Mastère Spécialisé® Expert en Contrôle de Gestion, Audit et Gestion de Système d'Information

Programme de SKEMA,

Reconnu par l'État à Diplôme visé.

Thèse Professionnelle

Promotion 2025

De quelle manière les exigences croissantes en matière de cybersécurité transforment-elles les approches et les outils de l'audit interne pour gérer les risques organisationnels et technologiques ?

Auteurs : Titouan Boyard et Violette Blanchard

Directrice de thèse professionnelle : Mme. Marie Paulus

Les propos tenus dans ce document n'engagent que leurs auteurs

Remerciements

Nous tenions tout d'abord à exprimer notre profonde gratitude à Madame Marie Paulus, Professeur d'audit interne et Directrice du Mastère Spécialisé® Expert en Contrôle de Gestion, Audit et Gestion de Système d'Information, pour son accompagnement et ses conseils avisés tout au long de la rédaction de cette thèse professionnelle. Ses cours et son suivi à travers ce travail nous ont permis de devenir des professionnels de l'audit performant et moderne.

Nous souhaiterions aussi remercier chaleureusement l'ensemble des personnes qui ont accepté de participer aux entretiens menés dans le cadre de cette recherche. Leur disponibilité et la richesse de leurs témoignages ont constitué une source précieuse d'informations tant sur l'aspect du travail de terrain que sur leurs réflexions quant aux liens entre l'audit interne et la cybersécurité. Ils ont largement contribué à nourrir notre réflexion sur ce sujet complexe.

Nous remercions ensuite SKEMA Business School, en sa qualité de grande école de commerce, pour l'opportunité qui nous a été donnée d'évoluer dans cet environnement académique stimulant et propice au développement intellectuel ainsi que personnel. Les enseignements reçus tout au long de cette année académique et les rencontres effectuées durant notre parcours, que ce soit avec des professeurs ou des professionnels pendant des conférences, ont constitué une véritable valeur ajoutée à notre formation et à notre vision du métier de l'audit.

Enfin, nous adressons nos remerciements à toutes celles et ceux qui, de près ou de loin, ont contribué à la réalisation de cette thèse professionnelle. Par leur soutien moral et leurs conseils, ils ont été un appui précieux dans les moments de doute ainsi qu'une source de motivation.

Avant-propos

Cette thèse professionnelle ainsi que sa problématique s'intéressent aux liens entre la fonction d'audit interne et la cybersécurité. En effet, dans un contexte où les organisations sont, de façon croissante, confrontées à ces menaces cyber sophistiquées et multiples, l'audit interne a un rôle clef à jouer dans leur protection et dans l'atténuation de ces risques.

Notre étude s'appuie sur une recherche qualitative, tant de la littérature en place que des retours terrains des personnes confrontées à ces risques cyber, visant donc à comprendre les liens, qui se renforcent de plus en plus, entre la cybersécurité et la fonction d'audit interne.

Malgré le fait que cette thèse professionnelle soulève beaucoup d'enjeux pour la profession, son objectif reste de formuler des recommandations pertinentes sous forme de pistes concrètes de réflexion qui permettront aux professionnels de mieux comprendre ces interactions. Ainsi, nous ambitionnons aussi de proposer des axes d'analyse pour de futurs étudiants souhaitant aborder à travers des recherches académiques ces sujets passionnants.

Table des matières

REMERCIEMENTS 3

AVANT-PROPOS 4

LISTE DES FIGURES 6

LISTE DE SIGLES 7

INTRODUCTION **9**

I- REVUE DE LITTERATURE **14**

1.1- LES ENJEUX ET EVOLUTIONS DE LA CYBERSECURITE EN ENTREPRISE 14

A- Définition de la cybersécurité *14*

B- Typologie des menaces cyber *16*

C- Impact sur les organisations *18*

D- Digitalisation et augmentation des risques technologiques *20*

E- Cadre réglementaire et normatif *22*

F- Stratégies cyber des entreprises *24*

1.2- AUDIT INTERNE : UN LEVIER STRATEGIQUE POUR LA MAITRISE DES RISQUES 25

A- Définition et rôle clé de l'audit interne dans les entreprises modernes *26*

B- Méthodologies et référentiels utilisés en audit interne *29*

C- L'évolution des missions de l'audit interne face aux défis technologiques *35*

D- Limitations et défis actuels de l'audit interne dans un environnement numérique *36*

E- L'importance croissante des outils analytiques pour l'analyse des données d'audit *38*

1.3- VERS UNE GESTION INTEGREE DES RISQUES TECHNOLOGIQUES ET ORGANISATIONNELS 40

A- Les nouveaux défis liés aux risques organisationnels dans un monde connecté *40*

B- L'impact de la digitalisation sur les méthodes de gestion des risques *42*

C- L'importance d'une approche intégrée combinant audit interne et cybersécurité *43*

D- Perspectives et recommandations pour une gestion des risques efficace *44*

II- METHODOLOGIE **47**

2.1- CHOIX DE L'APPROCHE QUALITATIVE 47

2.2 – STRATEGIE D'ECHANTILLONNAGE 48

2.3 - CONSTRUCTION DU GUIDE D'ENTRETIEN 49

III- DISCUSSION DES RESULTATS **51**

3.1. ÉVOLUTION DE LA CYBERSECURITE 51

3.2. LE TERRAIN AVEC LE RISQUE CYBER 56

3.3. ÉCART AVEC LA THEORIE 61

3.4 FUTUR DE L'AUDIT INTERNE AVEC LA CYBER ET RECOMMANDATIONS POUR L'AVENIR 64

CONCLUSION **69**

ANNEXES **73**

BIBLIOGRAPHIE **105**

Liste des figures

Figure 1 : Top priorité en termes de risque en 2025 pour les directeurs d'audit interne (Source : ECIIA, 2024)

Figure 2 : Coût des cyberattaques en France en milliards de dollars américains de 2016 à 2024 (Source : Statista, 2025)

Figure 3 : NIST Framework (Source : NIST, 2024)

Figure 4 : Modèle Trois Lignes de Défense (Source : IIA, 2020)

Figure 5 : Ecosystème de l'audit interne (Source : Guemas, 2022)

Figure 6 : Nouvelles normes d'audit interne 2024 (Source : IFACI Certification – Benoit Harel, 2025)

Figure 7: Composantes du COSO ERM 2017 (Source: COSO, 2017)

Figure 8 : Détail des Composantes du COSO ERM 2017 (Source : COSO, 2017)

Figure 9 : Audit traditionnel vs audit TAAOs (Source : Fülöp, M, 2024)

Figure 10 : MITR ATT&CK Framework (Source : MITRE ATT&CK®, 2025)

Liste de sigles

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

APT : Advanced Persistent Threats

CAC : Commissaire aux Comptes

CER : Critical Entities Resilience

CERT : Computer Emergency Response Team

CMMI : Capability Maturity Model Integration

CNIL : Commission Nationale de l'Informatique et des Libertés

COBIT : Control Objectives for Information and Related Technologies

COSO ERM : Committee of Sponsoring Organizations – Enterprise Risk Management

CRIPP/IPPF : Cadre de Référence International des Pratiques Professionnelles - *International Professional Practices Framework* en anglais

CSRD : Corporate Sustainability Reporting Directive

DAI/CAE : Directeur d'audit interne – *Chief Audit Executive* en anglais

DPO : Délégué à la protection des données

DSI : Direction des systèmes d'information

ENISA : European Union Agency for Cybersecurity

IA : Intelligence artificielle

IIA : Institute of Internal Auditors

IFACI : Institut Français de l'Audit et du Contrôle Interne

ISACA : Information Systems Audit and Control Association

ISO 27001 : International Organization for Standardization

KPIs : Key Performance Metric

NIS 2 : Network and Information Security Directive 2

NIST : National Institute of Standards and Technology

OIV : Opérateur d'Importance Vitale

OSE : Opérateur de Services Essentiels

PCA/BCP : Plan de continuité de l'activité - *Business continuity plan* en anglais

PRA/DRP : Plan de reprise de l'activité - *Disaster Recovery Plan en anglais*

RGPD/GDPR : Règlement Général sur la Protection des Données - *General data protection regulation* en anglais

RPAI : Référentiel Professionnel de l'Audit Interne

RSSI / CISO : Responsable de la Sécurité des Systèmes d'Information - *Chief Information Security Officer* en anglais

TAAOs / CAATs : Techniques d'Audit Assistées par Ordinateur - Computer-aided audit tools en anglais

Triangle CIA : Confidentiality, Integrity, and Availability

Introduction

À l'ère de la transformation numérique généralisée, les entreprises font face à un paradoxe de taille : si la digitalisation représente un levier de compétitivité incontournable, elle expose également les organisations à des menaces inédites et souvent complexes. La révolution numérique de ces 25 dernières années a entraîné une profonde mutation des modes de fonctionnement des organisations, impactant l'ensemble de leurs fonctions stratégiques et opérationnelles. En parallèle, le volume de données échangées à travers le monde n'a jamais été aussi massif, rendant les systèmes d'information des entreprises privées et publiques plus critiques mais aussi plus vulnérables. Dans ce contexte, la cybersécurité s'impose comme un enjeu transversal dépassant les seuls enjeux techniques. En effet, elle s'inscrit aujourd'hui pleinement dans la stratégie globale de l'organisation. Pour les organisations, il ne s'agit plus seulement de protéger des infrastructures informatiques mais plutôt de garantir la continuité des activités. Le sujet de la conformité réglementaire et le renforcement de la confiance des parties prenantes font aussi partie de ces enjeux clés car in fine, c'est la pérennité de l'organisation doit être assurée.

Depuis le début des années 2020, on observe une intensification sans précédent des cyberattaques. Selon le rapport « Risk in Focus 2025 » (European Confederation of Institutes of Internal Auditing, 2024), près de 70 % des directeurs d'audit interne en Europe ont identifié la cybersécurité et la résilience des systèmes d'information comme une priorité absolue pour les trois prochaines années.

Audit area	Global Average	Africa	Asia Pacific	Latin America	Europe	Middle East	North America
Cybersecurity	69%	56%	63%	67%	74%	65%	87%
Governance/corporate reporting	56%	55%	55%	46%	64%	59%	58%
Business continuity	55%	58%	60%	49%	47%	60%	53%
Regulatory change	46%	39%	52%	47%	51%	35%	54%
Financial liquidity	45%	55%	30%	49%	40%	50%	46%
Fraud	41%	48%	43%	52%	36%	40%	29%
Supply chain (including third parties)	31%	29%	28%	29%	36%	31%	35%
Human capital	31%	36%	33%	29%	28%	35%	27%
Digital disruption (including AI)	25%	24%	23%	19%	23%	31%	33%
Organizational culture	23%	25%	25%	30%	24%	22%	15%
Communications/reputation	20%	24%	23%	22%	14%	18%	17%
Market changes/competition	16%	12%	25%	17%	13%	18%	10%
Health and safety	16%	15%	16%	13%	18%	17%	16%
Climate change/environment	12%	9%	16%	11%	20%	5%	9%
Geopolitical uncertainty	8%	10%	6%	12%	6%	9%	3%
Mergers/acquisitions	6%	4%	2%	7%	7%	7%	10%

Figure 1 : Top priorité en termes de risque en 2025 pour les directeurs d'audit interne (ECIIA, 2024)

En France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information), service gouvernemental français créé en 2009, rapporte une augmentation de plus de 37 % des attaques signalées entre 2020 et 2023. Les secteurs privés et publics ont été touchés sans distinction, notamment ceux de la santé ou des télécommunications. On parle notamment d'opérateurs de services essentiels (OSE), qui sont des entreprises publiques ou privées, fournissant des services informatiques essentiels. Les OSE peuvent aussi être associé aux opérateurs d'importance vitale (OIV), qui sont des organismes identifiés par l'État comme indispensable à la survie de la nation (centrales nucléaires, hôpitaux etc..). Parmi les cas récents figurent les attaques contre des hôpitaux français, France Travail, SFR ou encore Free, entraînant la compromission de données sensibles telles que les adresses mail, numéros de téléphone ou informations bancaires. Ces événements soulignent et illustrent la portée stratégique du risque cyber, dont les conséquences dépassent les seuls aspects techniques. En effet, le risque cyber est intimement liés aux risques de réputation ou encore de non-conformité réglementaire et bien sûr de pertes de résultats économiques. Face à des menaces évolutives et souvent invisibles, les organisations doivent donc désormais adopter une approche proactive et résiliente en matière de cybersécurité afin de protéger leurs intérêts.

Dans ce contexte de vulnérabilité accrue, la place de la fonction d'audit interne, qui était historiquement positionné comme une fonction d'évaluation indépendante de la maîtrise des risques, se voit transformer en un acteur stratégique de la gouvernance des organisations. Son rôle ne se limite donc plus uniquement à évaluer l'efficacité des contrôles au sein de l'entreprise mais s'étend désormais à l'accompagnement de toutes les parties prenantes de cette dernière. Cette place de l'audit interne évolue et peut maintenant prendre parfois la forme d'analyse et d'atténuation des risques cyber. En effet, la fonction s'inscrit désormais dans une logique de co-construction, contribuant à renforcer la culture du risque au sein des organisations. Pour ce faire, elle mobilise des référentiels et cadres reconnus tels que le COSO ERM 2017, le cadre COBIT 2019 ou encore les normes d'audit interne de l'IIA (Institute of Internal Auditors). Elle collabore aussi étroitement avec des acteurs clés tels que les RSSIs (Responsables de la sécurité des systèmes d'information), garant de la protection informatique mais aussi les DPOs (Délégués à la protection des données). Cette nouvelle posture implique une montée en

compétences techniques des auditeurs internes et une meilleure maîtrise des référentiels de cybersécurité. Parmi ces référentiels, les plus connus et utilisés comme ISO 27001, NIST ou encore la directive européenne NIS 2 entrée en vigueur récemment sont des outils clefs. En effet, les missions de l'audit interne ne se limitent pas à une fonction de contrôle ponctuel des risques, elles incluent également des rôles de conseil, d'alerte et d'aide à la décision pour la direction générale. L'audit interne est garant d'une vision globale et indépendante de l'efficacité des processus et notamment ceux liés à la sécurité de l'information et à la gestion des données critiques. Dans une structure pour qui le numérique constitue un enjeu critique, il est essentiel que ses auditeurs disposent de compétences leur permettant d'évaluer les processus classiques de contrôle. Mais donc aussi tous les aspects liés à la cybersécurité ; les dispositifs de sécurité applicables aux systèmes d'information, la gestion des accès et aussi la conformité aux obligations réglementaires en matière de protection des données type RGDP par exemple. Cela suppose une hybridation croissante des profils, mêlant compétences en audit, en gestion des risques, en informatique, en droit du numérique et en analyse de données. Cette modernisation de la fonction passe aussi par l'adoption de nouveaux modèles d'audit dits "agiles", permettant des interventions plus fréquentes et plus adaptées aux environnements numériques mouvants des entreprises actuelles. La fonction d'audit interne tend donc à contribuer de plus en plus à la gouvernance de la cybersécurité en participant aussi à la création d'une culture de gestion des risques partagée où chaque acteur organisationnel comprend son rôle dans la protection des actifs numériques. La collaboration avec le RSSI permet, par exemple, d'évaluer les mesures de prévention et de détection tandis que l'interaction avec le DPO garantit la prise en compte des enjeux de confidentialité et de conformité. L'audit interne devient donc ainsi une fonction charnière à la croisée de la technique, de la gouvernance et la stratégie, en pouvant jouer un rôle de facilitateur dans l'alignement des objectifs de cybersécurité avec la stratégie de l'organisation. En cela, la posture des auditeurs évolue pour tendre vers un rôle clef concernant la résilience organisationnelle. La capacité de la fonction d'audit interne à formuler des recommandations pertinentes, permet donc de constituer un levier essentiel de maturité pour l'organisation. Néanmoins, ces transformations nécessitent un accompagnement fort. Tant en matière de formation continue que d'adaptation des méthodes et outils d'audit avec pour objectif de performance globale et durable pour les organisations.

C'est dans cette dynamique de transformation que s'inscrit donc la problématique centrale de cette thèse professionnelle : de quelle manière les exigences croissantes en matière de

cybersécurité transforment-elles les approches et les outils de l'audit interne pour gérer les risques organisationnels et technologiques ? Cette question implique d'analyser d'un côté les méthodes de travail et les référentiels utilisés et de l'autre la manière dont les normes et régulations en matière de cybersécurité influencent les pratiques d'audit. Comprendre comment les professionnels de l'audit adaptent leurs missions à ces nouvelles exigences réglementaires et sécuritaires constitue un enjeu majeur. C'est cet enjeu que cette thèse professionnelle propose d'explorer à travers une approche théorique et empirique ancrée dans les pratiques du terrain.

Les objectifs de cette thèse professionnelle sont multiples. Sur le plan académique, elle vise à enrichir la réflexion sur les mutations de l'audit interne dans un environnement digitalisé et réglementaire en pleine évolution, notamment au sein de l'Union Européenne. Sur le plan professionnel, il ambitionne de fournir des leviers concrets pour renforcer les synergies entre audit interne et fonctions de cybersécurité, en apportant une identification des défis rencontrés au quotidien par les auditeurs. Le travail repose sur l'analyse des référentiels normatifs, des bonnes pratiques organisationnelles et aussi sur des retours d'expérience collectés auprès de professionnels en poste.

Pour cela, une méthodologie qualitative a été retenue. Huit entretiens semi-directifs seront réalisés auprès de professionnels exerçant des fonctions clés dans la cybersécurité et l'audit (Directeurs d'audit interne, RSSI, DPO, experts data…). Ces entretiens, fondés sur un guide structuré, ont été analysé à travers un codage thématique rigoureux. L'analyse porte sur trois axes principaux : (1) les perceptions des évolutions récentes des menaces et normes cyber, (2) les impacts sur les missions, les outils et compétences de l'audit interne et (3) les dynamiques de collaboration entre les 3 lignes de défenses (opérationnels, contrôles internes, gestions des risques et audits internes). Cette approche permet de croiser les enseignements de la littérature avec la réalité des pratiques observées sur le terrain.

