, c'est un sous-ensemble de ce qu'on appelle la sécurité des systèmes d'informations au sens large, la « SSI ». (§14)

(S10) : « Et dans la banque, on se met en cas d'attaque, on se met en mode de gestion de crise avec tous métiers qui sont concernés dans la banque pour faire face à l'attaque et pour appliquer des mesures, des contres mesures qui vont nous être demandées par les opérateurs informatiques d'une part, et dans la pilule de crise, on a aussi le métier de communication qui communiquera si nécessaire aux collaborateurs de la banque et ou aux clients, s'il y a des attaques sur les clients. » (§15)

(S11) : « Moi, personnellement, en tant que responsable de la sécurité des systèmes d'information en cas de crise et moi qui réunirait la cellule de crise avec tous les métiers dont je vous ai parlé tout à l'heure. Et c'est moi qui fais l'interface entre ces métiers et les opérateurs informatiques. (§15)

(S12) : « Oui selon un protocole…un protocole de gestion de crise au niveau des opérateurs informatiques qui lorsqu'ils sont avertis d'une cyberattaque importante…Ils réuniraient les RSSI des établissements rattachés à ces opérateurs. (§17)

(S13) : « **En cellule de crise**, charge après au responsable de la sécurité des systèmes d'information d'établissements de réunir sa propre cellule de crise dans l'établissement. (§17)

(S14) : « …analyser les impacts que ce soit pour les collaborateurs ou les clients…analyser les risques… (§18)

(S15) : « C'est ce que je vous ai expliqué plutôt le travail des opérateurs informatiques. On confit notre informatique à un opérateur et c'est eux qui sont en charge de mettre en place des contres mesures pour éviter le risque de cyber attaque. (§19)

(S16) : « Dans chaque établissement, on a nommé un responsable de la sécurité des informations pour la BPVF : c'est moi…et parmi la politique de sécurité des systèmes d'information, chaque établissement doit désigner un responsable de la sécurité des systèmes d'information, un « RSSI ». (§20)

(S17) : « Et c'est à moi de mettre en place, de faire appliquer la politique de sécurité des systèmes d'information par les collaborateurs, car c'est à moi de faire la sensibilisation des collaborateurs aux comités des risques qui nous passent sur des liens. (§20)

(S18) : « Responsable de la cybersécurité sur nos infrastructures informatiques, ce sont seulement les opérateurs informatiques. » (§20)

(S19) : « en termes de cybersécurité, l'une des vulnérabilités la plus importante c'est l'humain… C'est les hommes plus que les machines. (§22)

(S20) : « on a mis en place un comité interne de sécurité…Nous on prépare les incidents et on intervient sur ce domaine. (§23)

(S21) : « Surtout par la sensibilisation des collaborateurs à mon niveau…la sensibilisation des collaborateurs, pour appliquer des règles de sécurité, et pour ne pas se faire piéger par des attaques de phishing, à vocation… (§24)

(S22) : « réduire ce risque de cyber sécurité. » (§24)

(S23) : « assurée au niveau des opérateurs informatiques. (§23)

(S24) : « tous les RSSI, bien réfléchi les opérateurs, des débiteurs logiciels…en deuxième niveau, au niveau quotidien, nous recevons ces informations, par mail, du groupe BPCE sur ces questions de sécurité, dès lors des alertes, dès lors des clients qui s'ont piégé... (§27)

(S25) : « moi je n'ai pas de relation avec l'audit. (§28)

(S26) : « Donc je ne pense pas qu'il doit adapter le fait que l'audit est confié à maintenir la cyber sécurité. (§29)

(S27) : « L'audit peut faire des missions périodiques sur les apparts de la cyber sécurité mais ne pas la maintenir en totale. (§29)

(S28) : « Je pense que le traitement opérationnel de la sécurité des systèmes d'information doit être au plus près des métiers. Il faut que ce soit très opérationnel par des gens qui ont des expertises et une connaissance de la sécurité des systèmes d'information. (§29)

(S29) : « **RSSI** lui il intervient en deuxième niveau sachant que les opérationnels de la sécurité interviennent en premier niveau. (§29)

(S30) : « **RSSI** doit réaliser un certain niveau de contrôle pour s'assurer que le premier niveau est bien réalisé. (§29)

(S31) : « L'audit, intervient en troisième niveau, effectue des missions thématiques sur un certain nombre de domaines, y compris dans la cybersécurité, puisqu'il y a des audits sur la sécurité des serveurs, des audits sur la sécurité des infrastructures en générale. (§29)

(S32) : « l'audit n'est pas dans un rôle opérationnel, mais effectue des missions en troisième niveau qui peuvent être beaucoup plus longues et plus approfondies mais ne sont pas dans le traitement opérationnel. (§29)

(S33) : « Mais ils ne sont pas dans le quotidien de la cyber sécurité…où l'audit est en troisième niveau, il n'est pas en opérationnel sur la sécurité des systèmes d'information. (§29)

(S34) : « …des structures qui s'occupent de lutter au quotidien contre la cybersécurité, avec ce qu'on appelle des « SOC », centre opérationnel de sécurité qui font de la veille sur tout ce qui est menace, tout ce qui vulnérabilité, et qui mènent des actions de réduction des risques au quotidien. (§31)

(S35) : « la cybersécurité est un métier d'expert, les auditeurs internes dans une banque sont **généralistes** dans les effets bancaires. (§33)

(S36) : « Mais sur ces sujets-là de cyber sécurité, on peut faire appel à des auditeurs externes qui ont une compétence technique particulière qu'on n'aurait pas forcement dans nos établissements sur ces sujets-là. (§33)

(S37) : « faire des tests d'intrusion sur des systèmes d'informations, on fait des appels à des auditeurs externes. (§33)

(S38) : « Si on décide, ou lorsque les opérateurs décident de faire des tests d'intrusion sur les systèmes, et qu'ils choisissent un auditeur externe. (§34)

(S39) : « le RSSI que je suis, à des relations avec les différents métiers qui s'occupe de l'informatique dans la banque. » (§39)

(S40) : « En se formant déjà, en faisant de la veille, savoir ce qui se passe, en identifiant régulièrement les nouveaux risques, avec encore une fois des opérateurs informatiques…Et en sensibilisant en fait sur l'audit. » (§42)

(S41) : « Moi, je n'ai pas connaissance d'expert d'orange cyber défense… » (§43)

(S42) : « faire intervenir des sociétés spécialisées en sécurité informatique pour faire par exemple des tests d'intrusion, sur notre périmètre relatif. » (§44)

(S43) : « ils font intervenir des experts puisqu'on travaille avec des prestataires de services qui sont experts en sécurité informatique. (§44)

(S44) : « …les banques, s'entourent des prestataires de services, spécialisés dans la cybersécurité, pour travailler justement à réduire ces risques. (§44)

(S45) : « Il y a les métiers qui réalisent des contrôles de premier niveau. Il y a des structures de contrôle permanent qui réalisent des contrôles de deuxième niveau, qui s'assurent que les contrôles de premier niveau sont bien faits. Et puis, il y a l'audit en troisième niveau, comme on disait tout à l'heure, qui effectue des missions ponctuelles, périodiques. (§51)

Nous allons ici faire des hypothèses en restant le plus près possibles du texte retranscrit. Nous allons rétablir les oppositions entre unités de diverses séquences-types :

- Si on a un problème, on appelle les opérateurs informatiques / En termes de SSI, c'est des expertises que nous n'avons pas; Je vais réunir la cellule de crise et travailler sur la sensibilisation des personnels.
- On n'est pas l'expertise / L'expertise se trouve ailleurs chez les opérateurs informatiques ;

L'opposition je sais/je ne sais pas concerne successivement ou simultanément trois catégories : Niveau de formation et progression de la carrière, fonction de superviseur en audit et conséquence de la cybersécurité sur la banque.

ii. La signification des actants : pareils/pas pareils et mieux/pire

Nous allons procéder de la même façon pour les actants du récit de Didier.

Nous résumons dans ce tableau ci-dessous les acteurs pareil et pas pareil à Didier.

Pareil	Pas Pareil
Directeur de l'audit Interne	Opérateurs informatiques I-BP
Directeur générale	Cabinet extérieur embauché
Clients de la banque	BCE
Auditeur interne	Prestataires externes informatiques
Les audités	Hackers (WannaCry)
Les collaborateurs	SOC

Nous pouvons maintenant analyser le sens de l'opposition Pareil/Pas Pareil en retrouvant les catégories associant la conjonction de deux termes.

iii. La signification des arguments : Facile/Pas facile

Didier précise dans son discours qu'elle n'a pas les compétences en informatique et en cybersécurité. Il dit je ne sais pas et ce n'est pas dans mon champ d'expertise la cybersécurité. Mais il oppose son discours en disant :

- Qu'il a de bonnes connaissances sur toutes les applications et les domaines informatiques.
- En disant que la cybersécurité est un risque très majeur mais il n'a pas beaucoup de contexte particulière sur cette thématique.