Incluant les entretiens, cette thèse professionnelle est structurée en trois grandes parties. La première partie développe le cadre théorique à travers une revue de littérature portant sur les enjeux de la cybersécurité, le rôle stratégique de l'audit interne et les approches intégrées de gestion des risques. La deuxième partie présente la méthodologie adoptée et détaille le processus de collecte et d'analyse des données qualitatives. Enfin, la troisième partie est consacrée à l'analyse des résultats empiriques, à leur confrontation avec les apports théoriques

et à l'élaboration de recommandations opérationnelles. Une conclusion générale viendra clore cette thèse professionnelle en apportant une réponse à la problématique initiale en proposant des pistes de recherche futures et des possibilités d'évolutions pour la fonction d'audit interne.

I- Revue de Littérature

1.1- Les enjeux et évolutions de la cybersécurité en entreprise

Dans cette partie, nous allons définir ce qu'est la cybersécurité, les typologies de menaces et l'impact sur les organisations. Ainsi, nous aurons une vue plus claire sur les éléments qui vont constituer une base pour notre compréhension du sujet. Par la suite, nous allons développer la digitalisation et l'augmentation des risques technologiques, le cadre réglementaire et normatif et enfin les stratégies cyber des entreprises.

A- Définition de la cybersécurité

La cybersécurité est aujourd'hui un enjeu essentiel pour toutes les organisations. Avec l'accélération de la digitalisation, la dépendance aux systèmes d'information est devenue totale dans de nombreuses entreprises. Le NIST (National Institute of Standards and Technology) évoque que la cybersécurité est parfois définie comme « la protection des informations et des systèmes d'information contre l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisée, afin d'assurer la confidentialité, l'intégrité et la disponibilité ». La cybersécurité regroupe l'ensemble des moyens techniques, humains et organisationnels qui visent à protéger les données et les systèmes informatiques contre des attaques. Elle repose sur trois grands principes fondamentaux : la confidentialité (confidentiality), l'intégrité (integrity) et la disponibilité (availability), souvent appelés le triangle CIA. La confidentialité consiste à s'assurer que seules les personnes autorisées peuvent accéder à une information. L'intégrité peut être définie comme le fait qu'une information n'a pas été modifiée de manière non autorisée. Enfin, la disponibilité garantit que les systèmes fonctionnent et que les données sont accessibles au moment où les utilisateurs en ont besoin.

Le guide des risques cyber publié par l'IFACI en 2020 explique comment ces principes sont au cœur des politiques de sécurité mises en place dans les entreprises. Le document insiste également sur la montée en puissance des menaces ainsi que sur la nécessité d'une vigilance constante. Alain Clapaud le souligne notamment, dans son œuvre Cybersécurité au défi des nouvelles menaces (2024), que les entreprises ne peuvent plus se contenter de solutions techniques classiques : elles doivent adapter en permanence leur stratégie de protection car les attaques deviennent plus intelligentes et ciblées.

Dans son ouvrage pédagogique La cybersécurité (2023), Charles Perez rappelle aussi que la cybersécurité ne concerne pas uniquement les grandes entreprises ou les spécialistes informatiques mais bien l'ensemble des entreprises, incluant les petites et moyennes organisations. La cybersécurité est désormais une priorité stratégique pour toutes les organisations, quel que soit leur secteur d'activité. Il précise que la protection des systèmes ne repose pas uniquement sur des pares-feux ou des antivirus mais aussi sur une culture de la sécurité à tous les niveaux de l'entreprise.

La cybersécurité, ce n'est donc pas seulement une affaire de technologie. C'est donc un levier pour garantir la continuité d'activité, la confiance des clients ainsi que le respect des lois. C'est ce qui en fait un enjeu majeur pour les entreprises aujourd'hui.

Selon le rapport "Panorama de la cybermenace 2024 : mobilisation et vigilance face aux attaquants", l'ANSSI a traité 4 386 attaques envers différents types de structures. Cela indique donc le nombre minimum d'attaques au cours de l'année 2024 car ce chiffre relate uniquement les événements de sécurité dont l'agence s'est occupée. Selon ce rapport, les attaques cyber se sont intensifiées de l'ordre de 15 % en 2024 par rapport à 2023.

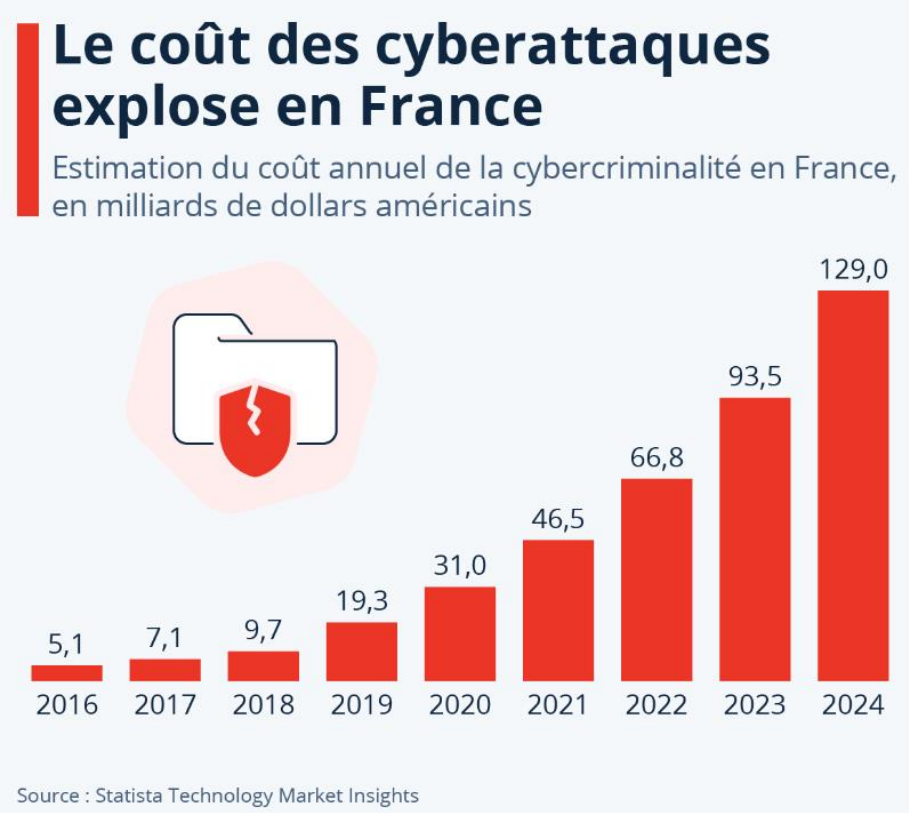


Figure 2 : Coût des cyberattaques en France en milliards de dollars américains de 2016 à 2024 (Source : Statista, 2025)

Selon le rapport Risk in Focus 2025, les risques cyber et la sécurité des données sont classés dans le top 5 des préoccupations de 83 % des auditeurs internes. Ces menaces évoluent vite et touchent tous les secteurs, y compris les start-ups, les hôpitaux et les administrations. Pour aller plus loin, des organismes comme l'ENISA (Agence de l'Union européenne pour la cybersécurité) publient des études sur les tendances actuelles des menaces cyber, des rapports annuels des cybermenaces dans l'Union, des bonnes pratiques pour faire face aux menaces et évoquent les normes notamment NIS2. Ces ressources permettent d'avoir une vision claire des attaques les plus courantes et de comment mieux s'y préparer. Comprendre la typologie des menaces est donc une étape essentielle pour que les organisations puissent mettre en place une stratégie de cybersécurité efficace. Cela permet d'anticiper les attaques en sensibilisant les équipes ainsi que de bâtir des systèmes de défense adaptés aux nouveaux risques.

B- Typologie des menaces cyber

Les menaces cyber sont variées, notamment par leur constante évolution et peuvent avoir des conséquences graves sur les organisations. Pour bien comprendre les risques auxquels font face les entreprises, il est utile de distinguer plusieurs types d'attaques.

La première menace très répandue est le rançongiciel ou ransomware. Il s'agit d'un logiciel malveillant qui bloque l'accès aux données ou au système, en demandant le paiement d'une rançon pour les débloquer. Ce type d'attaque a paralysé de nombreux hôpitaux en France ces dernières années, comme le Centre Hospitalier Universitaire de Brest (mars 2023) ou celui de Versailles (décembre 2022). Ces attaques peuvent forcer un hôpital à suspendre ses opérations, ce qui met directement en danger la vie des patients. Le rapport 2024 de l'ANSSI indique que les attaques par ransomware sont les plus fréquentes dans le secteur public en France. Selon un article du journal le point "Pourquoi les hôpitaux français restent les cibles privilégiées des cybercriminels" (2025) et de la mutuelle Verspiren "Risques cyber pour les hôpitaux : pourquoi le secteur de la santé doit renforcer sa cybersécurité" (2025), les hôpitaux sont des cibles faciles du fait du matériel vieillissant et les interconnexions avec l'extérieur (médecins libéraux et les laboratoires) ce qui permet une plus grande surface d'attaque. De plus, selon ces deux sources, les hôpitaux français consacrent en moyenne 1,7% de leur budget dans le numérique avec

seulement 7 % des hôpitaux qui ont un responsable de la sécurité des systèmes d'information (RSSI) à plein temps.

Une autre menace classique est le phishing ou hameçonnage. C'est une méthode qui consiste à envoyer de faux e-mails imitant des messages légitimes pour tromper les utilisateurs et récupérer leurs identifiants ou informations confidentielles. Comme le montre Charles Perez, dans La cybersécurité (2023), cette méthode reste redoutablement efficace parce qu'elle s'appuie sur l'erreur humaine plutôt que sur des failles techniques. Le phishing fait aujourd'hui partie intégrante de la vie des Français. Selon Cybermalveillance.gouv.fr qui a publié un article en 2024 sur les Français face aux cybermenaces, nous pouvons découvrir que 73 % des Français ont été confrontés au moins une fois au phishing par texto, mail ou encore appel téléphonique. La dernière attaque en date est la réception d'un texto comme celui-ci "Bonjour, vous êtes chez vous ?" c'est une attaque basique qui permet de diminuer la vigilance des personnes ciblées qui vont répondre et par la suite recevoir un lien qui permet de vous voler vos données. L'hameçonnage est parfois très ciblé ce qui encore une fois diminue la vigilance des personnes visées avec leur nom, leurs informations personnelles afin de donner de la légitimité au mail ou SMS reçu.

Il existe aussi des attaques ciblées, qu'on appelle aussi menaces persistantes avancées (APT). Les APT sont des cyberattaques discrètes qui permettent aux attaquants de garder un accès au réseau de l'entreprise ciblée. Sur le site de l'entreprise Oracle, un article détaille les possibilités qu'offrent les APT. Les APT sont donc une intrusion discrète. Ils peuvent aussi être définis comme les créateurs de portes dérobées dans le réseau IT de l'entreprise, permettant aux cybercriminels d'accéder au réseau quand ils le souhaitent. Ces attaques sont organisées, discrètes et visent une cible spécifique pour obtenir des informations sensibles ou perturber l'activité. En 2024, France Travail (anciennement Pôle Emploi) a été victime de ce type d'attaque massif ayant exposé les données personnelles de millions d'utilisateurs français. Ces menaces sont souvent liées à des groupes criminels organisés qui peuvent aussi avoir des intérêts géopolitiques. Depuis le déséquilibre de l'ordre mondial à partir de la guerre en Ukraine, les attaques cyber contre la France se sont multipliées. La Russie et la Chine sont deux pays qui ont beaucoup recours aux cyberattaques à but politique afin de déstabiliser les pays cibles. Selon l'ANSSI, les attaquants réputés à la Chine et à la Russie sont considérés comme faisant partie des 3 principaux risques pour l'écosystème national d'un point de vue

systémique. Selon l'article de l'ANSSI (2025), les attaquants réputés à intérêts russes ont notamment continué leurs attaques pour la recherche d'informations pouvant soutenir leurs efforts militaires et/ou diplomatiques. Quant aux attaquants réputés à intérêts chinois, ils ont eu une activité davantage tournée vers la captation de renseignements d'ordre stratégique et économique. Le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) publie régulièrement des bulletins d'alerte sur ces menaces et les techniques utilisées. Les publications sont classifiées en six catégories, dont les alertes de sécurité, les menaces et incidents, les indicateurs de compromissions ou encore les bulletins d'actualité.

Le guide des risques cyber de l'IFACI (2020) propose une classification détaillée des risques cyber, en expliquant comment les auditeurs internes peuvent les détecter et les prévenir. Il insiste notamment sur l'importance de prendre en compte non seulement les aspects techniques mais aussi les comportements des utilisateurs.

Ces trois typologies de menaces sont les plus connues et les plus répandues aujourd'hui. Néanmoins, cela ne nous permet pas réellement de connaître les dommages que celles-ci peuvent représenter pour les organisations ciblées. De ce fait, nous allons évoquer les principaux impacts sur les organisations que ces menaces constituent.

C- Impact sur les organisations

Les attaques cyber ne sont pas seulement des incidents techniques : elles peuvent avoir des conséquences directes sur la performance et la réputation des organisations. Un système informatique compromis peut entraîner des pertes financières importantes, des interruptions d'activité partielles ou totales mais aussi des sanctions juridiques et une perte de confiance des clients et investisseurs.

L'un des premiers impacts concerne la performance opérationnelle. Une attaque réussie peut paralyser tout ou une partie de l'entreprise. Comme l'explique Alain Clapaud, certaines entreprises mettent plusieurs semaines à se remettre d'une cyberattaque. Cela signifie des retards dans la production, des pertes de contrats, voire une cessation temporaire d'activité. Afin de limiter le temps entre l'arrêt de l'activité et la reprise de celle-ci, il est demandé aux entreprises de mettre en place des processus de plan de continuité d'activité, autrement appelés

PCA. Le PCA permet aux entreprises de savoir comment réagir en cas d'attaque et de limiter au maximum l'impact d'une attaque. Par la suite, il faut mettre en place le plan de reprise d'activité (PRA). Le PRA a pour objectif de définir l'ordre et la nature des actions à mettre en place pour une reprise d'activité normale. Sans PCA et PRA, une entreprise peut mettre plusieurs semaines, voire des mois, avant de pouvoir retrouver une bonne performance dans sa production ou dans la qualité de service. Ces deux éléments permettent un retour à la performance opérationnelle pré-attaque plus rapide et organisé.

Ensuite, il y a un enjeu juridique et réglementaire. Depuis l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en 2018, les entreprises doivent protéger toutes les données personnelles (clients et collaborateurs) qu'elles traitent. En cas de faille de sécurité, elles sont tenues de la déclarer à la CNIL (Commission nationale de l'informatique et des libertés) et peuvent se voir infliger des amendes pouvant aller jusqu'à 4% de leur chiffre d'affaires annuel mondial. Le guide pratique de Ligaudan (2024) explique comment le RGPD oblige les entreprises à mettre en place des procédures claires de gestion des incidents et à documenter leurs actions de prévention.

Le coût réputationnel est également un impact fort pour les entreprises. Ce coût réputationnel peut se caractériser par une fuite de données ou bien simplement une communication sur l'entreprise pour des faits avérés ou non. Par exemple, une entreprise qui subit une fuite de données sensibles peut entraîner une perte de confiance de ses clients et de ses investisseurs mais plus globalement, de l'ensemble de ses parties prenantes. Cela est d'autant plus vrai dans les secteurs dits « sensibles » comme la santé, les télécommunications ou encore les services publics. Jamison souligne, dans The Future of Cybersecurity in Internal Audit (2018), que les entreprises qui réagissent mal à une crise cyber voient leur image durablement dégradée. La récente attaque qu'a subie l'entreprise Naval Groupe, groupe industriel spécialisé dans la construction navale de défense, est le parfait exemple du risque réputationnel. L'entreprise publie un communiqué le 26 juillet 2025, sur LinkedIn, à propos d'une attaque sans réelle intrusion dans ses environnements informatiques. L'entreprise déplore que l'enjeu soit simplement stratégique afin de déstabiliser ses partenaires et potentiels clients au vu de la situation géopolitique actuelle. Il semblerait donc que Naval Groupe n'ait pas subi de réelle intrusion dans ses systèmes, mais une telle information relayée sur les réseaux sociaux peut faire bien plus de mal à une entreprise qu'une réelle perte de données. Les clients de Naval

Groupe sont confidentiels pour des raisons stratégiques ; certains pays actuellement en négociation pourraient se retirer des négociations. L'attaque qu'a subi Naval Groupe est suffisante pour mettre à mal sa réputation, que l'attaque soit avérée ou non. Naval Groupe a communiqué rapidement sur cet incident afin de limiter les risques réputationnels.

Pour mieux gérer ces risques, plusieurs indicateurs de performance (KPIs) liés à la cybersécurité peuvent être utilisés dans les organisations. Par exemple, le temps moyen de détection aux standards de sécurité, tester les employés avec des campagnes de phishing pour savoir quelle population n'est pas assez vigilante, test d'intrusion dans les systèmes avec deux équipes ou encore challenger le PCA et PRA. La mise en place d'audit continu via un outil, permettrait d'avoir une information plus fiable avec l'ensemble des données de l'entreprise et d'avoir une vue d'ensemble non figée sur une période précise. Le rapport de Deloitte, « Cybersecurity and the role of internal audit – an urgent call to action » (S.d.), recommande aux entreprises de suivre ces indicateurs pour mieux évaluer leur posture face aux cybermenaces.

Les entreprises doivent donc intégrer la cybersécurité dans leur stratégie globale, non seulement pour éviter les pertes mais aussi pour garantir leur pérennité à long terme.

D- Digitalisation et augmentation des risques technologiques

La transformation numérique est aujourd'hui incontournable pour les organisations, mais elle entraîne aussi une augmentation des risques liés aux technologies. Plus les systèmes sont interconnectés, plus la surface d'attaque s'élargit.

Selon l'étude de KPMG intitulée Explorer les nouveaux horizons technologiques (s.d.), les nouvelles technologies comme le cloud, l'intelligence artificielle ou l'internet des objets (IoT) offrent des opportunités importantes pour les entreprises mais introduisent également de nouvelles vulnérabilités. Par exemple, seul 43% des entreprises se disent capables d'évaluer les technologies utilisées. Cela montre des lacunes dans les domaines qui prennent davantage de place dans nos entreprises comme l'intelligence artificielle ou le cloud. Il est encore aujourd'hui difficile pour les entreprises d'identifier et d'évaluer les risques liés aux outils informatiques, à l'IA et au cloud. L'étude nous indique également que l'intelligence artificielle est la technologie la moins bien maîtrisée dans le cadre d'audit interne étant donné sa croissance

importante. Néanmoins, la cybersécurité et les données personnelles (RGPD) semblent bien maîtrisées avec respectivement 75 et 80% des interrogés en capacité d'auditer ces sujets.

Harisaiprasad, dans son analyse comparative entre COBIT 5 et COBIT 2019, montre que les référentiels de gouvernance IT ont évolué pour répondre à ces nouveaux défis. Par exemple, le COBIT 5 comptait cinq principes de gouvernance lorsque le COBIT 19 en compte six. Il y a des changements de terminologie pour certains processus. Les principes du cadre de gouvernance ont également été ajoutés dans le COBIT 19 et la technique pour mesurer la performance a été changée. La mesure de la performance était calquée sur l'échelle de 0 à 5 du standard ISO/IEC 33000 ; maintenant, l'échelle de 0 à 5 du CMMI est utilisée. Cette échelle donne davantage de détails sur les paliers et permet d'être moins dans l'interprétation et d'être guidé. De manière plus générale, le COBIT 5 se concentrait essentiellement sur les objectifs métier et l'alignement stratégique. Or le COBIT 19 introduit une approche personnalisable de la gouvernance des technologies. Ce nouveau cadre théorique propose une architecture plus modulable permettant aux organisations une certaine adaptabilité de ces principes de gouvernance à leurs priorités. Une avancée majeure de COBIT 2019 réside dans l'intégration de la gestion des risques cyber dès la phase de conception des processus numériques.

Le rapport Risk in Focus 2025 de l'ECIIA confirme que les auditeurs internes placent la digitalisation et la cybersécurité parmi les préoccupations prioritaires. En effet, chaque innovation technologique s'accompagne de nouveaux risques : cybercriminalité, mauvaise gestion des données ou encore dépendance à des prestataires externes.

Jamison insiste sur le rôle central que doit jouer l'audit interne pour anticiper et gérer ces risques technologiques. Il explique notamment que la transformation digitale doit aller de pair avec le renforcement des dispositifs de sécurité, sans quoi l'innovation peut se retourner contre l'organisation.

Enfin, la digitalisation, si elle est mal accompagnée, comporte des risques de fragiliser l'entreprise. C'est pourquoi il est essentiel d'intégrer la gestion des risques cyber dans chaque projet numérique ou informatique.

E- Cadre réglementaire et normatif

Face à l'intensification des cybermenaces, les organisations évoluent dans un environnement de plus en plus normé par des dispositifs réglementaires. Ces cadres, qu'ils soient nationaux, européens ou internationaux, ont pour objectif de structurer la gouvernance de la cybersécurité et d'harmoniser les bonnes pratiques dans la gestion des risques.

En France, la loi informatique et libertés de 1978 constitue la base légale en matière de protection de données personnelles. Cette dernière a été révisée à plusieurs reprises. Elle a été adaptée pour intégrer les exigences du Règlement général sur la protection des données (RGPD) dès son entrée en vigueur en 2018. L'autorité de référence, d'un point de vue national, reste la CNIL (Commission nationale de l'informatique et des libertés), qui accompagne les organisations dans leur mise en conformité et peut sanctionner en cas de manquement.

Certaines obligations du RGPD ont dû être transposées au niveau national comme :

- La désignation obligatoire d'un Délégué à la protection des données (DPO) (toutes structures manipulant des données personnelles ou établissement publics)
- L'obligation de notifier toute violation de données dans un délai maximum de 72 heures

Le guide pratique de Ligaudan (2024) revient sur ces obligations et leur mise en œuvre au sein des entreprises françaises. Depuis 2018, la CNIL a renforcé ses contrôles avec une montée en puissance des sanctions dans les secteurs de la santé et de la finance.

Au niveau européen, l'adoption du RGPD s'est faite en avril 2016 avec une entrée en vigueur mi-2018. L'objectif de cette réglementation est de protéger les droits fondamentaux des citoyens européens, d'harmoniser la législation nationale et de responsabiliser les entreprises en matière de traitement des données. Le RGPD oblige les entreprises à obtenir le consentement explicite des utilisateurs pour utiliser leurs données, le droit à l'oubli, donc la suppression de leurs données. Le RGPD a considérablement transformé les pratiques dans l'Union européenne. Cela a permis une prise de conscience commune des enjeux liés à la donnée et renforce la posture sécuritaire dans les grandes organisations.

En parallèle, d'autres textes encadrent la cybersécurité à un niveau plus large. En effet, la directive NIS2 (Network and Information Security), qui a été adoptée par l'Union européenne en novembre 2022, implique un renforcement des exigences de sécurité et impose des obligations de reporting plus strictes pour les organisations. Comme pour le RGPD, la

notification des incidents majeurs doit être faite dans un délai de 24 à 72 heures aux autorités compétentes et les amendes sont calculées sur un pourcentage du chiffre d'affaires mondial. Pour NIS2, les amendes vont jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial.

Sur le plan national, la retranscription des nouvelles normes de l'audit interne par l'IFACI, indique que certains éléments technologiques doivent être mis en place par les directions d'audit interne. Les éléments à mettre en place sont énoncés dans la norme 10.3. Cette norme s'intitule « Norme 10.3 Ressources technologiques ». Cette norme met en évidence l'importance de la mise en place de ressources technologiques pour le bon fonctionnement des départements d'audit interne. Le guide énumère la méthode pour mettre en place une nouvelle technologie. Cette méthode consiste à évaluer les ressources actuelles de technologies et à rechercher des façons d'améliorer l'efficacité de la fonction audit interne. Ensuite, le responsable de l'audit interne doit informer le conseil et la direction générale des limites en termes de ressources auxquelles ils font face. Enfin, le responsable de l'audit interne doit prévoir les formations adéquates à l'utilisation de ces nouvelles technologies et rentrer en contact avec les équipes IT pour maximiser le bon déploiement des outils.

Sur le plan international, plusieurs normes guident les entreprises. La norme ISO/IEC 27001 est la plus connue. Elle permet de structurer un système de management de la sécurité de l'information (SMSI). La dernière révision de cette norme date de 2022. ISO/IEC 27001 repose sur une logique d'amélioration continue et propose une cartographie complète des exigences organisationnelles et techniques. L'adoption de cette norme par les grandes entreprises et les organisations certifiées témoigne de sa légitimité. Le second standard est promulgué par l'IIA via le Cybersecurity Topical Requirements (2025). Ce standard vise à assurer une bonne maîtrise des risques cyber. Il fournit une approche compréhensive afin d'évaluer la mise en place d'une gouvernance et la gestion du contrôle de la cybersécurité. Nous trouvons donc un volet spécifique sur la gouvernance, sur le management des risques et sur les contrôles à mettre en place. Ce standard définit la base des éléments à mettre en place pour évaluer la cybersécurité dans une organisation. On peut donc considérer que ce Topical Requirements soit une première entrée dans le monde de la cybersécurité et soit complété par les normes COBIT fournies par l'ISACA. Enfin, le troisième référentiel international connu est le NIST Cybersecurity Framework (CSF). Le référentiel est principalement utilisé aux États-Unis et est également une référence pour structurer les efforts de cybersécurité en cinq fonctions :

identifier, protéger, détecter, répondre et récupérer. Ce référentiel est recommandé pour les entreprises souhaitant se doter d'un cadre opérationnel sans nécessairement viser une certification formelle.

Figure 3 : NIST Framework (Source : NIST, 2024)

Le guide de l'IFACI recommande d'aligner la gouvernance cyber sur ces normes pour assurer une gestion structurée des risques. De même, le rapport du COSO (2017) insiste sur l'intégration des risques cyber dans la stratégie globale de l'entreprise.

Respecter ces cadres réglementaires et normatifs permet non seulement d'être en conformité mais aussi d'asseoir une véritable culture de la sécurité au sein de l'organisation.

F- Stratégies cyber des entreprises

Face à la complexité des menaces, les entreprises développent de plus en plus des stratégies globales de cybersécurité. Ces stratégies s'appuient sur plusieurs piliers : la gouvernance, les plans de résilience ou encore la formation et la culture cyber.

La gouvernance de la cybersécurité consiste notamment à définir des rôles et des responsabilités clairs. Le rapport de KPMG, « Internal audit: key thematic areas to consider in 2025 » publié en 2024, souligne l'importance de désigner clairement un responsable de la sécurité des systèmes d'information (RSSI) et de l'intégrer dans les instances de décision. Les comités d'audit doivent aussi s'impliquer davantage dans ces questions cyber.

Les plans de résilience permettent aux entreprises de réagir efficacement en cas d'incident. Il s'agit notamment de mettre en place des procédures de gestion de crise ou encore de sauvegarde des données. Mais le plus important et crucial reste au niveau de la continuité d'activité, d'où l'importance d'avoir un PCA et un PRA détaillés et clairs.

La formation est un autre levier essentiel. Jamison explique que de nombreuses attaques réussissent parce que les collaborateurs ne sont pas suffisamment formés aux risques cyber. Il faut donc organiser des campagnes de sensibilisation régulières afin de tester les réactions des employés face à des scénarios d'attaque.

Enfin, une véritable culture de la cybersécurité doit être développée dans les organisations. Cela signifie que la sécurité ne doit pas être perçue comme un frein par certains collaborateurs ou personnes dirigeantes mais comme une condition du bon fonctionnement de l'entreprise. Les référentiels de l'IIA, les normes internationales pour la pratique professionnelle de l'audit interne (2024) et de l'IFACI, Référentiel professionnel de l'audit interne (RPAI) actualisé en 2025, suggèrent l'importance de diffuser cette culture à tous les niveaux.

Adopter une stratégie complète de cybersécurité, ce n'est pas seulement acheter des outils techniques, c'est aussi faire évoluer les comportements, les procédures et les modes de gouvernance.

Les référentiels encadrant la cybersécurité sont multiples et se complètent. Après une compréhension du sujet et une définition claire de la cybersécurité et des impacts potentiels sur les entreprises, nous allons ainsi préciser le rôle de l'audit interne dans la mise en place de la cybersécurité.

1.2- Audit interne : un levier stratégique pour la maîtrise des risques

Dans cette partie, nous allons définir ce qu'est l'audit interne et quel est son rôle au sein des organisations. Ensuite, nous évoquerons les différentes méthodologies qu'utilise la fonction d'audit interne et puis nous verrons comment se fait l'évolution de l'audit interne et de ses missions dans des environnements de plus en plus digitalisés. Enfin, nous aborderons les outils technologiques et les méthodes d'audit utilisés pour faire face à ces nouveaux risques.

A- Définition et rôle clé de l'audit interne dans les entreprises modernes

Abordons maintenant une partie cruciale de cette thèse professionnelle, l'audit interne. Il existe plusieurs définitions de l'audit interne. Pour cette thèse professionnelle, la définition retenue est celle de l'Institute of Internal Auditors, institut voué à l'établissement de standards professionnels d'audit interne créé en 1941 aux États-Unis. L'IIA a pour objectif de défendre à l'international les intérêts de la profession d'audit interne, regroupant 165 pays. L'audit interne est donc défini par l'IIA comme une activité « indépendante et objective qui contribue à la réussite de l'organisation en soutenant la protection et la création de valeur dans un cadre de gouvernance, de gestion des risques et de contrôle.» Cette nouvelle définition marque une évolution significative par rapport à l'ancienne version du Cadre de Référence International des Pratiques Professionnelles de l'audit interne (CRIPP) de 2012, qui mettait davantage l'accent sur l'assurance et les conseils apportés par l'audit interne. En effet, ici l'accent est clairement mis sur la notion de contribution directe à la réussite de l'organisation avec pour objectif l'intégration totale de la logique de création de valeur dans un cadre stratégique et non plus seulement opérationnel.

Cette reformulation souligne la transformation progressive de la fonction qui passe progressivement d'un rôle de contrôle a posteriori à un acteur intégré au dispositif de gouvernance. L'auditeur interne est donc désormais considéré comme une ressource stratégique ayant la capacité d'apporter une analyse transversale des risques ainsi que de soutenir la performance de l'entreprise à travers des recommandations concrètes et utiles.

Cette évolution est également reflétée dans la mise à jour du Référentiel Professionnel de l'Audit Interne (RPAI) 2025. Contrairement à l'édition de 2012, qui reposait sur quatre principes (indépendance, compétence, déontologie, approche fondée sur les risques), le nouveau cadre introduit une lecture plus intégrée de la fonction d'audit. En particulier, le Domaine III "Gouvernance" précise que l'audit interne doit renforcer la transparence, l'approbation (accountability en anglais) ainsi que favoriser la prise de décision fondée sur les risques. Ce domaine insiste aussi sur l'importance du positionnement de l'audit au sein de la gouvernance, en tant qu'interlocuteur actif et indépendant du comité d'audit, des instances dirigeantes et des autres lignes de défense.

La fonction d'audit interne s'inscrit d'ailleurs dans le modèle "Three Lines of Defense" de l'IIA, crée en 2013 et réactualisé en 2020. Ce modèle constitue un cadre de référence théorique

qui vise à clarifier les différents rôles et responsabilités liées à la gestion du risque en distinguant trois fonctions complémentaires : la première ligne de défense dite ”opérationnelle”, la deuxième ligne liée aux fonctions de contrôle interne, de conformité et de gestion des risques et enfin la troisième ligne qui correspond à l'audit interne. Ce modèle de ligne de défense a pour objectif de construire une gouvernance robuste autour de la gestion du risque avec un contrôle permanent, effectué par la première et la deuxième ligne et un contrôle périodique effectué par l'audit interne. La réactualisation du modèle en 2020, réaffirme l'importance de la gouvernance globale et de la collaboration entre ces trois lignes. L'objectif de création de valeur reste central et clair pour ces trois fonctions, qui doivent se coordonner et s'articuler pour assurer une gestion des risques solide en fournissant une assurance à l'ensemble des parties prenantes.

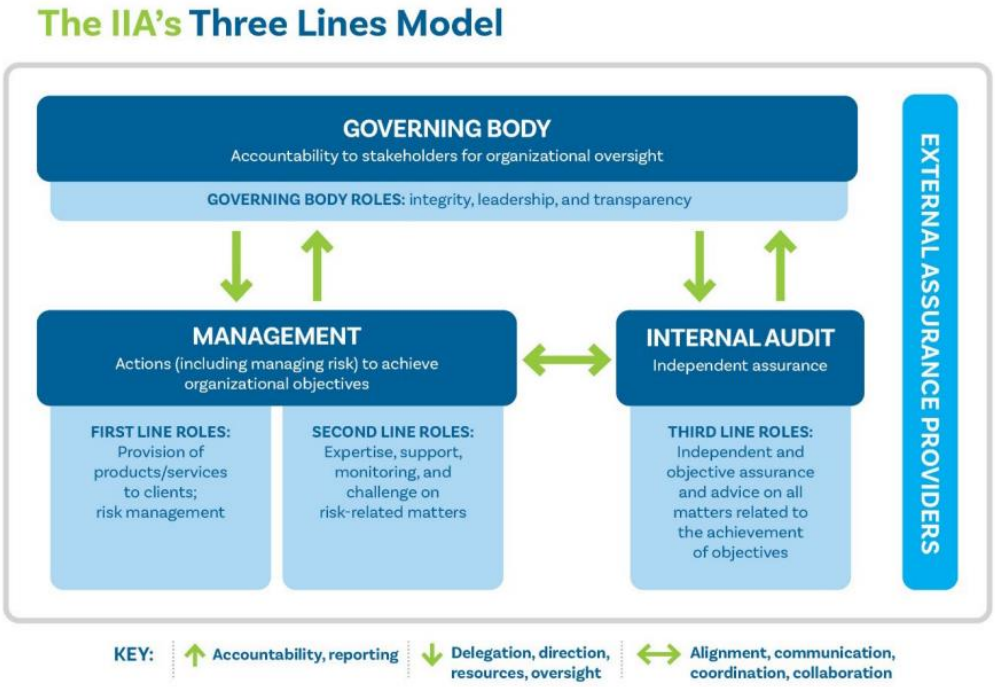


Figure 4 : Modèle Trois Lignes de Défense (Source : IIA, 2020)

Dans un environnement marqué par la transformation digitale rapide et des exigences réglementaires nationales et internationales croissantes, l'audit interne est donc appelé à jouer un rôle clé. Il accompagne les parties prenantes dans l'identification des risques mais surtout dans la conception et l'anticipation de dispositifs de maîtrise. Ce positionnement en amont de ces dispositifs permet d'augmenter leur maturité de contrôle et d'apporter une valeur ajoutée stratégique aux projets transversaux.

De plus, l'audit interne est aujourd'hui un acteur central de la gouvernance. Il est l'interlocuteur privilégié du comité d'audit, auquel il rend compte de ses travaux. Ce même comité le mandate d'ailleurs pour réaliser ses missions d'audit dans le respect de son indépendance. Il peut aussi intervenir auprès du conseil d'administration, notamment pour éclairer les zones de risques majeurs en lien avec la résilience technologique ou encore la conformité aux exigences règlementaires (type RGPD ou Sapin 2). Cette proximité avec les organes de gouvernance, comme le souligne le Domaine III des nouvelles normes d'audit interne de 2024, est donc essentielle pour garantir une gouvernance transparente, comportant une orientation forte vers la performance durable. La crédibilité et l'utilité des travaux d'audit reposent sur cette posture indépendante mais aussi sur leur impact pour les parties prenantes internes.