Nous analysons ces oppositions pour trouver la totalité qui donne sens à ces couples, découvrir la conjonction qui englobe cette disjonction.

c. La structuration de l'univers sémantique et la logique du récit

Rappelons les résultats acquis à ce stade de l'analyse. Une première opposition je sais/je ne sais pas structure les séquences de Didier. Nous l'avons décomposée selon trois propriétés combinées qui permettent de qualifier les renseignements de cybersécurité dans la banque :

- Je ne sais pas = Pas de compétence technique informatique + Pas d'expertise + recours à un cabinet externe ou prestataires externes
- Je sais = Compétence technique spécialisé en informatique + Expertise technique + assurer la cybersécurité

Une seconde opposition pareil/pas pareil structure les segments du récit qui mettent en scène des actants de la vie de Didier. Nous en avons trouvé deux propriétés principales qui permettent de qualifier les significations d'une autre « totalité » que l'on peut appeler statut :

- Pareil=Pas d'expertise+Pas de responsabilité
- Pas pareil= Expertise technique+Responsabilité de cybersécurité

Une autre opposition a été introduite pour rendre compte de la structuration du récit des actants : mieux/pire, qui renvoie à une autre « totalité » qu'il faut y avoir une collaboration pour réduire les failles et les cybers attaques.

Une troisième opposition nous a permis de structurer la narration de Didier et de qualifier la relation précédente facile/pas facile. Nous allons extraire donc les propriétés suivantes :

- Facile=expertise technique acquise+compétence technique+connaissance
- Pas Facile=Incompétent domaine informatique+coûte cher+Prend du temps

Nous allons terminer notre analyse par-là construction d'axes croisés permettant d'attribués des propriétés identiques à plusieurs significations dégagées antérieurement. Nous proposons pour l'entretien de Didier les schémas suivants :

Tableau 1. Situation et perspectives professionnelles de Didier

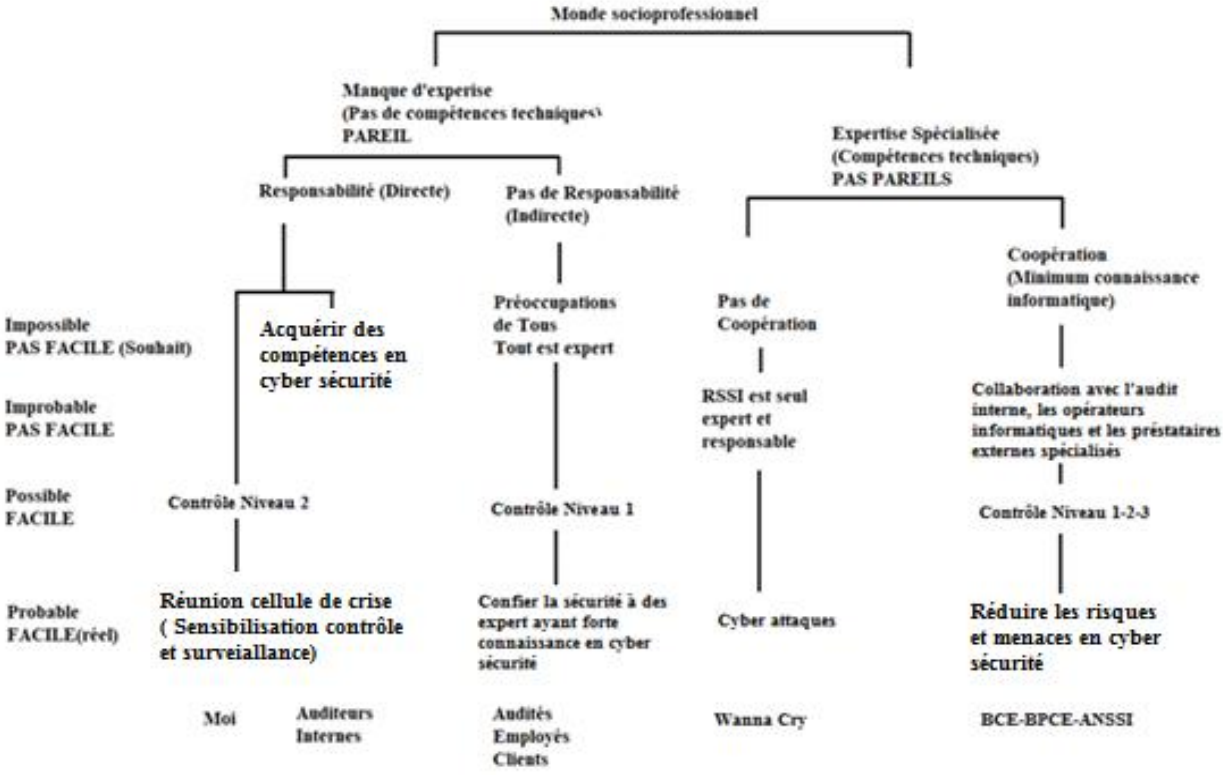
	Positives (Je sais)	Négatives (Je ne sais pas)
Possible (Facile)	Réunion cellule de crises et sensibilisation	Cabinet Externe et Coopération avec l'audit interne et les opérateurs informatiques
Impossible (Pas Facile)	Prestataire externe expert et spécialiste ITEKIA	Préoccupation de tous, il faut du travail.