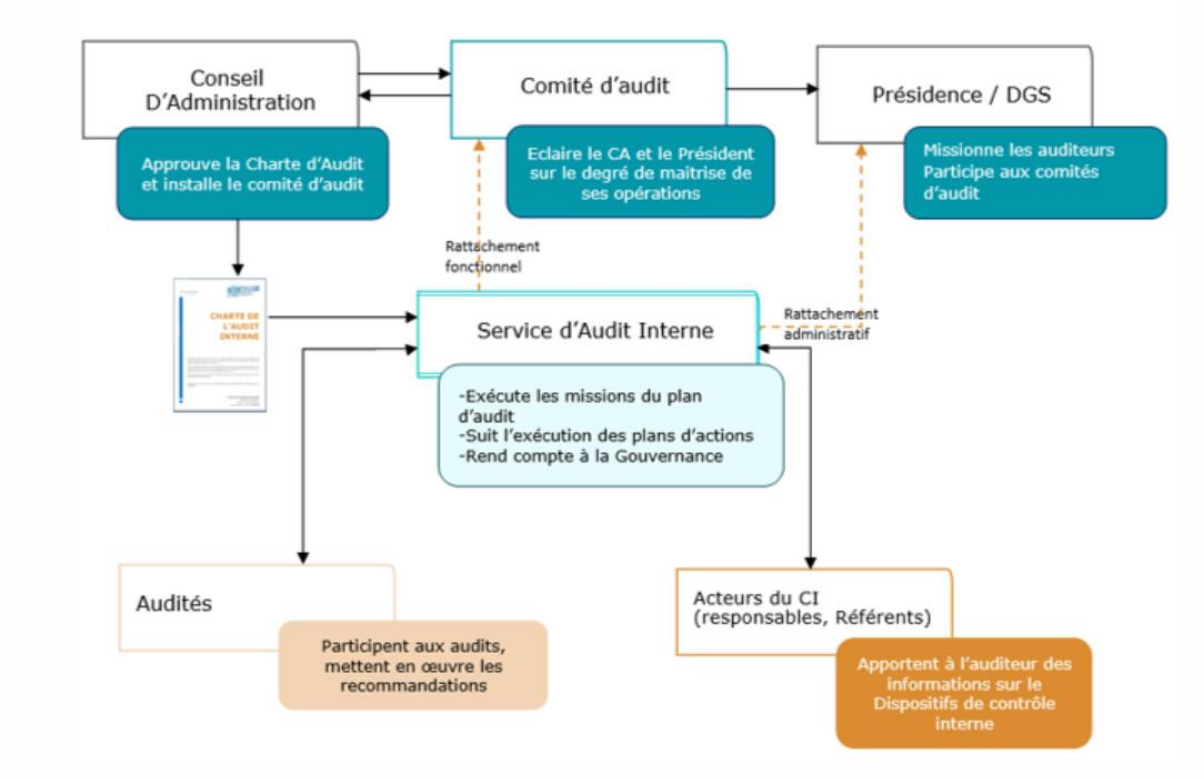


Figure 5 : Ecosystème de l'audit interne (Source : Guemas, 2022)

En parallèle de cet aspect gouvernance, la notion de création de valeur par l'audit interne a pris de l'ampleur depuis les années 90. Il ne s'agit plus uniquement de produire des rapports ou encore de constater des écarts mais plutôt d'accompagner les directions métiers dans l'amélioration de leur pilotage. Comme le rappellent les auteurs du Risk in Focus 2024 (2023), cette valeur passe par 3 points clefs ; la qualité des échanges, la pertinence des

recommandations et la compétence de l'auditeur à comprendre le contexte opérationnel spécifique de chaque entité auditée. En effet, au-delà de la maîtrise des compétences techniques (hard skills) nécessaire au bon déroulement des missions d'audit, les compétences comportementales (soft skills) sont aujourd'hui tout aussi, voir plus importantes que ces dernières. La communication, l'esprit critique, l'adaptabilité et la capacité à instaurer la confiance avec les audités sont des clefs que les auditeurs se doivent de maitriser. Concrètement, la compétence la plus importante de l'auditeur interne doit résider dans sa posture assertive en tous points.

B- Méthodologies et référentiels utilisés en audit interne

Les pratiques d'audit interne sont encadrées par des référentiels, assurant une qualité et une universalité entre des missions d'audit, indépendamment des secteurs d'activités. Cela permet aux parties prenantes des entreprises, notamment les actionnaires, d'avoir une vision claire des activités de l'audit interne. Le cadre de l'IIA repose notamment sur l'International Professional Practices Framework (IPPF), dans sa version française Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne (CRIPP), qui définit les normes professionnelles de la profession. Ce cadre, mis à jour en 2024, expose 15 principes clefs, de l'éthique au suivi des plans d'action.

À travers cette réforme, le référentiel de 2024 introduit une nouvelle structuration qui clarifie les attentes à l'égard de la fonction d'audit interne dans un environnement de plus en plus digitalisé et exposé à des risques multidimensionnels. Le RPAI 2025, transposition française du nouveau cadre de l'IIA, repose désormais sur cinq domaines précis qui définissent clairement le cadre normatif de la profession :

- Domaine I – Mission de l'audit interne, qui précise la raison d'être de la fonction et sa contribution directe à la réussite stratégique de l'organisation.
- Domaine II – Éthique et professionnalisme, fixant les principes essentiels à respecter pour les auditeurs internes en termes d'intégrité, d'objectivité, de compétence, de conscience professionnelle et de confidentialité.
- Domaine III – Gouvernance de la fonction d'audit interne, domaine central qui clarifie le mandat ainsi que la position de l'audit interne au sein de l'organisation. Notamment

en rappelant l'importance du soutien du comité d'audit et du conseil d'administration mais aussi la nécessité absolue d'une indépendance opérationnelle.

- Domaine IV – Gestion de la fonction d'audit interne, qui expose les exigences en matière de gestion des ressources, de supervision des missions et de mesure de la performance de la fonction.
- Domaine V – Réalisation des activités d'audit interne, détaillant les processus concrets de conduite des missions d'audit, depuis la planification jusqu'au suivi des plans d'action

Figure 6 : Nouvelles normes d'audit interne 2024 (Source : IFACI Certification – Benoit Harel, 2025)

Cette nouvelle structuration rend le référentiel plus lisible et plus cohérent avec la réalité opérationnelle en proposant une adaptation aux enjeux actuels des organisations. Elle permet et donne la possibilité aux fonctions d'audit interne d'assurer un haut niveau de performance. Elle donne aussi les moyens de renforcer leur rôle stratégique et leur capacité à influencer positivement la gouvernance.

Un élément fondamental de cette nouvelle version réside dans le Domaine III : "Gouvernance", qui réaffirme la place centrale de l'audit interne au sein de l'architecture de gouvernance de l'entreprise. Ce domaine ne se contente pas de rappeler les liens entre l'audit interne et les organes décisionnels mais insiste sur l'approbation et la capacité de la fonction à influencer les

décisions en matière de gestion des risques, de part notamment son rôle d'atténuation. Cette approche complète et plus ambitieuse qu'auparavant du rôle de l'audit interne renforce ce que nous avons déjà mentionné plus tôt dans cette thèse professionnelle : à savoir que l'audit interne n'est plus un simple observateur ou évaluateur mais un véritable partenaire stratégique du comité d'audit et du conseil d'administration.

En lien avec ce qui a été développé précédemment, le référentiel précise également que cette proximité avec la gouvernance ne peut produire de valeur que si l'indépendance de la fonction est garantie et si les résultats produits sont jugés utiles. Cela rejoint la logique selon laquelle la légitimité de l'audit interne repose aujourd'hui autant sur sa compétence technique que sur sa capacité à se positionner comme acteur de gouvernance, notamment sur des sujets critiques comme le nôtre ; la cybersécurité.

Le RPAI 2025 pousse également les fonctions d'audit interne à s'adapter aux nouveaux enjeux technologiques et à adopter une posture plus agile et davantage tournée vers l'accompagnement du changement des organisations. Il promeut une approche plus fluide entre les lignes de défense (opérationnelle, contrôle interne et audit interne) et invite l'audit interne à jouer un rôle de facilitateur entre ces acteurs du contrôle, dans un environnement où les frontières entre les fonctions mitigeant le risque ; conformité, éthique et gestion des risques deviennent de plus en plus perméables. En résumé, le nouveau référentiel consacre l'audit interne comme acteur intégré et stratégique de la gouvernance. Il redéfinit ses missions à travers une grille plus lisible et plus orientée vers la valeur et la performance. Cette mise à jour permet aussi d'être plus en phase avec les défis numériques actuels et de donner les armes aux auditeurs pour renforcer leur professionnalisme. Ce cadre constitue donc un socle essentiel pour légitimer l'intervention de l'audit sur des enjeux complexes et transverses.

Parmi les principaux référentiels utilisés en audit interne, le COSO (Committee of Sponsoring Organizations of the Treadway Commission) est créatrice de cadres incontournables. COSO est une commission américaine indépendante créée en 1985 par James Treadway (ancien commissaire de la Security and Exchange Commission) avec pour objectif d'analyser les causes des fraudes financières pour les entreprises cotées et de proposer des solutions concrètes en termes de gouvernance et de transparence. Avec le soutien d'autres organisations professionnelles, dont l'IIA, l'objectif était d'élaborer un cadre de référence commun. Cela a donné naissance au COSO 1 de 1992 sur le contrôle interne, revisité par la suite en 2013.

Concernant le management des risques, le COSO ERM (Enterprise Risk Management) a été créé en 2004 dans sa première version. Néanmoins le COSO ERM dans sa version de 2017 constitue un plus cadre actuel pour les entreprises. En effet, il s'agit d'une évolution importante par rapport à la première version publiée de 2004, dans la mesure où le référentiel ne se limite plus à une approche strictement défensive de la gestion des risques. Le COSO ERM 2017 propose une vision plus globale dans laquelle le risque n'est plus seulement perçu comme une menace à éviter mais plutôt comme un élément stratégique à piloter pour créer de la valeur à long terme. Ce cadre met notamment l'accent sur le lien entre gestion des risques et stratégie de l'entreprise. Notamment en considérant que les dispositifs de maîtrise des risques doivent être intégrés dès la définition des objectifs et non uniquement dans leur mise en œuvre. Cela permet d'ancrer les pratiques de contrôle dans une logique de performance durable en renforçant le lien direct avec la création de valeur pour l'organisation.

Le modèle s'articule autour de cinq grandes composantes, structurant la manière dont l'organisation gère ses risques :

- Gouvernance et culture : ce pilier englobe les mécanismes de gouvernance, les valeurs partagées ainsi que la manière dont la culture d'entreprise influence la gestion des risques.
- Stratégie et définition des objectifs : le référentiel insiste sur la nécessité de prendre en compte les risques dès la phase de définition des objectifs stratégiques.
- Performance : il s'agit d'évaluer comment les risques identifiés au sein de l'organisation peuvent influencer les résultats de l'organisation et comment ces risques sont suivis au fil du temps.
- Revue et amendement : le modèle invite à intégrer une logique d'ajustement et d'apprentissage à partir des retours d'expérience.
- Information, communication et reporting : ce pilier concerne la qualité et la circulation de l'information liée aux risques dans l'ensemble de l'organisation.

Figure 7: Composantes du COSO ERM 2017 (Source: COSO, 2017)

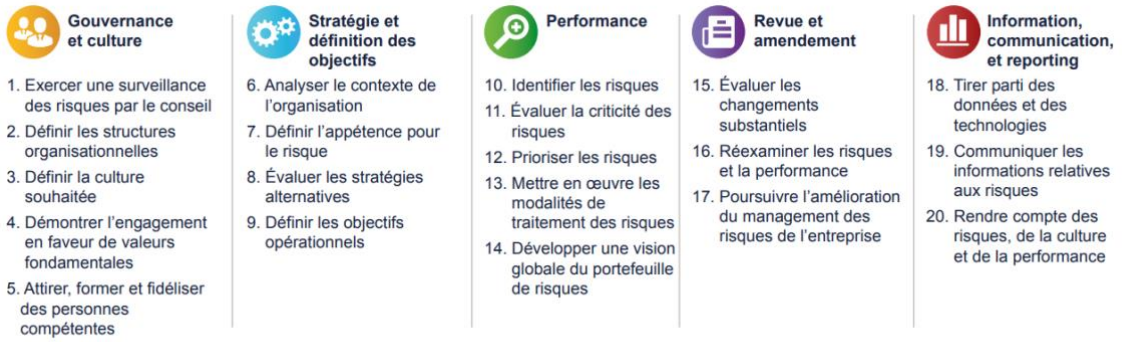


Figure 8 : Détail des Composantes du COSO ERM 2017 (Source : COSO, 2017)

L'un des atouts du COSO ERM 2017 réside en effet dans sa flexibilité. Il peut être appliqué aussi bien dans des grandes entreprises que dans des structures plus petites mais et surtout est adaptable à n'importe quels secteurs d'activité. Cela en fait un outil solide pour la fonction d'audit interne, qui peut s'en servir pour évaluer de manière structurée la maturité du dispositif de gestion des risques de son organisation.

Le référentiel COBIT (Control Objectives for Information and Related Technology), dans sa version la plus récente de 2019, est un cadre de gouvernance des systèmes d'information développé par l'ISACA (Information Systems Audit and Control Association) très utilisé par les auditeurs. COBIT a été développé à la base dès 1996 par l'ISACA pour répondre aux besoins des auditeurs d'avoir un cadre de bonnes pratiques, notamment pour évaluer le contrôle interne en termes de technologies de l'information. Il est utilisé lorsque les enjeux IT sont au

cœur des activités de l'entreprise comme notamment la cybersécurité. Après plusieurs modifications, le COBIT 2019 a vu le jour et reste le référentiel le mieux à jour actuellement. Le COBIT 2019 repose donc sur une logique d'alignement stratégique entre les objectifs métiers et les technologies mises en place pour les atteindre. Il ne s'agit pas uniquement d'un outil technique mais bien d'un cadre de référence qui permet de mettre en lien la performance des systèmes d'information avec la performance globale de l'organisation. Cela le rend particulièrement utile pour l'auditeur interne car il voit sa fonction transformée par la nécessité d'évaluer des dispositifs complexes liés à la cybersécurité ou à la gouvernance digitale. Ce référentiel permet aussi de structurer les missions d'audit en s'appuyant sur des domaines de gouvernance clairs comportant des processus précis à évaluer comme planification stratégique IT, gestion de la performance technologique, gestion des risques informatiques, respect des exigences réglementaires numériques etc. En offrant une grille d'analyse standardisé, il facilite aussi la comparabilité des évaluations entre différentes entités ou au fil du temps. Cette comparabilité peut aussi faciliter le travail de l'auditeur qui est amené dans sa carrière à souvent changer d'entreprise, lui permettant donc d'appliquer et de comparer les résultats d'évaluations entre ses deux structures.

L'intérêt du COBIT réside aussi dans sa capacité à intégrer toutes les parties prenantes de l'organisation. Il prend en compte les rôles et responsabilités de chacun dans la gestion de la performance IT. Le COBIT apporte une distinction entre les fonctions de pilotage et d'exécution au sein d'une organisation. Cela permet notamment à l'auditeur de mieux comprendre les interactions entre les métiers que ce soit la DSI (Direction des Systèmes d'Information), la direction générale ou autres les fonctions support. En pratique, cela facilite aussi les échanges avec les CISO (Chief Information Security Officer) et les équipes techniques en s'appuyant sur un vocabulaire commun. Enfin, ce référentiel intègre une dimension d'adaptation contextuelle avec un système de notation de la maturité des processus (de 0 à 5) qui permet d'aider l'auditeur à formuler des recommandations en lien avec le niveau de maturité réel de l'organisation. Cela permet notamment d'éviter les recommandations trop théoriques ou déconnectées des réalités opérationnelles des organisations. Ces recommandations peuvent aussi facilement être reliés à une criticité de risque en fonction de la notation, renforçant encore plus le lien avec la gestion des risques.

Aussi, le rapport Internal Audit Key Focus Areas 2025 (KPMG, 2024) insiste également sur la nécessité pour les fonctions d'audit de revisiter régulièrement leur méthodologie, afin de s'adapter aux mutations de l'environnement externe. Dans notre cadre, cela suppose de passer d'un audit purement rétrospectif à un audit prédictif, fondé sur la data en incluant les aspects IT et cybersécurité de l'entreprise. Mais cette transformation dans les organisations doit être impulsée par les personnes dirigeantes (top management), qui est le seul à pouvoir modifier pleinement la fonction de fonctionner de ses équipes. Parfois, ce dernier fait face à d'importants défis technologiques, couplés à une certaine réticence au changement de la part des auditeurs eux-mêmes.

C- L'évolution des missions de l'audit interne face aux défis technologiques

Comme évoqué plus tôt, la transformation numérique a profondément modifié le périmètre et les méthodes de l'audit interne. L'essor de la digitalisation et de l'explosion de la masse de données (big data), couplé à la montée des risques cyber conduisent à une reconfiguration de certains aspects de la fonction. En effet, le rapport "Risk in Focus 2025" (European Confederation of Institutes of Internal Auditing, 2024) indique que 82 % des responsables d'audit internes interrogés, classent la cybersécurité et la résilience technologique comme leur priorité numéro un. Ce chiffre reflète une prise de conscience généralisée du caractère stratégique et critiques de ces risques. En 2020, dans le rapport "Risk in focus 2020", (European Confederation of Institutes of Internal Auditing, 2019), ce risque était évalué à 78%. La fonction d'audit interne est donc amenée à intégrer ces nouvelles thématiques dans son champ d'intervention : sécurité des systèmes d'information, conformité au RGPD (pour les entreprises opérant au sein de l'Union Européenne), gouvernance des données, continuité d'activité, risques liés aux fournisseurs cloud etc.

Ces enjeux exigent une double compétence de la part des auditeurs : maîtrise des référentiels technologiques et compréhension des processus métiers. Dès lors, l'auditeur ne peut plus se contenter d'une analyse documentaire ou d'entretiens avec les opérationnels. Il doit s'outiller, se former et parfois s'appuyer sur des experts techniques pour auditer efficacement un environnement numérique complexe. En effet, les directions d'audit interne n'hésitent pas à recruter un externe pour une mission spécifique hors de leur champ de compétence actuel (pour RGPD par exemple). Le rapport de Deloitte "Cybersecurity and the Role of Internal Audit"

datant de 2017, souligne d'ailleurs la nécessité pour les auditeurs d'adopter des approches multidisciplinaires. Ces approches doivent combiner des compétences en cybersécurité, en analyse de données et donc aussi en management des risques. Cette évolution conduit également à revoir les plans d'audit : on passe d'une planification annuelle figée à des approches dynamiques et agiles. Les plans d'audit doivent être adaptables pour être capables de réagir aux incidents opérationnels ou aux évolutions réglementaires en temps réel. Dans les organisations les plus matures, l'audit interne contribue aussi à évaluer les projets de transformation digitale en amont (audit de cybersécurité sur une nouvelle infrastructure cloud ou au développement d'un nouvel outil digital). Ce positionnement préventif et non plus correctif permet de réduire les potentiels coûts de non-qualité et d'assurer une intégration sécurisée des technologies dans les processus métiers. C'est aussi dans ce contexte que le rapport de Jamison, Morris & Wilkinson (2018) recommande explicitement la mise en place de binômes composés d'un auditeur interne et d'un expert IT, permettant en théorie de renforcer la capacité des équipes à appréhender ces enjeux techniques. Ce modèle de binôme présente en effet plusieurs avantages. Il permet de combiner les compétences méthodologiques et analytiques de l'auditeur, avec la maîtrise technique approfondie de l'environnement audité apportée par l'expert IT. Ensemble, ils peuvent élaborer un plan de mission plus précis pour identifier les failles techniques potentielles mais aussi mieux évaluer la qualité des dispositifs en place. Ce travail en duo facilite également la compréhension mutuelle entre les équipes d'audit et les services informatiques internes, qui est souvent marquée par une distance opérationnelle liée au langage. Ce fonctionnement en binôme ne doit néanmoins pas impliquer une dilution du rôle de l'auditeur mais bien un renforcement de sa capacité à traiter des sujets hautement techniques.

D- Limitations et défis actuels de l'audit interne dans un environnement numérique

Malgré cette montée en puissance sur les aspects numériques, l'audit interne fait face à plusieurs limites structurelles. La première d'entre elles concerne la complexité croissante des systèmes d'information audités. Les systèmes d'information sont d'ailleurs tous interconnectés entre eux, ce qui contribue à renforcer la difficulté de compréhension pour quelqu'un de non-expert. Dans de nombreuses entreprises, ces systèmes sont mutualisés entre plusieurs entités du groupe, voir même externalisés partiellement à des prestataires. Cela complexifie donc la

visibilité que peut avoir l'auditeur sur la chaîne complète d'information. De plus, les compétences spécialisées manquent parfois en interne, d'où la pertinence des binômes avec des experts IT. Comme le met en lumière le rapport "The Future of Cybersecurity in Internal Audit" (Crowe & IIA, 2018), les directions d'audit peinent à recruter des profils disposant d'une double expertise technique et audit. Mais le recours à des experts IT externes ou même internes n'est aussi pas toujours possible pour des raisons financières ou de culture d'entreprise. Il est donc nécessaire que les auditeurs internes possèdent aussi ces compétences et que la formation des auditeurs évolue vers cela.

Un autre défi pour l'audit interne concerne la gestion des données personnelles et sensibles, particulièrement dans un contexte post-RGPD. Depuis l'entrée en application du Règlement Général sur la Protection des Données en mai 2018, les entreprises évoluant dans l'UE sont soumises à des obligations strictes en matière de données à caractères personnelles de leurs parties prenantes. La fonction d'audit interne est donc souvent confrontée à ces problématiques liées à l'accès et à la sécurisation des données contenant des informations personnelles. Cela rend donc indispensable la coordination entre l'audit interne et la Délégation à la Protection des Données (DPO), comme le suggère le guide pratique du RGPD de L. Ligaudan (2024). L'auditeur doit être formé aux obligations légales en matière de traitement des données, notamment dans des secteurs qui récupèrent beaucoup de données clients comme le retail ou le bancaire par exemple.

De plus, l'intégration de l'audit interne dans les processus de transformation pose également question. Comme expliqué plus tôt, les auditeurs interviennent le plus souvent en bout de chaîne dans une logique d'évaluation a posteriori. Or, pour jouer pleinement son rôle stratégique, la fonction devrait être mobilisée en amont. Dès la conception des projets, l'audit interne doit avoir un rôle clé à jouer pour anticiper les zones de risques et apporter son expertise dans leur atténuation. Le rapport KPMG "Internal Audit: Key Focus Areas 2025" (2024) insiste sur ce point en indiquant que l'audit interne doit évoluer vers un modèle plus "project-based" (basé sur des projets) et "embedded" (incorporé), permettant à ce que sa valeur ajoutée pour l'organisation repose autant sur sa capacité d'alerte que sur son rôle de conseil. Le rapport recommande notamment que les directions d'audit soient associées dès les comités de pilotage de projet. C'est donc un défi stratégique pour la profession car il questionne directement son

positionnement. L'audit interne doit réussir à démontrer sa valeur ajoutée en amont des projets pour rester pleinement aligné avec les enjeux de transformation digitale des organisations.

E- L'importance croissante des outils analytiques pour l'analyse des données d'audit

L'un des leviers les plus puissants pour dépasser les limitations de l'audit interne réside dans l'adoption d'outils analytiques. L'usage des données et des technologies permet d'une part de gagner en efficacité et l'autre d'aussi d'améliorer la précision des analyses. Les outils d'audit analytics permettent donc de collecter et analyser des volumes de données importants. Grâce à ces derniers, les auditeurs peuvent détecter des anomalies ainsi que des tendances pouvant guider leurs travaux. Selon le rapport de Grant Thornton & Dauphine PSL (2023), 67 % des départements d'audit en Europe ont commencé à utiliser des outils analytiques pour renforcer leurs missions. Ces outils, peuvent être classés en deux grandes catégories. Dans un premier temps, les outils dits "techniques d'audit assistées par ordinateur" (TAAOs) ou Computer-aided audit tools, CAATs en anglais. Ces outils sont traditionnellement utilisés par les Commissaires aux Comptes (CAC) pour analyser les données financières des entreprises mais sont aussi de plus en plus généralisés dans les directions d'audit interne. Ils sont conçus pour permettre aux auditeurs de détecter les anomalies, de tester des contrôles ou encore d'identifier des fraudes. La force de ces outils réside aussi dans le fait qu'ils puissent traiter des quantités de données très importantes en appliquant des règles de contrôles complexes (doublons, seuils, écarts etc.). Parmi ces TAAOs très utilisés, on peut notamment citer ACL (Audit Command Language) ou encore IDEA, développé par l'entreprise américaine Caseware. Dans un second temps, les autres outils très utilisés par les auditeurs sont des outils dits de "data visualisation" (visualisation de données). Ces outils permettent de créer des visualisations graphiques dynamiques pour suivre des KPIs grâce à une connexion directe avec les bases de données des entreprises. Cela permet aux auditeurs de dépasser le cadre manuel de suivis des KPIs pour avoir un contrôle continu sur les données clefs. Parmi ces outils, les plus utilisés sont PowerBi et Tableau mais de nombreux autres existent, pouvant s'adapter aux besoins de chaque utilisateur. Néanmoins, il convient de nuancer que l'utilisation de ce genre d'outils informatiques ne se limite pas qu'à l'audit interne, de nombreuses fonctions des entreprises les utilisent au quotidien afin de visualiser les données souhaitées en temps réel.

Ce type d'audit, "data-driven audit" (basé sur les données) transforme donc profondément la manière de conduire les missions. Il permet de passer d'un audit par échantillonnage à un audit exhaustif, où par exemple, l'ensemble des transactions peut être analysé. Cette capacité peut aussi changer radicalement le niveau d'assurance apporté par la fonction d'audit car elle permet d'avoir des audits plus exhaustifs et précis. Grâce à ces techniques, la fonction peut enfin renforcer sa gestion des risques et son pouvoir d'atténuation.

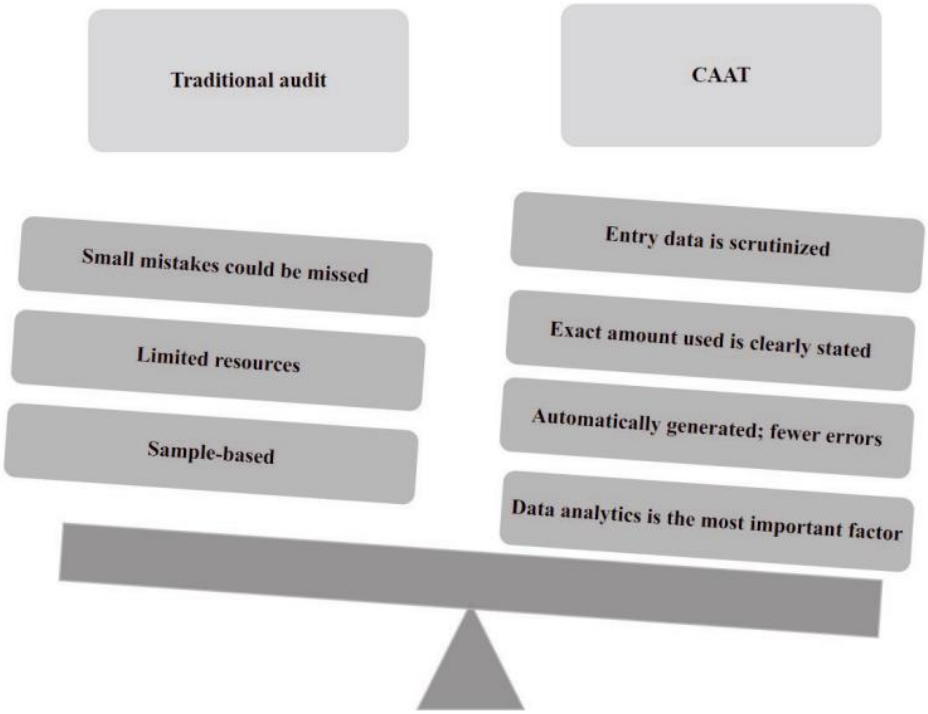


Figure 9 : Audit traditionnel vs audit TAAOs (Source : Fülöp, M 2024)

L'intelligence artificielle (IA) est aussi en train de transformer la profession d'audit interne. En effet, l'IA permet aux auditeurs de traiter un très gros volume de données et de détecter plus facilement des anomalies significatives, avec encore plus d'efficacité que les outils cités précédemment. Grâce à ces nouvelles technologies, les auditeurs possèdent une nouvelle arme performante pour réaliser leurs missions. Par ailleurs, les nouvelles normes d'audit interne de 2024 abordent aussi ce sujet dans la norme 10.3 « Ressources technologiques ».

Cette norme explique très clairement que pour améliorer l'efficacité et l'efficience de son département, le DAI doit recourir à des technologies permettant l'aide au traitement de la donnée pour les auditeurs mais aussi à la visualisation de données.

En effet, cette dimension est évoquée à plusieurs niveaux : celui des compétences des auditeurs internes, du plan d'audit interne, mais aussi au niveau des ressources. Par exemple, la Norme 10.1 demande à ce que les auditeurs internes disposent bien des moyens pour se former et pour acquérir les bons outils technologiques, afin de rendre les services définis dans leur mandat. Il est indiqué que le directeur de l'audit interne doit évaluer régulièrement la technologie utilisée et réfléchir à la façon d'améliorer encore son efficacité, en collaborant notamment avec les responsables des systèmes d'information. Enfin, concernant la technologie, les risques technologiques et organisationnels sont en plein cœur du métier d'auditeur interne. Nous les aborderons dans la partie suivante.

1.3- Vers une gestion intégrée des risques technologiques et organisationnels

Dans cette partie, nous allons définir les nouveaux défis liés aux risques organisationnels dans le monde connecté que nous connaissons. Ensuite, nous évoquerons l'impact de la digitalisation sur les méthodes de gestion des risques, l'importance d'une approche intégrée combinant audit interne et cybersécurité et enfin les perspectives et recommandations pour une gestion des risques efficace.

A- Les nouveaux défis liés aux risques organisationnels dans un monde connecté

Dans un monde où les systèmes sont de plus en plus interconnectés entre eux, les risques organisationnels ne peuvent plus être abordés isolément. L'entreprise ne dépend plus uniquement de ses propres ressources mais aussi de l'ensemble de ses parties prenantes.

Le rapport Risk in Focus 2025 (ECIIA, 2024) nous rappelle que la dépendance accrue à ces tiers numériques constitue un facteur critique de vulnérabilité. Aujourd'hui, une cyberattaque sur un sous-traitant peut avoir des conséquences directes et sévères sur l'entreprise cliente. Ces risques dit de quatrième partie sont d'autant plus préoccupants qu'ils sont difficilement maîtrisables par l'entreprise.

Cette interdépendance rend les chaînes de valeur plus fragile. Selon Clapaud (2024), les attaques sur les chaînes logistiques numériques ont explosé ces dernières années et les dispositifs de sécurité ne sont pas harmonisés entre les différents acteurs d'un même réseau. Le rapport Risk in Focus 2025 (ECIIA, 2024) pointe également l'importance des chaînes de

logistique dans leur préoccupation ; cet élément fait partie du top 10 de leur préoccupation du moment. Une gouvernance fragmentée accroît donc la surface d'attaque. Cela pousse les fonctions d'audit et de contrôle interne à revoir leurs méthodes de surveillance et à intégrer une logique de cartographie des dépendances critiques.

Par ailleurs, les risques non technologiques évoluent eux aussi. On observe une montée des risques liés à la réputation, ou encore à la conformité. Dernièrement, le cas de l'entreprise Naval Groupe est un bon exemple de risque réputationnel comme évoqué plus tôt. L'entreprise Orange a également subi une cyberattaque le 25 juillet 2025 sur un de ses systèmes d'information. Ces attaques n'ont pour le moment pas de réelle influence sur la vie des clients, car nous n'avons pas assez de recul sur ce qui s'est passé et les données qui pourraient avoir été exfiltrées. Néanmoins, la perception d'une crise peut devenir un risque en soi, indépendamment de son impact technique réel. Une mauvaise gestion de crise, une réaction tardive face à un incident cyber ou encore une communication maladroite pourraient amplifier les conséquences d'un événement en altérant la confiance des parties prenantes.

Ces risques dits « immatériels » deviennent centraux dans un monde où l'information circule très vite. Selon Jamison et al. (2018), la fonction d'audit interne doit renforcer ses capacités d'analyse sur ces sujets en combinant des indicateurs techniques avec des facteurs humains et organisationnels. Le facteur humain reste l'un des maillons les plus vulnérables d'un dispositif de sécurité. Des négligences ainsi que des comportements à risque peuvent anéantir des investissements importants en cybersécurité. Le modèle des trois lignes (IIA, 2020) insiste sur la nécessité de clarifier les rôles entre opérationnels, fonctions de surveillance et audit, dans un contexte de transformation numérique.

Dans ce contexte, les modèles traditionnels de gestion des risques atteignent leurs limites. Le COSO ERM (2017) souligne la nécessité de passer d'une approche compartimentée à une gouvernance des risques intégrée et alignée avec la stratégie globale de l'entreprise. Il ne s'agit plus de cartographier les risques métier mais bien d'adopter une approche interfonctionnelle et dynamique.

B- L’impact de la digitalisation sur les méthodes de gestion des risques

La transformation digitale a profondément modifié la manière dont les organisations perçoivent, analysent et enfin traitent les risques. L’adoption généralisée de solutions numériques, la migration vers le cloud et aussi l’introduction de l’utilisation de l’IA dans ces dernières bouleversent les référentiels de contrôle classiques. Ces nouvelles habitudes de travail forcent les entreprises à repenser leurs approches du risque. Les outils numériques génèrent des volumes de données de plus en plus importants, permettant en théorie, une détection plus rapide des signaux critiques faibles. Néanmoins, cette abondance d’informations suppose aussi de nouveaux savoir-faire pour les analyser de manière pertinente. Selon Dauphine PSL et Grant Thornton (2023), l’analyse avancée des données devient un levier central pour améliorer la pertinence des évaluations de risques, notamment dans le cadre des missions d’audit interne.

Le rapport de KPMG sur les thèmes clés à considérer en 2025 montre que la digitalisation oblige les fonctions de contrôle à évoluer. Les méthodes traditionnelles d’échantillonnage cèdent progressivement la place à des analyses en continu grâce à des solutions d’audit automatisé mais aussi à des techniques de data analyse. Ces techniques permettent d’identifier des anomalies ou des comportements inhabituels en temps réel et offre une capacité de réaction beaucoup plus rapide qu’avec les dispositifs traditionnels.

Mais la digitalisation a aussi un effet paradoxal : elle complexifie les risques. Des environnements hybrides (cloud, logiciels interconnectés, applications métier) rendent les frontières floues entre les différents types de menaces : technologiques, humaines ou réglementaires. Comme le souligne Bubilek dans « Importance of Internal Audit and Internal Control in an organization » (2017), le rôle de l’audit interne se transforme donc : il ne s’agit plus uniquement de contrôler les processus existants mais en effet de comprendre et d’anticiper les dynamiques de risque dans un environnement mouvant. L’auditeur devient alors un chef d’orchestre, capable de naviguer dans cette complexité pour faire dialoguer les différentes lignes de défense.

La cybersécurité est emblématique de cette complexité. Selon Clapaud (2024), chaque brique technologique intégrée dans le système d’information d’une entreprise introduit un risque potentiel qui peut évidemment se propager très rapidement. Les référentiels comme COBIT 2019 ou le COSO ERM 2017 recommandent dès lors de rapprocher les démarches IT et les

démarches de gouvernance des risques, afin d'éviter les silos organisationnels et de favoriser une surveillance cohérente et continue.

Le COSO ERM recommande l'adoption d'une logique de cycle de vie du risque, tout en intégrant les risques émergeants issus du digital dès les phases de conception des projets. Quant au COBIT 2019, ce référentiel met en avant la gouvernance IT qui s'aligne sur la création de valeur et la réduction des risques en intégrant les enjeux de confidentialité, de résilience numérique ou encore de conformité.

C- L'importance d'une approche intégrée combinant audit interne et cybersécurité

Dans ce nouveau contexte marqué par la complexification des systèmes d'information et l'intensification des menaces numériques, l'approche intégrée de la gestion des risques devient incontournable. Il ne s'agit plus de traiter la cybersécurité comme un domaine purement technique mais plutôt de bien l'inscrire dans une logique de gouvernance globale, partagée entre les fonctions métiers, IT et de contrôle interne.

Selon l'étude de Grant Thornton et Dauphine PSL, « Quelle est la place de l'Intelligence Artificielle dans les pratiques d'audit interne ? » de 2023, l'intelligence artificielle et les technologies d'automatisation doivent être vues comme des catalyseurs d'une meilleure anticipation des risques. Elles permettent à l'audit interne de cibler plus précisément les zones à risque, d'exploiter des techniques d'analyse prédictive ainsi que de mettre en œuvre des dispositifs de surveillance continue. Cependant, cette évolution nécessite une collaboration plus soutenue entre les équipes informatiques et les équipes gestionnaires du risques (3 lignes de défenses).

L'approche collaborative est également mise en avant par le référentiel professionnel de l'audit interne de l'IFACI (2025), qui insiste sur la fin du cloisonnement entre les fonctions de contrôle. Il recommande que les missions d'audit intègrent systématiquement des volets liés à la cybersécurité et cela même lorsque celle-ci ne semble pas être le sujet principal. En parallèle, les nouvelles normes internationales de l'IIA (2024) redéfinissent les attentes vis-à-vis des auditeurs. En effet, ceux-ci doivent désormais posséder une compréhension suffisante des risques numériques et les comités d'audit doivent également être sensibilisés à ces enjeux technologiques.