Tableau 2. Personnages propre et perspectives professionnelles de Didier

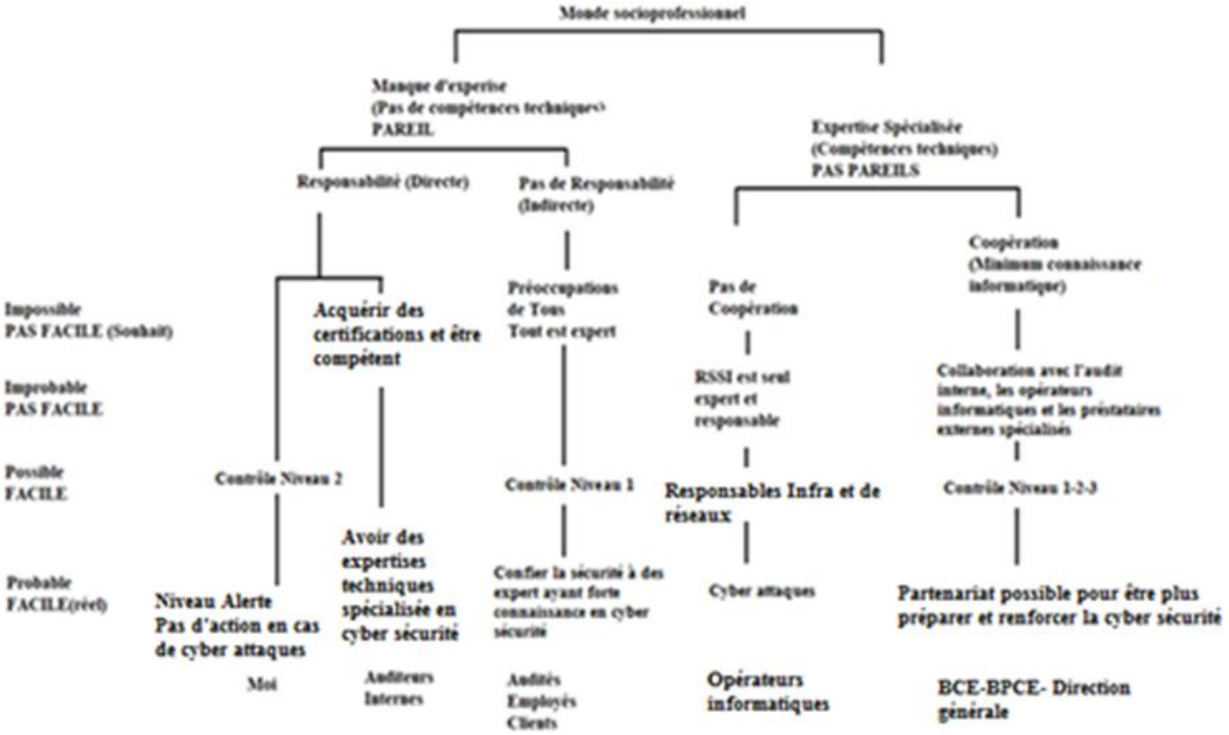
	Semblables (Pareil)	Différents (Pas Pareil)
Positives (Mieux)	Auditeurs internes, Directeur générale, Directeur de l'audit interne	Cabinet externe spécialiste, Prestataire externe expert, Opérateurs informatiques
Négatives (Pire)	Collaborateurs, clients, Audités	RSSI seul responsabilité

Annexe C : Les schèmes spécifiques

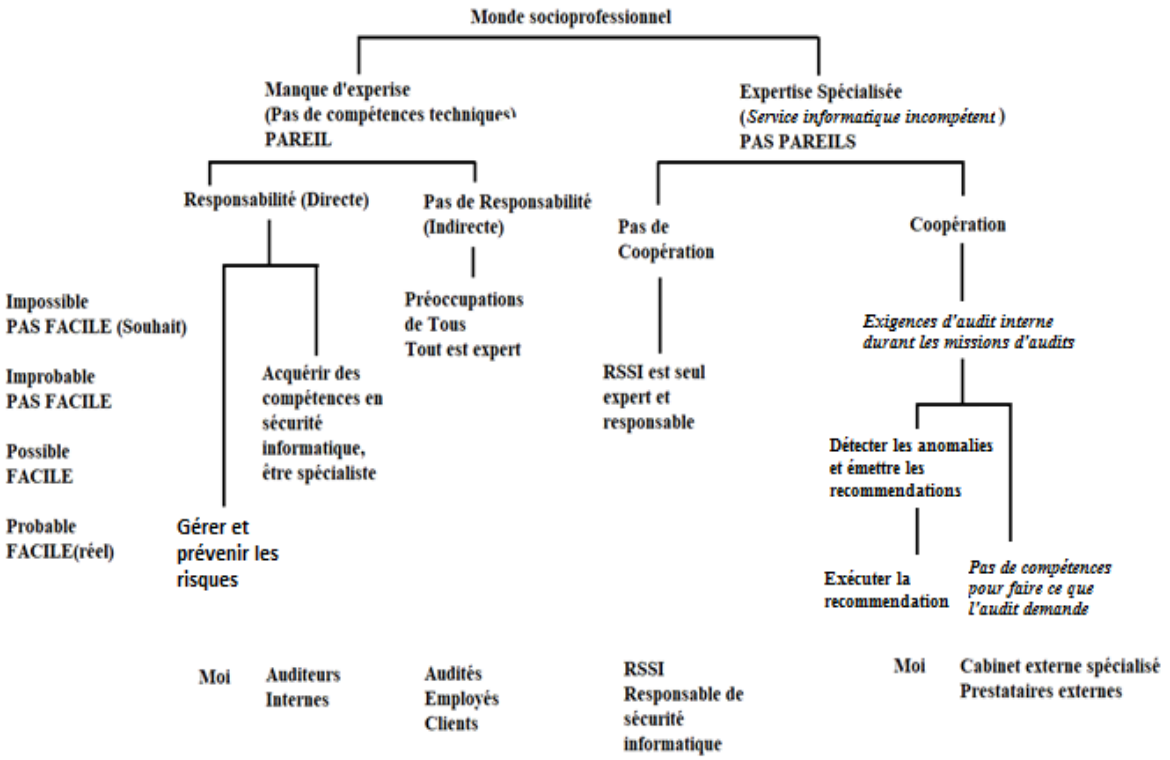
C1. Schème spécifique du RSSI D.G au sein de la BPVF