Le modèle des trois lignes de défense (2020) prend toute sa pertinence dans ce contexte. Il souligne que la sécurité numérique ne peut plus être uniquement portée par la ligne IT (ligne 1) mais doit aussi être coordonnée avec les fonctions de gestion des risques (ligne 2) et d'audit interne (ligne 3). Ce modèle, mis à jour, décrit une évolution importante dans la répartition des responsabilités où chaque acteur de la chaîne de valeur de l'organisation doit contribuer à la résilience numérique.

De son côté, le cabinet Deloitte (2024) rappelle que l'audit interne doit jouer un rôle actif dans la réponse aux cybermenaces en apportant aux autres parties prenantes une perspective indépendante sur les vulnérabilités critiques. Mais aussi en évaluant la maturité des contrôles en place et enfin en facilitant le dialogue entre la direction générale et les équipes opérationnelles. Cette posture proactive constitue selon eux un impératif stratégique dans un environnement en constante mutation.

L'émergence de nouvelles obligations réglementaires renforce encore cette dynamique intégrée. Par exemple, Bon-Michel et Cappelletti soulignent (2025) que la directive européenne CSRD (Corporate Sustainability Reporting Directive) introduit une approche étendue de la responsabilité des entreprises. Au-delà des aspects environnementaux et sociaux, les organisations devront démontrer comment elles protègent leurs données, leurs actifs numériques ainsi que leurs infrastructures critiques. Ces exigences appellent une gestion transversale des risques, incluant les dimensions techniques, humaines et bien sûr réglementaires du risque cyber.

Par ailleurs, les travaux d'Alem et Ben Zekri (2019) rappellent que les technologies de l'information, lorsqu'elles sont bien intégrées au contrôle interne, permettent une meilleure détection de la fraude. Notamment par le croisement automatisé d'informations et la détection d'anomalies comportementales. Cette dimension est particulièrement pertinente dans la lutte contre les cyberattaques internes qui sont souvent liées à des failles humaines ou organisationnelles.

D- Perspectives et recommandations pour une gestion des risques efficace

Pour répondre aux défis croissants liés à la transformation numérique, aux cybermenaces persistantes et aux exigences réglementaires en constante évolution, les entreprises doivent

adopter une gouvernance des risques agile et résiliente. Cette gouvernance ne peut reposer uniquement sur des dispositifs techniques ou sur des procédures figées : elle doit refléter une vision systémique, où les fonctions d'audit, de cybersécurité, de contrôle interne et de gestion des risques travaillent en synergie.

Les recommandations suivantes s'imposent progressivement comme des leviers stratégiques de cette transformation :

- Créer des synergies durables entre audit interne, cybersécurité et gestion des risques, en favorisant les échanges d'information, les comités conjoints et la mutualisation des outils.
- Investir dans les compétences, en formant les auditeurs aux enjeux numériques et les experts IT aux principes de gouvernance des risques.
- Renforcer la culture du risque, en sensibilisant l'ensemble des collaborateurs à leur rôle dans la protection du système d'information.
- Utiliser les référentiels existants, comme COBIT, COSO ou l'ISO 27001, pour structurer la démarche et assurer une couverture complète des risques.
- Intégrer l'innovation dans la gestion des risques, en expérimentant des outils d'IA ou de surveillance en continu, tout en gardant un regard critique sur leurs limites.

En conclusion, la cybersécurité est un élément complexe à comprendre et à mettre en place. Des standards ont été publiés afin de permettre une organisation des entreprises autour des risques cyber. Les menaces auxquelles peuvent faire face les entreprises sont multiples ainsi que leurs impacts. Les entreprises se doivent de mettre en place une ou plusieurs stratégies cyber pour faire face à la digitalisation et à l'augmentation des risques technologiques.

L'audit interne a un rôle clé à jouer dans la réponse aux risques cyber. L'audit interne est également soumis à certaines normes et référentiels pour assurer un bon fonctionnement du service. Les normes de l'audit interne ont été actualisées en 2024, mises en application début 2025, afin de répondre à certaines interrogations, assurer une meilleure couverture des différentes structures et intégrer les technologies qui font aujourd'hui partie de notre quotidien.

Enfin, la gestion des risques du XXIe siècle ne peut plus être fragmentée. Elle doit refléter l'interconnexion croissante entre les dimensions techniques, humaines, organisationnelles mais aussi réglementaires. L'efficacité doit passer par une vision stratégique de long terme, intégrée

dans la culture d’entreprise et doit être soutenue par des référentiels solides ainsi qu’être alimentée par des compétences transversales. Les entreprises les plus résilientes seront celles qui sauront transformer la complexité numérique en avantage concurrentiel grâce à une gouvernance des risques modernisée, fluide et collaborative.

II- Méthodologie

2.1- Choix de l'approche qualitative

Dans le cadre de cette thèse professionnelle, nous avons choisi de mobiliser une approche qualitative afin de mieux comprendre les dynamiques à l'intersection de la cybersécurité et de l'audit interne. Ce choix repose avant tout sur la volonté d'explorer des perceptions, des pratiques mais aussi des représentations propres aux professionnels évoluant dans ces domaines spécifiques. La cybersécurité, tout comme l'audit interne, implique des réalités organisationnelles complexes. Une approche quantitative ne nous aurait pas permis d'avoir autant de détails dans les réponses et une difficulté supplémentaire d'adapter les questions à un plus grand public. En effet, les enjeux ne résident pas seulement dans les dispositifs techniques ou les indicateurs de conformité mais aussi dans la manière dont les acteurs perçoivent les risques. La prise en compte de leurs décisions, les interactions avec leurs services ou le développement d'une culture d'entreprise en lien avec le cyber, n'auraient pas été analysables avec une méthodologie quantitative. Enfin, le côté très actuel du sujet cyber fait qu'une analyse quantitative n'aurait pas été pertinente, étant donné le manque de recul sur le sujet et le manque de données, ce sujet étant très confidentiel pour les organisations.

L'approche qualitative nous permet donc de donner la parole aux professionnels en leur offrant l'espace nécessaire pour exprimer leur vision. Cette approche permet aussi de comprendre leurs contraintes et la réalité du terrain face à la théorie. Elle s'avère particulièrement pertinente dans un cadre professionnel dans lequel les pratiques réelles peuvent parfois diverger des politiques formelles ou encore des cadres normatifs. Les témoignages recueillis permettent d'ancrer l'analyse dans des situations concrètes, en tenant compte de la diversité des contextes (secteur d'activité, niveau de maturité cyber et taille de l'entreprise).

Par ailleurs, les domaines de la cybersécurité et de l'audit interne sont aujourd'hui principalement développés dans les grandes organisations, qui disposent des ressources humaines ainsi que techniques nécessaires pour structurer ces fonctions. Dans ce contexte, l'approche qualitative s'impose encore une fois comme une méthode adaptée pour accéder à des retours d'expérience riches issus de professionnels occupant des fonctions clés que nous avons interrogés (RSSI, auditeurs internes, DPO, CISO).

En somme, cette démarche vise à comprendre le vécu des acteurs et à identifier les leviers et freins à l'intégration de la cybersécurité dans les pratiques de gestion des risques, en particulier dans le cadre des missions d'audit interne. Elle constitue une étape essentielle pour dégager des recommandations cohérentes avec la réalité du terrain.

2.2 – Stratégie d'échantillonnage

Dans le prolongement de notre approche qualitative, nous avons ciblé des profils directement impliqués dans la gestion des risques organisationnels et technologiques, afin de recueillir des témoignages à forte valeur ajoutée. Les personnes interviewées occupent des fonctions stratégiques telles qu'auditeur interne, responsable de la cybersécurité, CISO (Chief Information Security Officer), DPO (Data Protection Officer) ou encore responsable data. Ce choix s'explique par la complémentarité de leurs rôles dans la construction d'un cadre de gouvernance robuste autour des enjeux cyber et de contrôle interne.

L'objectif était de capter une pluralité de points de vue sur la manière dont la cybersécurité est intégrée aux dispositifs de gestion des risques et aux pratiques d'audit, tout en tenant compte des réalités propres à chaque organisation. Les échanges ont permis de mettre en lumière aussi bien des bonnes pratiques que des freins organisationnels ou encore des zones de tension entre exigences de sécurité, performance et conformité.

Pour garantir la richesse et la pertinence des retours, une attention particulière a été portée à la diversité des profils interviewés, tant en ce qui concerne le secteur d'activité, la taille des structures que leur niveau de maturité cyber. Ainsi, les entretiens ont été menés auprès de professionnels issus :

- D'un cabinet d'audit disposant d'une expertise avancée dans l'accompagnement des grandes organisations sur les enjeux cyber et IT ;
- D'une entreprise cotée au CAC 40 dans l'industrie du retail, reconnue pour la maturité de sa stratégie cybersécurité ;
- D'une grande entreprise internationale du secteur de l'hospitalité, également très avancée sur les sujets de sécurité numérique ;
- D'un groupe hôtelier de grande taille, présentant une maturité légèrement moins avancée mais disposant toutefois d'un socle solide en matière de cybersécurité.

- D’une entreprise d’agroalimentaire, leader dans le domaine du poisson et des crustacés. L’entreprise a une bonne maturité en ce qui concerne les risques cyber, mais ne considère pas que ce soit un risque majeur pour l’entreprise.

Cette hétérogénéité dans les profils a permis d’identifier des logiques d’organisation différentes et influencées par le contexte sectoriel et la taille des structures. Le contraste entre des acteurs très matures en cybersécurité et d’autres encore en phase d’évolution permet d’enrichir l’analyse et de mettre en évidence les facteurs de succès, les défis communs mais aussi les axes d’amélioration dans la collaboration entre fonctions audit et sécurité.

Finalement, cette diversité constitue une force pour cette étude, en assurant une représentativité qualitative des pratiques observées dans des environnements complexes et exigeants, tant en France qu’à l’international.

2.3 - Construction du guide d’entretien

Afin de répondre à la problématique de cette thèse professionnelle, un guide d’entretien semi-directif a été construit autour de quatre grands axes thématiques, directement issus de la revue de littérature : l’évolution des missions d’audit interne, l’intégration des outils et référentiels liés à la cybersécurité, la collaboration entre les fonctions clefs (Audit Interne, DSI, RSSI) et les compétences requises pour faire face aux nouveaux enjeux numériques. Le format semi-directif a été privilégié pour garantir une certaine souplesse dans les échanges, tout en assurant une cohérence dans les thématiques abordées auprès des différents profils interrogés. Cette approche permet également d’explorer les perceptions et pratiques professionnelles dans un cadre structuré mais non rigide, conforme aux recommandations méthodologiques en science de gestion.

Ce guide a été élaboré à partir d’axes identifiés dans la littérature récente, notamment les rapports de l’European Confederation of Institutes of Internal Auditing (ECIIA) (Risk in Focus 2024 et 2025), les publications de l’IFACI (Guide des risques cyber 2.0, 2020), ainsi que les orientations méthodologiques proposées par l’IIA dans les nouvelles normes d’audit interne 2024. Cette construction s’inscrit également dans les recommandations d’acteurs professionnels, qui soulignent aussi l’importance de croiser les points de vue opérationnels et stratégiques dans l’évaluation des dispositifs de sécurité. Ce guide a aussi été validé et testé par

un professionnel de l'audit interne, permettant d'ajuster la formulation de certaines questions et d'en améliorer la pertinence et la clarté. Il a aussi été validé par la responsable pédagogique d'un Master Spécialisé en audit interne d'une grande école de commerce parisienne.

Ce guide est donc structuré en trois blocs cohérents : une première série de questions vise à recueillir les perceptions générales sur l'évolution du risque cyber en entreprise et son impact sur les missions d'audit ; une seconde série, portant sur les pratiques concrètes, les outils utilisés et les points de frictions observés ; et un troisième et dernier axe orienté vers une réflexion prospective sur l'évolution de la fonction d'audit interne, en lien avec les compétences et l'intégration stratégique de la cybersécurité. Ce découpage méthodique permet une lecture progressive des enjeux, partant des constats de terrain pour aller vers une discussion plus analytique et détaillée. L'objectif est de rechercher de la cohérence avec l'approche qualitative retenue. Les entretiens sont menés auprès de huit professionnels : Directeur d'Audit Interne, RSSI, Responsables cyber, tous sélectionnés selon des critères de diversité énoncés auparavant (secteur d'activité, taille d'entreprise, niveau de maturité cyber). Les échanges se dérouleront en visioconférence ou en présentiel, pour une durée de 45 minutes à une heure et seront enregistrés avec l'accord des participants. Les questions abordent aussi bien les aspects organisationnels que techniques, en accord avec les recommandations de l'IIA. Cet organisation précise dans les nouvelles normes de 2024, que l'audit interne doit "contribuer à la réussite de l'organisation en soutenant la protection et la création de valeur dans un cadre de gouvernance, de gestion des risques et de contrôles" (IIA, 2024, p. 9).

Enfin, cette approche permet de confronter les attentes de la littérature aux réalités opérationnelles, en y intégrant les recommandations de rapports comme « Internal Audit Key Focus Area 2025 » (KPMG, 2024), qui appelle à une implication plus en amont de la fonction d'audit interne dans les projets technologiques. « The Future of Cybersecurity in Internal Audit » (Jamison, Morris et Wilkinson, 2018) insiste aussi sur l'importance du travail conjoint entre auditeurs et experts IT pour évaluer efficacement les nouveaux risques.

III- Discussion des résultats

3.1. Évolution de la cybersécurité

L'analyse des entretiens réalisés met en évidence une transformation profonde de la perception et du traitement du risque cyber au cours de la dernière décennie. Tous les professionnels interrogés, issus de secteurs aussi variés que l'agroalimentaire, la grande distribution, l'hôtellerie, les services IT ou encore le conseil, s'accordent sur un point central : la cybersécurité n'est plus un sujet périphérique réservé aux services techniques type DSI mais un enjeu majeur qui touche la continuité d'activité et la réputation. Concrètement, le risque cyber peut grandement impacter la continuité des activités d'une organisation et même parfois sa survie. Toutefois, cette évolution ne s'est pas opérée de manière homogène et son rythme dépend fortement du secteur. La culture managériale et du degré d'exposition aux menaces sont aussi évidemment des facteurs expliquant la façon dont les organisations ont muté face à la croissance de ces risques.

Dans certains secteurs, comme l'agroalimentaire, la cybersécurité a progressé mais reste considérée comme un risque secondaire face aux priorités traditionnelles. L'auditrice interne de Cité Marine l'explique clairement : pour cette entreprise industrielle, la priorité demeure la sécurité sanitaire et la qualité des produits. Selon elle, "une attaque pourrait perturber la production ou retarder les livraisons mais elle n'aurait pas le même impact structurel que dans d'autres secteurs fortement numérisés" (Entretien n°1). Les efforts en lien avec la cybersécurité se concentrent donc sur la mise à jour de l'ERP, l'installation de pare-feu, la protection contre le phishing ainsi que sur des campagnes de sensibilisation de base pour les collaborateurs de l'entreprise. La cybersécurité est perçue comme sérieuse mais toujours en arrière-plan par rapport à un risque sanitaire ou à un risque supply chain.

À l'inverse, dans des groupes fortement digitalisés comme des boîtes du CAC40, le risque cyber est devenu tellement central et stratégique qu'au fil des années il a été intégré au plan d'audit. Guillaume Litvak, Directeur exécutif de l'audit interne et des risques chez Carrefour, insiste sur cette montée en puissance : "le risque cyber n'a cessé de croître ces dernières années, jusqu'à devenir un axe incontournable du plan d'audit chez Carrefour" (Entretien n°2). L'entreprise a ainsi choisi de renforcer ses équipes en recrutant des experts à l'international (notamment André Antunes de la banque Carrefour au Brésil) pour bâtir un plan d'audit cyber

spécifique. Ce dernier repose sur l'identification de thématiques clés pour le Groupe et est voué à évolué au fil des identifications de nouveaux risques cyber. En effet chaque année, de nouvelles sous-thématiques sont intégrées en fonction de ces évolutions. Cette dynamique illustre bien que dans les grands groupes et notamment de retail, la cybersécurité est désormais pensée comme un sujet mouvant et doit être suivi et adapté en permanence.

Cette évolution tient aussi à la mutation des types d'attaques subies par les entreprises. Plusieurs interlocuteurs rappellent qu'il y a encore quelques années, les menaces principales concernaient des défaçages de sites internet ou des intrusions à finalité destructrice. Comme le note Guillaume Cécile, CISO du Groupe Carrefour : « il y a cinq ou six ans, les risques concernaient surtout le défaçage ou des intrusions destructrices. Aujourd'hui, l'extorsion de fonds et les attaques par ransomware représentent la menace principale » (Entretien n°5). Ces ransomwares ne visent plus seulement à bloquer les systèmes mais s'accompagnent le plus souvent d'une exfiltration massive de données, notamment des données clients. Ces dernières sont utilisées comme levier de chantage ou revendues au plus offrant sur des marchés parallèles comme le darknet. Cette logique est confirmée par les experts d'EY, Mathieu Gras et Nabil Babaci, qui constatent une tendance de fond : « le ransomware, autrefois perçu comme la menace majeure, tend à devenir secondaire : les attaquants privilégient désormais la revente de données » (Entretien n°7).

Derrière cette mutation se cache un phénomène plus global de professionnalisation et d'industrialisation du cybercrime, au même titre que d'autres activités criminelles. Les spécialistes interrogés évoquent une véritable « ubérisation du crime ». Aujourd'hui, des acteurs spécialisés échangent et coopèrent sur des messageries chiffrées, comme Telegram ou Signal, pour se répartir les tâches et maximiser les profits. De vraies équipes structurées se forment avec certains experts dans le vol de données, d'autres dans l'intrusion, d'autres encore dans la revente de ces données. Cette segmentation du travail criminel rappelle le fonctionnement des entreprises qui en sont victimes. Les entreprises doivent donc affronter des adversaires mieux structurés et plus outillés. En effet, leur capacité de frapper avec une rapidité inédite rend le cybercrime extrêmement préoccupant. Cette industrialisation s'accompagne aussi d'une spécialisation des défenses. Dans de nombreuses organisations, on distingue des experts qui se séparent en deux équipes pour simuler des attaques ; typiquement la blue team

(défenseurs) et la red team (attaquants, souvent internes lors de pentests). Elle reflète le fait que la cybersécurité est désormais pensée comme un jeu permanent d'attaque et de défense.

La multiplication des vulnérabilités critiques des systèmes contribue également à renforcer cette perception du risque. Les participants évoquent un véritable « feu d'artifice » de failles concernant des éditeurs majeurs comme SAP ou Microsoft, dont les logiciels sont utilisés dans le monde entier. Nabil Babaci insiste sur la dimension géopolitique de ce phénomène : « certains États peuvent chercher à exploiter ces vulnérabilités pour cibler des entreprises stratégiques » (Entretien n°7). Même des responsables politiques initialement sceptiques, comme Donald Trump aux États-Unis, ont fini par reconnaître l'importance stratégique du financement des CVE. Dans ce contexte, les entreprises voient dans la cybersécurité un enjeu qui dépasse la simple technique : il s'agit d'un facteur de souveraineté, de stabilité économique et, comme expliqué précédemment, de continuité de l'activité.

Au-delà des outils et des vulnérabilités, le facteur humain ressort comme l'un des maillons les plus fragiles. Même si ce facteur peut être très souvent sous-estimé, plusieurs entretiens en témoignent. L'auditrice de Cité Marine souligne le besoin de renforcer la sensibilisation des salariés au phishing, tandis que les experts d'EY racontent un test édifiant : « même le CFO a cliqué » lors d'une campagne de phishing interne (Entretien n°7). Le cas illustre la difficulté à assurer un niveau homogène de vigilance, même pour des personnes ayant des responsabilités importantes au sein des organisations. Christophe Pernot, DPO de Louvre Hôtels Group, insiste lui aussi sur l'importance de l'éducation et de la formation du personnel, expliquant qu'il consacre une partie importante de ses audits à « éduquer les membres du personnel pour éviter d'avoir des faiblesses humaines » (Entretien n°4).

Comme évoqué plus tôt, cette évolution de la perception du risque cyber ne s'est toutefois pas faite au même rythme selon les secteurs. Dans des secteurs où les données clients sont centrales, le risque est considéré comme stratégique depuis plusieurs années. Christophe Pernot explique que son groupe n'a pas attendu le RGPD pour structurer une approche de cybersécurité car une attaque aurait pu représenter une interruption massive d'activité, comparable à l'effet du COVID sur l'hôtellerie (Entretien n°4). Dans le secteur IT, Amadeus a également anticipé ces évolutions en mettant en œuvre des standards comme ISO 27001, NIS2 ou PCI-DSS bien avant leur obligation légale afin de développer la protection des actifs critiques comme les données de paiement, de voyage de ses clients et autres PII (Entretien n°6). À l'inverse, dans des

secteurs moins digitalisés comme l'agroalimentaire, la cyber n'a gagné en importance que récemment et souvent à la marge.

Dans ce contexte de montée en puissance des risques, il est légitime de s'interroger sur le rôle qu'a joué et joue aujourd'hui l'audit interne. Plusieurs entretiens montrent que cette fonction a connu une évolution notable, notamment via l'intégration progressive de la cybersécurité à ses préoccupations. Historiquement, l'audit interne était centré sur le contrôle des processus financiers et opérationnels avec une expertise limitée en matière de technologies de l'information. Mais la transformation numérique des organisations a conduit à une nécessaire adaptation. Comme le souligne André Antunes, directeur audit IT et cyber chez Carrefour, c'est parfois l'audit qui a permis de faire émerger le sujet au sein des directions générales : "quand l'audit interne (l'audit interne de la banque Carrefour au Brésil. NDLR) a mis en place une évaluation basée sur le NIST, ça a forcé les dirigeants à regarder le sujet de plus près" (Entretien n°3). L'audit est donc devenu un véritable catalyseur, développant sa capacité de traduire les enjeux techniques en constats structurés et en recommandations compréhensibles pour le top management.

Pour autant, les perceptions quant au rôle de l'audit interne dans la mitigation du risque cyber ne sont pas homogènes dans toutes les entreprises interrogées. Chez Carrefour, l'audit est vu comme un partenaire essentiel qui aide à formaliser et à donner du poids aux équipes cyber dans leurs discussions avec les dirigeants. Guillaume Cécile explique à ce propos que « l'audit est parfois perçu comme contraignant, mais il constitue un levier puissant : sa capacité à mettre en lumière des risques et à formuler des recommandations donne du poids aux équipes cybersécurité » (Entretien n°5). À l'inverse, dans des entreprises plutôt alimentaires/industrielles comme Cité Marine, l'audit est davantage perçu comme un acteur périphérique. Il joue un rôle ponctuel de relais de confiance, mais avec une influence minime sur la stratégie cyber, car cette dernière est souvent confiée à la DSI et à un prestataire externe.

Cette diversité de perception reflète les limites actuelles de la fonction. Plusieurs interlocuteurs soulignent que l'audit interne souffre encore d'un manque de compétences spécialisées pour aborder efficacement les enjeux cyber. Comme le résume Mathieu Gras, « on est sur une phase de maturité où l'audit interne n'est pas forcément sur les sujets cyber car il manque de compétences dans beaucoup de boîtes » (Entretien n°7). Ce déficit limite la capacité et la possibilité de la fonction d'audit à jouer un rôle central dans la mitigation du risque. Malgré

tout, les attentes évoluent et des signaux montrent que l'audit est de plus en plus appelé à s'impliquer dans les questions cyber. Par le biais de missions intégrant des volets IT ou en s'appuyant sur des référentiels comme ISO 27001, son rôle évolue.

Cette montée en puissance se heurte cependant à deux obstacles majeurs : la technicité croissante des sujets et le manque de ressources budgétaires. André Antunes observe qu'il est beaucoup plus efficace de former un expert cyber à l'audit que l'inverse, tant la marche technique est haute : « former un auditeur à la cyber, ça marche rarement » (Entretien n°3). Ce constat témoigne donc de la difficulté pour l'audit interne de devenir un acteur pleinement compétent sans un soutien fort en formation ou en collaboration avec des experts spécialisés.

Enfin, la reconnaissance de l'audit interne comme acteur clé dépend aussi de son positionnement institutionnel au sein des organisations. Les témoignages recueillis montrent que là où les lignes de défense sont claires et là où le CISO est indépendant de la DSI, l'audit interne peut jouer son rôle de troisième ligne plus efficacement. De l'autre côté, là où ces séparations n'existent pas, l'audit interne risque d'être relégué à un rôle secondaire. La question du « tone at the top », déjà évoquée, est donc double : il s'agit non seulement d'obtenir l'exemplarité des dirigeants en matière de pratiques cyber mais aussi de garantir un cadre de gouvernance où l'audit puisse exercer pleinement son rôle.

En résumé, l'évolution de la cybersécurité au cours des dix dernières années, telle qu'elle ressort de ces entretiens, peut être décrite comme un passage d'un risque secondaire ou technique à un enjeu stratégique. La reconnaissance comme telle par les directions, même si elle peut être encore inégale selon les secteurs, joue grandement à l'importance de sa prise en compte. Les modes d'attaque se sont aussi transformés en passant du vandalisme numérique à l'exploitation économique de la donnée. Le cybercrime s'est professionnalisé et industrialisé, tandis que les vulnérabilités critiques et la dimension géopolitique ont ajouté de nouvelles couches de complexité au monde de la cybersécurité. Dans le même temps, un des maillons faibles reste le facteur humain et la diffusion d'une culture cyber dépend donc largement de l'engagement du top management. Enfin, le rôle de l'audit interne est en pleine mutation et oscille encore entre fonction périphérique et acteur de premier plan selon les organisations. Les entretiens montrent que lorsqu'il dispose des compétences et de la légitimité nécessaires, l'audit peut être un catalyseur essentiel dans la mitigation du risque cyber, mais que ce rôle reste à consolider dans certains cas.

3.2. Le terrain avec le risque cyber

L'évolution de la perception du risque cyber qui a été analysée dans la partie précédente, n'a de sens que si elle s'accompagne d'une mise en œuvre effective dans les organisations. Grâce aux entretiens réalisés, l'étude du terrain permet de comprendre comment les entreprises traduisent ces menaces en dispositifs opérationnels, notamment à travers leur outillage IT et en pratiques de gouvernance. Une certaine convergence autour de référentiels et d'outils partagés ainsi que des divergences fortes selon les secteurs, les cultures organisationnelles ou encore les contraintes réglementaires seront exposées dans la partie suivante. Dans ce contexte, Amadeus et Louvre Hôtels Group illustrent particulièrement bien les difficultés spécifiques liées à la conformité internationale et à la gestion quotidienne des données clients. De l'autre côté, Carrefour et d'autres acteurs montrent la maturité croissante d'approches pragmatiques et industrialisées.

Un premier constat tient au rôle central joué par les référentiels et normes sectorielles dans la cybersécurité. Dans les entreprises interrogées, la plupart des pratiques cyber sont adossées à ces cadres structurants. Le NIST est le plus cité, notamment par Carrefour qui l'utilise chaque année pour auditer l'ensemble de ses Business Units. Guillaume Cécile explique que ce référentiel « est assez généraliste et permet une comparabilité internationale » (Entretien n° 5). André Antunes rappelle aussi qu'à la banque Carrefour au Brésil, c'est l'audit interne qui a introduit une évaluation basée sur le NIST et que « ça a forcé les dirigeants à regarder le sujet de plus près » (Entretien n°3). Mais si le NIST s'impose comme un standard largement reconnu, d'autres cadres viennent compléter le panel d'atténuation du risque cyber. On peut notamment parler de MITRE ATT&CK, utilisé pour cartographier les tactiques et techniques des cybercriminels, ainsi que de l'OWASP, avec son fameux "Top 10" des vulnérabilités applicatives, qui sont régulièrement mobilisés par les équipes cyber. "MITRE est une matrice des techniques d'attaque observées dans le monde réel", explique André Antunes, tandis qu'OWASP fournit une liste des dix vulnérabilités les plus critiques" (Entretien n°3). Enfin, ISO 27001 demeure une référence incontournable dans plusieurs environnements, en particulier dans des secteurs où la conformité réglementaire est forte.

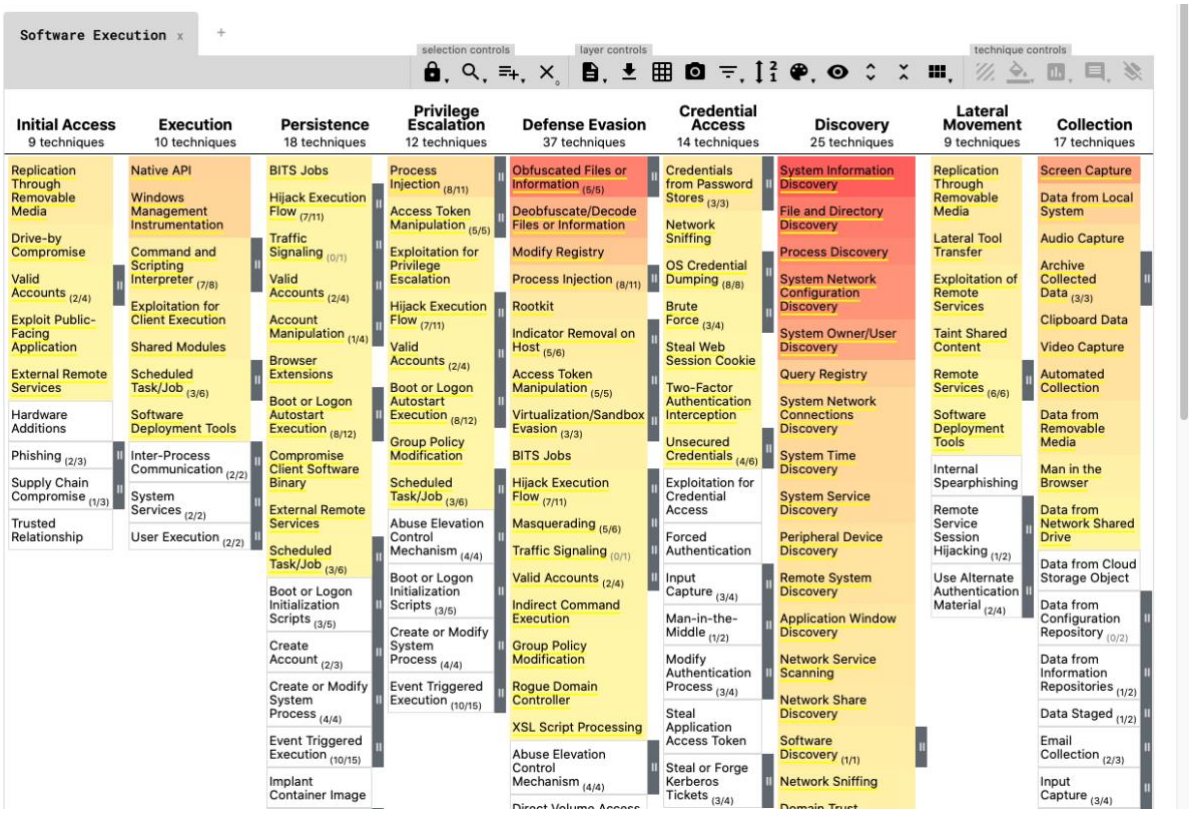


Figure 10 : MITR ATT&CK Framework (Source : MITRE ATT&CK®, 2025)

C'est le cas chez Amadeus, entreprise IT du secteur du voyage, dans laquelle la dimension internationale impose une conformité multiple notamment en lien avec le fort volume de données clients exploitées. Notre interlocuteur explique que la société doit être à la fois conforme à ISO 27001, à NIS2 mais aussi à PCI-DSS, ce dernier étant spécifique à la protection des données de carte bancaire imposée par Visa et Mastercard. Il souligne aussi la difficulté de "traduire" les réglementations européennes dans les différentes législations nationales : en Espagne, par exemple, Amadeus doit appliquer la version espagnole du RGPD, légèrement différente de la française (Entretien n°6). En effet, de par la transposition des lois européennes dans les pays membres de l'UE, certaines transpositions peuvent varier et compliquer le travail des entreprises opérant dans plusieurs pays européens. Le travail de mapping des obligations réglementaires devient alors une tâche réellement à part entière. Elle nécessite de mobiliser des ressources importantes pour assurer que toutes ces exigences locales soient respectées. Cette complexité propre aux multinationales contraste avec des acteurs plus locaux comme Cité Marine, pour lesquels les référentiels dominants restent ceux de la qualité agroalimentaire (ISO

22000, IFS Food) qui comporte seulement quelques points transposables à la cyber (gestion des accès, sauvegardes).

Louvre Hôtels Group illustre une autre approche sectorielle. Pour un groupe d'hospitalité manipulant quotidiennement des données clients, ISO 27001 est le cadre utilisé pour auditer les processus de cybersécurité. Néanmoins, la pratique repose aussi sur des outils très concrets. Christophe Pernot, DPO de l'entreprise, explique que cette dernière utilise un outil de contrôle des comptes utilisateurs, permettant de vérifier qu'ils ne soient pas partagés entre plusieurs employés ni connectés simultanément sur différents postes. Cet outil est essentiel pour garantir que chaque collaborateur dispose d'un niveau d'accréditation correspondant à son poste. Cela est aussi essentiel car ça assure que la ségrégation des pouvoirs soit assurée et que les utilisateurs ne puissent pas valider des demandes qu'ils auraient eux-mêmes formulées précédemment. Il mentionne également un système bloquant les mots de passe non conformes aux recommandations de la CNIL : « cet outil permet de bloquer les mots de passe qui ne respectent pas les règles définies par la CNIL » (Entretien n°4). La CNIL demande par exemple que les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux. Ce type de mesure illustre le lien direct entre réglementation nationale et pratiques quotidiennes de sécurité.

L'utilisation des outils suit par ailleurs une logique pragmatique et progressive. Chez Carrefour, la stratégie consiste à tester d'abord des solutions plutôt open source puis à migrer vers des versions premium si ces solutions gratuites s'avèrent efficaces et bien adaptées aux besoins. Guillaume Cécile résume ce modèle par une formulation simple : « on part sur l'open source, puis on bascule sur une version premium » (Entretien n°5). Cette approche a été notamment appliquée chez Carrefour avec CNAPP, qui est une plateforme de protection des applications cloud. D'abord testé dans sa version open source avant d'être remplacée par une solution plus robuste couvrant 90 % des vulnérabilités contre 20 % auparavant, ce test d'open-source a été donc très concluant. Le même schéma a été suivi avec le SOAR qui est un logiciel utilisé pour catégoriser les alertes et filtrer les faux positifs avant de les transmettre au SOC (Security Operations Center). On retrouve ici un processus d'expérimentation et d'industrialisation permettant d'optimiser les budgets et de sécuriser l'adoption d'outils complexes par les équipes de cybersécurité.

Comme expliqué précédemment dans cette thèse professionnelle, l'expérience de Louvre Hôtels Group illustre également la recherche de solutions pragmatiques adaptées aux besoins. Christophe Pernot met en avant des outils qui, sans être spectaculaires, apportent une réelle valeur ajoutée pour sécuriser les opérations quotidiennes dans les hôtels. Mais il insiste aussi sur le rôle de la sensibilisation et de la pédagogie. Lors de ses missions dans les hôtels du groupe, il consacre une part importante de son temps à expliquer aux collaborateurs pourquoi ces contrôles sont nécessaires et comment éviter des comportements à risque. "Lors des audits dans les hôtels, je passe du temps à éduquer le personnel pour éviter d'avoir des faiblesses humaines" (Entretien n°4). On retrouve ici une différence de culture entre un groupe international côté en bourse comme Carrefour, qui industrialise ses outils à grande échelle, même si la pédagogie est clef aussi. Les pratiques opérationnelles mises en avant par les différents interlocuteurs mettent en avant cette diversité d'approches. Carrefour et EY insistent sur le recours à des auto-évaluations et des tests d'intrusion réguliers (pentests). Ces derniers sont parfois complétés par des simulations OSINT pour évaluer la robustesse des défenses. Un expert d'EY rappelle ainsi que « sans faire de pentest complet, on simule des scénarios réalistes » (Entretien n° 7). Du côté de l'agroalimentaire, Cité Marine privilégie des contrôles plus simples. La vérification des sauvegardes ou la traçabilité des données sont plus adaptées à sa taille et à ses priorités. Cette pluralité illustre bien que la cybersécurité n'est pas un bloc homogène de pratiques mais bien un ensemble adapté aux réalités sectorielles des organisations.