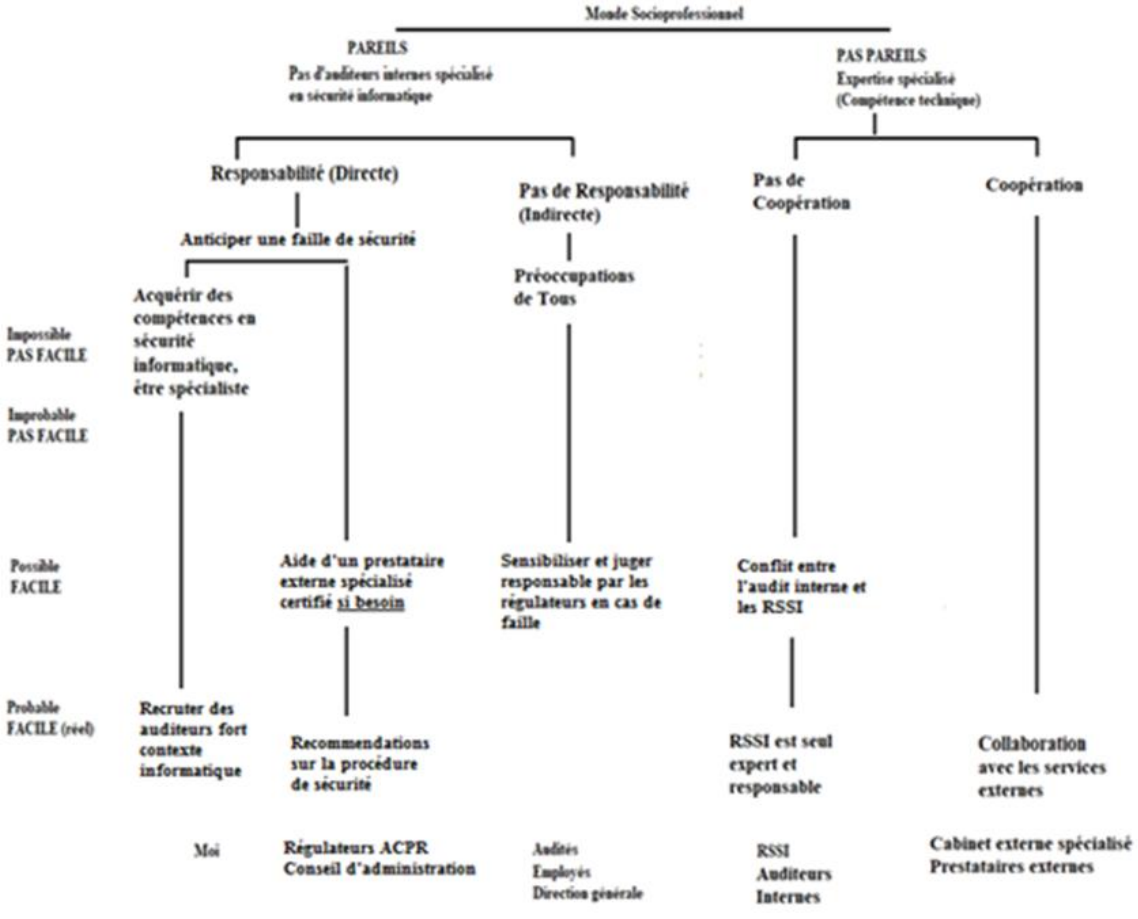
C2. Schème spécifique du directeur de l'audit interne M.C au sein de la BPVF



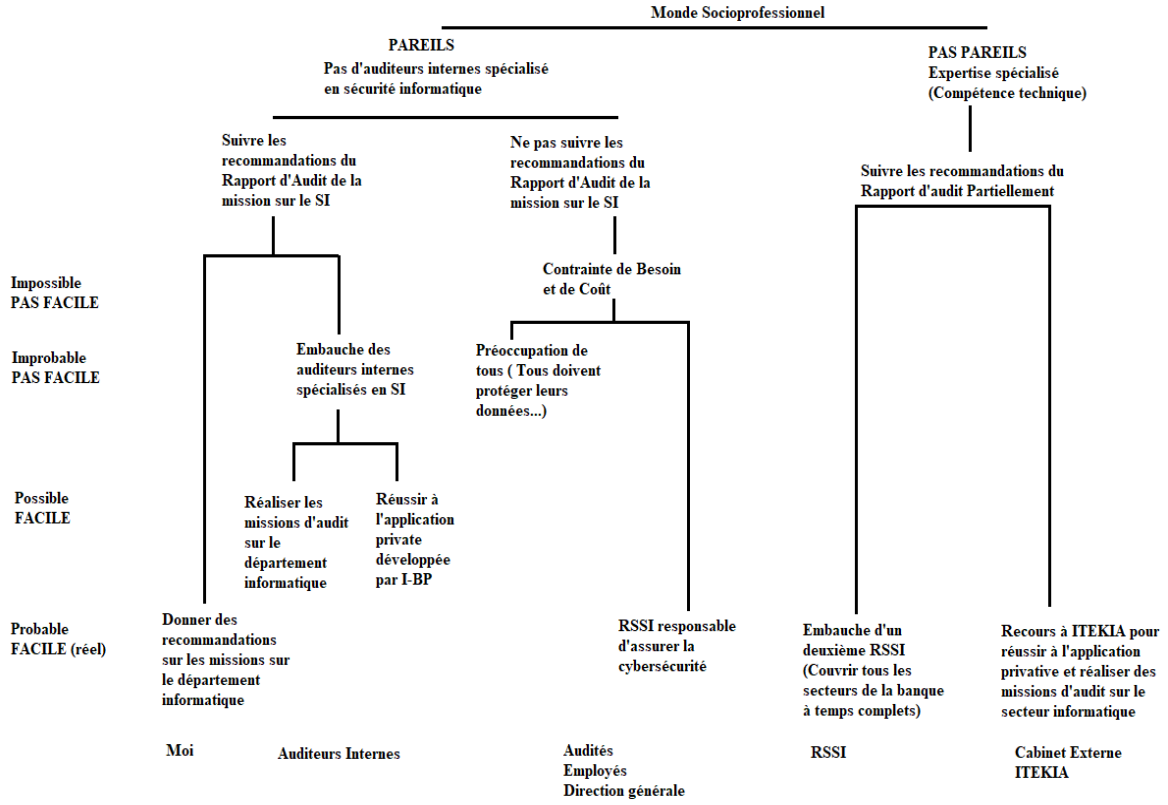
C3. Schème spécifique du directeur de la conformité P.G au sein de la BPVF



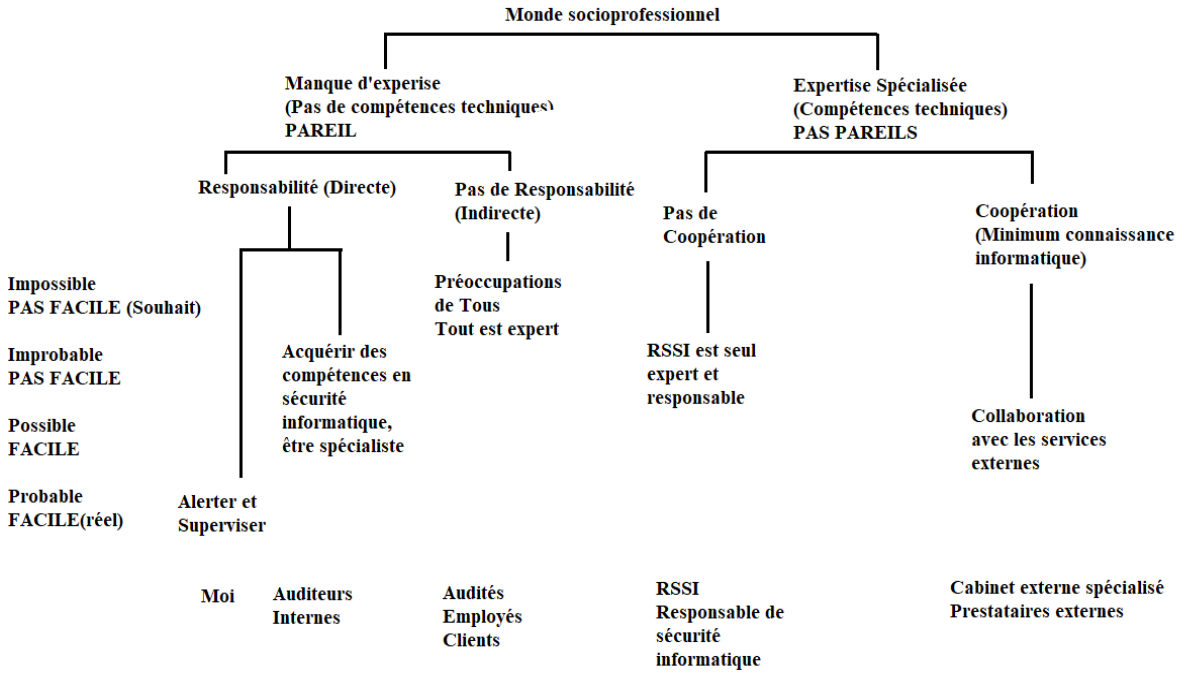
C4. Schème spécifique du directeur de l'audit interne P.C au sein de l'I-BP



C5. Schème spécifique du chef de mission audit interne T.L au sein de la BPVF



C6. Schème spécifique du superviseur de l'audit interne A.S au sein de la BPVF



ANNEXES D : LISTE D'ACRONYMES

D1. Liste d'acronymes des termes techniques et non techniques

Acronyme	Signification
BCE	Banque centrale européenne
BDL	Banque du Liban
BLF	Banque Libano-Française
BLOM Banque	Banque du Liban et D'Outre-Mer
BNP Paribas	Banque Nationale de Paris – Paribas
BOB	Banque of Beirut
BPCE	Banque populaire Caisses d'épargne
BPVF	Banque populaire Val de France
CEO	Chief Executive Officier
CERT	Computer Emergency Response Team
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
DDOS	Distributed Denial of Service
DPO	Data Protection Officer
DSI	Direction des Systèmes d'Information
E&Y	Ernst & Young
FBI	Federal Bureau of Investigation
FINRA	Financial Industry Regulatory Authority
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley
IA	Intelligence artificielle
IAM	Identity and Access Management
IBM	International Business Machines Corporation
IBP	Informatique - Banque Populaire
IFACI	Institut Français de l'Audit et du Contrôle Internes
IIA	Institute of Internal auditors
ISACA	Information Systems Audit and Control Association
ISO	L'organisation internationale de normalisation
NIST	National Institute of Standards and Technology
NSA	Agence de sécurité nationale
PDG	Président-directeur général
PIB	Produit intérieur brut
PwC	PricewaterhouseCoopers
RCCA	Réseau canadien des comités d'audit
RGDP	Règlement Général sur la Protection des Données
RSSI	Responsable Sécurité des Systèmes d'information
SEC	Securities and Exchange Commission
SGBL	Société générale de banque au Liban
SLA	Service Level Agreements
SOC	Operation Center
SOC	Security Operations Center
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UIT	Union internationale des télécommunications

Résumé / Summary

LE ROLE DE L'AUDIT INTERNE DANS LA CYBERSÉCURITÉ D'ÉTABLISSEMENT BANCAIRE :
Une collaboration interprofessionnelle aux prismes des identités professionnelles

Le rôle crucial de l'audit interne dans le domaine de la cybersécurité bancaire est examiné sous l'angle des identités professionnelles et comment la collaboration entre les auditeurs internes et les responsables de la sécurité de l'information (RSSI) influence la protection des données financières. Notre recherche vise à étudier l'identité professionnelle des acteurs impliqués, en mettant en lumière leurs compétences, leurs responsabilités et leurs valeurs dans un contexte où la sécurité informatique est devenue un enjeu stratégique. Nous avons pu observer durant ces cinq ans les différences significatives entre le secteur bancaire français et libanais à travers des entretiens biographiques et un codage selon Dubar et Demazière. Nous analysons les dynamiques identitaires des auditeurs internes et des RSSI en insistant sur la nécessité d'une approche plus cohérente et coordonnée pour relever les défis de la cybersécurité, en particulier dans le contexte libanais. Nous offrons une vision approfondie et nuancée de la cybersécurité bancaire et de l'importance de la collaboration interprofessionnelle pour faire face aux menaces numériques en constante évolution. Nous constatons que la sécurité informatique n'est plus seulement une question technique, mais un élément essentiel de la gestion globale des risques et de la stratégie commerciale des institutions financières.

Mots clés : Cybersécurité, identités professionnelle, menaces numériques, système d'information collaboratif, stratégie globale.

THE ROLE OF INTERNAL AUDIT IN THE CYBERSECURITY OF BANKING INSTITUTIONS:
Interprofessional collaboration through the prisms of professional identities

The crucial role of internal audit in banking cybersecurity is examined through the lens of professional identities and how collaboration between internal auditors and Chief Information Security Officers (CISOs) influences data protection financial. Our research aims to study the professional identity of the actors involved, by highlighting their skills, responsibilities and values in a context where IT security has become a strategic issue. During these five years, we were able to observe the significant differences between the French and Lebanese banking sectors through biographical interviews and coding according to Dubar and Demazière. We analyze the identity dynamics of internal auditors and CISOs, emphasizing the need for a more coherent and coordinated approach to address cybersecurity challenges, particularly in the Lebanese context. We provide an in-depth and nuanced view of banking cybersecurity and the importance of cross-industry collaboration to address ever-evolving digital threats. We see that IT security is no longer just a technical issue, but an essential part of the overall risk management and business strategy of financial institutions.

Keywords: Cybersecurity, professional identities, digital threats, collaborative information system, global strategy.