Durant nos entretiens, la question de la gouvernance est apparue comme un élément déterminant dans beaucoup de ces derniers. Guillaume Litvak rappelle que la séparation des rôles entre DSI et CISO avec un double rattachement de ce dernier à la direction générale et à la DSI a été un « levier de maturité » (Entretien n°2). Cette clarification des responsabilités a permis à Carrefour de renforcer sa crédibilité au niveau de sa politique de cybersécurité auprès du top management. Amadeus, de son côté, souligne l'importance de l'implication du « board » dans la gouvernance cyber. Notre interlocuteur explique que « la prise de conscience s'est faite à partir du moment où d'autres entreprises ont subi des pertes massives de données, entraînant parfois leur disparition » (Entretien n°6). Cette expérience a servi de catalyseur pour convaincre les dirigeants d'investir dans la cybersécurité et aussi d'intégrer ces enjeux dans la stratégie de gouvernance globale.

Dans ce contexte, l'audit interne joue un rôle ambivalent. Chez Carrefour, il est perçu comme un "aidant" qui permet de formaliser les constats et de donner du poids aux équipes cyber face au management, notamment pour des demandes budgétaires (Entretien n°5). À Cité Marine, il reste un acteur secondaire permettant de relayer parfois des constats à la DSI mais sans jouer un rôle central. Chez Amadeus, l'audit interne est encore peu impliqué, les audits de cybersécurité étant menés directement par le département CISO. En revanche, chez LHG, le DPO explique que la collaboration avec l'audit interne pourrait devenir un levier important, à condition que les auditeurs montent en compétence sur les normes et sur les aspects techniques des systèmes.

Malgré ces progrès, de nombreux freins persistent. Le premier est culturel. Les opérationnels, en particulier dans la grande distribution, peuvent parfois percevoir certaines mesures comme trop intrusives. Le cas du MFA est révélateur car imposer une authentification multifacteur trop fréquente ralentit les tâches et pousse parfois les employés à contourner les règles. Guillaume Cécile explique qu'« il faut trouver un équilibre entre sécurité et fluidité opérationnelle » (Entretien n°5). André Antunes souligne quant à lui que « la techno, tu la trouves ; la volonté de changer, c'est une autre histoire » (Entretien n°3). Christophe Pernot insiste sur le manque de formation, l'obligeant à consacrer une partie de ses audits à la sensibilisation des équipes (Entretien n°4). Le deuxième frein est budgétaire. La difficulté à démontrer un retour sur investissement freine souvent les investissements. Comme le résume Guillaume Cécile, « comparer le coût d'une assurance et celui d'un outil permet de parler le langage des décideurs » (Entretien n°5). Enfin, dans un contexte international comme celui d'Amadeus, la complexité réglementaire constitue une contrainte supplémentaire. De plus, comme expliqué précédemment, la diversité des normes et des transpositions nationales entraîne une lourdeur qui ralentit la mise en place de mesures et crée parfois des distorsions de concurrence entre pays.

En définitive, l'analyse du terrain montre que la cybersécurité est désormais présente dans toutes les organisations même si des formes variées existent. Certaines adoptent donc une logique d'industrialisation et d'optimisation budgétaire tandis que d'autres privilégient des approches pragmatiques centrées sur la sensibilisation et la pédagogie. Les référentiels constituent un socle commun, mais leur mise en œuvre est adaptée à chaque contexte et à chaque secteur. L'audit interne joue enfin un rôle plus ou moins central selon les cas, oscillant

entre un simple relais d'information et un facilitateur reconnu par le management. Côté freins, ils restent largement partagés : résistance au changement, contraintes budgétaires, complexité des normes. Ces constats soulignent l'écart entre les bonnes pratiques théoriques et leur application réelle ; un écart que la partie suivante analysera plus en détail.

3.3. Écart avec la théorie

Si les organisations interrogées affirment avoir progressé dans la prise en compte du risque cyber, leurs pratiques révèlent encore un décalage important avec les recommandations des référentiels ainsi que les discours académiques. Ce décalage ne signifie pas un manque d'actions de la part des entreprises. Il illustre plutôt les limites entre un cadre théorique idéal face à une réalité faite de contraintes, d'arbitrages et aussi de limites humaines. Lors de ces entretiens, cinq dimensions apparaissent particulièrement révélatrices : les compétences des auditeurs internes, la difficulté à mobiliser des ressources externes, la gouvernance parfois incomplète des dispositifs, l'adaptation partielle des normes aux réalités quotidiennes, et enfin la difficulté des référentiels à suivre le rythme de menaces hybrides et évolutives.

Le premier écart constaté se situe au niveau des compétences disponibles. Tous les interlocuteurs insistent sur le fait que les auditeurs internes ne disposent aujourd'hui pas d'un socle suffisant en matière de cybersécurité. Ce manque se traduit par des difficultés concrètes. André Antunes illustre ce constat lorsqu'il explique que les questionnaires d'auto-évaluation en matière de plans de reprise après sinistre (DRP) existent sur le papier mais que « nous ne savons pas vraiment évaluer si c'est bien ou pas » (Entretien n°3). Autrement dit, l'outil de gouvernance est présent, mais l'absence de compétences techniques dans l'audit interne empêche d'en vérifier l'efficacité réelle. Christophe Pernot, de Louvre Hôtels Group, fait le même constat : « il faut comprendre comment les informations passent d'un outil à un autre avant de prétendre les auditer » (Entretien n°4). Or, faute de la compréhension de base, les auditeurs sont contraints à émettre des constats de surface, sans pouvoir apprécier la robustesse des mesures mises en place. Dans les structures plus petites, comme Cité Marine, l'écart est encore plus visible : l'audit interne peut vérifier des sauvegardes ou l'existence de contrôles d'accès, mais il n'a pas la capacité d'analyser finement la sécurité des environnements IT. En théorie, l'audit interne doit être capable de challenger tous les dispositifs de maîtrise des risques ; en pratique, son expertise reste largement cantonnée aux processus classiques.

Cette faiblesse interne pourrait être compensée par le recours à des ressources externes. Mais une nouvelle fois, la réalité se heurte à des contraintes budgétaires. Plusieurs participants reconnaissent que l'idéal théorique, de compléter l'audit interne par des experts spécialisés en cyber, est difficile à mettre en place. André Antunes estime qu'il est plus efficace de « prendre un expert cyber et de le former à l'audit que l'inverse » (Entretien n°3). Mais cette solution suppose de recruter ou de contracter des profils coûteux. Cependant, dans les entreprises où le cyber n'est pas perçu comme prioritaire, ces arbitrages budgétaires sont rarement en faveur de l'audit. Cité Marine illustre cette situation en faisant appel à un prestataire externe (ACCEIS) qui prend en charge la cybersécurité, tandis que l'audit interne reste cantonné à un rôle secondaire, faute de moyens. À l'opposé, Carrefour dispose des ressources nécessaires pour associer des experts, mais même dans ce groupe, Guillaume Cécile reconnaît que les investissements doivent sans cesse être justifiés auprès des décideurs. "Comparer le coût d'une assurance et celui d'un outil permet de parler le langage des décideurs" (Entretien n°5). On peut observer ici un écart entre un discours académique qui insiste sur l'importance d'investir massivement et une pratique contrainte par la nécessité de démontrer un retour sur investissement tangible, parfois à court terme.

Sur le plan de la gouvernance, un autre écart apparaît mais distinct de la question institutionnelle déjà abordée précédemment. Ce décalage concerne la culture et l'exemplarité des dirigeants des organisations. Dans la théorie, les référentiels insistent sur la nécessité d'un engagement clair du « tone at the top ». Néanmoins, plusieurs témoignages révèlent que cette impulsion reste très souvent insuffisante. André Antunes évoque ainsi des cas où certains dirigeants ne respectent pas eux-mêmes les règles élémentaires de cybersécurité, comme l'utilisation de l'authentification multifactorielle (Entretien n°3). Cette absence d'exemplarité affaiblit les efforts de diffusion d'une culture cyber dans l'organisation. Plus largement, plusieurs interlocuteurs relèvent que les dirigeants comprennent l'impact financier d'une attaque mais pas les mesures opérationnelles qui permettent de s'en préserver. Guillaume Cécile résume cette tension en disant : « les aspects techniques apparaissent trop terre-à-terre pour une partie des dirigeants » (Entretien n°5). On retrouve donc un décalage entre les attendus théoriques et une réalité où la cybersécurité reste souvent perçue comme une contrainte technique et non encore comme un levier stratégique.

Un quatrième écart concerne la compatibilité des normes aux réalités organisationnelles. Tous les interlocuteurs reconnaissent la valeur structurante et précieuse des standards comme NIST, ISO 27001 ou COBIT, mais leur application intégrale se heurte à des contraintes de terrain. Christophe Pernot insiste sur l'importance de la pédagogie pour transposer ces cadres dans les hôtels : « avant de vouloir évaluer, il faut comprendre ce qui est en face de nous » (Entretien n°4). Guillaume Cécile estime de son côté que les normes ISO sont trop complètes pour un usage quotidien dans l'industrie du retail et qu'elles risquent de décourager les équipes opérationnelles (Entretien n°5). Les interlocuteurs convergent sur le constat que ces normes doivent être adaptées, simplifiées ou « sur mesure » pour correspondre à la réalité des métiers. Amadeus illustre bien cette tension. La conformité aux standards est incontournable pour une entreprise IT internationale, néanmoins l'empilement des normes et des réglementations locales contribue à créer une complexité difficilement compatible avec une bonne fluidité opérationnelle. L'écart se situe donc entre un idéal de conformité exhaustif et une pratique qui privilégie l'adaptation pragmatique aux besoins ainsi qu'aux ressources disponibles.

Enfin, la cinquième dimension d'écart concerne la nature même des menaces. Les référentiels et la littérature académique tendent à catégoriser les risques de manière claire et structurée (phishing, ransomware, perte de données, etc.). Or, les témoignages montrent que la réalité est beaucoup plus hybride et évolutive. Mathieu Gras et Nabil Babaci décrivent un « feu d'artifice de vulnérabilités » (Entretien n°7), où les cybercriminels combinent différentes techniques et s'appuient sur une véritable industrialisation du crime. L'apparition de l'intelligence artificielle ajoute davantage à cette complexité. Pour ces experts, l'IA peut aussi bien renforcer la défense que malencontreusement multiplier les capacités d'attaque, rendant les référentiels existants rapidement obsolètes. Le décalage se situe donc dans la vitesse d'évolution des normes, qui fournissent un cadre statique, alors que les menaces évoluent en permanence. Cela explique pourquoi certains audits concluent à des risques « modérés » alors que, dans la pratique, le danger est bien plus critique.

En définitive, ces écarts soulignent les limites de la transposition mécanique des cadres théoriques dans les organisations. L'idéal académique et normatif se heurte à des obstacles concrets avec un manque de compétences, des budgets contraints, des dirigeants peu exemplaires, des normes trop lourdes, des menaces trop mouvantes. L'audit interne, censé être le garant d'une évaluation indépendante et rigoureuse, se retrouve souvent dans une position

ambivalente, assez présent pour alerter mais pas suffisamment compétent ou doté de moyens pour évaluer pleinement le risque cyber. Ce constat appelle une réflexion sur l'avenir de la fonction. Comment combler ces écarts, renforcer les compétences, adapter les normes et faire de l'audit interne un véritable acteur d'atténuation du risque cyber ? Ces pistes d'avenir, mises en avant par nos interlocuteurs, seront développées dans la section suivante.

3.4 Futur de l'audit interne avec la cyber et recommandations pour l'avenir

Les constats dressés précédemment sur l'évolution de la cybersécurité et sur les écarts persistants entre théorie et pratique invitent à réfléchir à l'avenir du rôle de l'audit interne. Si cette fonction est déjà reconnue comme un acteur de gouvernance incontournable dans la majorité des organisations, sa contribution spécifique à la maîtrise du risque cyber reste hétérogène parmi les secteurs et parfois limitée. Pourtant, tous les entretiens montrent que la tendance est à une intégration croissante des sujets cyber dans les missions d'audit interne. L'enjeu n'est plus de savoir si l'audit doit s'en saisir mais plutôt comment il peut le faire efficacement et durablement. Cette dernière section propose d'explorer les perspectives d'évolution de la fonction, autour de six dimensions : la généralisation de l'intégration cyber, la montée en compétences des équipes, la question budgétaire, l'impact des régulations, la sensibilisation élargie des parties prenantes et la nécessité d'un modèle d'audit intégré. Chaque dimension est analysée à la lumière des propos recueillis et accompagnée de recommandations.

Le premier axe concerne la généralisation de l'intégration de la cybersécurité dans les missions d'audit interne. Aujourd'hui, comme l'ont souligné nos entretiens, l'implication de l'audit reste en effet très variable selon les secteurs. Chez Carrefour, la cybersécurité est devenue un pilier du plan d'audit, notamment avec des thématiques prioritaires actualisées chaque année (Entretien n°2). À l'inverse, dans des entreprises industrielles comme Cité Marine ou Louvre Hôtels Group, l'audit se limite à vérifier ponctuellement certains points plutôt IT (Entretien n°1 et 4). Cette diversité démontre un retard relatif alors que la théorie invite l'audit à traiter le cyber comme un risque transversal majeur. L'avenir passe donc par une extension systématique des volets cyber dans toutes les missions, même celles qui ne sont pas purement IT. Comme le souligne Guillaume Cécile, l'audit est souvent perçu comme « un aidant » qui formalise et donne du poids aux équipes cyber (Entretien n°5). C'est dans ce rôle de catalyseur que la

fonction doit s'ancrer, en intégrant le cyber non comme un audit à part mais comme une dimension transversale de chaque mission.

Recommandation : inscrire la cybersécurité dans toutes les cartographies de risques auditées, en veillant à adapter le périmètre des contrôles au secteur et aux ressources disponibles. L'audit ne doit plus être limité à des missions spécifiques mais devenir un relais systématique de la culture cyber.

Le second axe porte sur les compétences. Tous les participants convergent sur le fait que la faiblesse actuelle de l'audit interne est son manque de maîtrise technique. André Antunes rappelle qu'« il est plus facile de former un expert cyber à l'audit que l'inverse » (Entretien n°3). Christophe Pernot confirme que les auditeurs manquent de compréhension technique des flux d'information (Entretien n°4). Ces témoignages soulignent que la valeur ajoutée de l'audit reste aujourd'hui freinée par ce manque de savoir-faire. Le futur de la fonction repose donc sur la montée en compétences des auditeurs avec des formations continues, certifications spécifiques (CISA, CISSP, ISO 27001 Lead Auditor) mais aussi développement de profils hybrides. Chez Carrefour, la politique d'une heure de formation mensuelle sur la cybersécurité pour les auditeurs (Entretien n°2) illustre une démarche concrète, qui pourrait être facilement généralisée. Les experts d'EY vont plus loin, estimant qu'un budget annuel de l'ordre de 200 000 € serait nécessaire pour constituer une équipe interne spécialisée (Entretien n°7).

Recommandation : mettre en place des parcours de formation obligatoires pour les auditeurs internes, en intégrant des briques cyber dans leur cursus et en recrutant ponctuellement des profils hybrides capables de faire le lien entre technique et gouvernance.

Le troisième axe concerne la question budgétaire. Les organisations peinent à investir durablement dans la cybersécurité faute de retour sur investissement immédiat. Comme l'a exprimé Guillaume Cécile, « comparer le coût d'une assurance et celui d'un outil permet de parler le langage des décideurs » (Entretien n°5). Ce constat montre bien que la logique budgétaire reste dominée par une vision à court terme. Alors que la cybersécurité appelle une approche de long terme. Les directions audit doivent apprendre à argumenter dans ces termes, en chiffrant d'un côté les pertes potentielles mais aussi de l'autre les gains indirects d'un renforcement cyber (réduction de primes d'assurance, continuité d'activité, préservation de la réputation). EY propose une approche plus volontariste des dirigeants en plaidant pour un

budget dédié à l'audit cyber, comparable au rôle des commissaires aux comptes dans la sphère financière (Entretien n°7).

Recommandation : élaborer des business cases structurés pour chaque investissement cyber, incluant l'impact sur les assurances, la réputation et la résilience, afin de faciliter l'arbitrage. Les départements d'audit doivent se positionner comme des porteurs de scénarios économiques pour convaincre le top management dans les cas où la cybersécurité est demandeuse d'aide.

Un quatrième axe réside dans l'impact des régulations. La multiplication des cadres réglementaires (RGPD, NIS2, DORA, CSRD) renforce la pression sur les entreprises. Amadeus illustre bien la difficulté de conformité internationale, où l'empilement des normes européennes et nationales nécessite un travail de mapping permanent (Entretien n°6). Pour Louvre Hôtels Group, ISO 27001 et les recommandations de la CNIL structurent déjà les pratiques (Entretien n°4). Ces exemples montrent que la réglementation joue un rôle d'accélérateur. Même si les référentiels sont jugés lourds, ils forcent les entreprises à se doter de pratiques qu'elles n'auraient pas adoptées spontanément. L'audit interne doit anticiper ce mouvement. Il ne peut plus se contenter de suivre la réglementation a posteriori : il doit devenir un acteur proactif en améliorant sa capacité à identifier les évolutions à venir et à accompagner la mise en conformité des projets dès les phases de conception.

Recommandation : intégrer une veille réglementaire cyber dans les missions d'audit interne et établir des passerelles régulières avec les fonctions juridiques et de conformité. Cette anticipation permettra de limiter les écarts entre théorie et pratique constatés aujourd'hui.

Le cinquième axe touche à la sensibilisation de l'ensemble des parties prenantes. Plusieurs témoignages rappellent que la cybersécurité reste encore perçue comme une affaire de spécialistes. Or, les attaques les plus courantes exploitent les failles humaines. L'auditrice de Cité Marine souligne que la formation au phishing serait essentielle pour ses collègues (Entretien n°1). Chez LHG, Christophe Pernot explique qu'une part importante de ses audits consiste à « éduquer le personnel pour éviter des faiblesses humaines » (Entretien n°4). Les experts d'EY abordent aussi cela en parlant du test de phishing qui a montré que même un CFO pouvait cliquer sur un lien frauduleux (Entretien n°7). Ces constats révèlent que la meilleure des technologies est inutile sans une culture cyber partagée par tous car rappelons-le mais la cybersécurité, au même titre que la gestion du risque est l'affaire de tous. L'audit interne peut

donc jouer un rôle clé de relais de sensibilisation, en intégrant des modules de formation dans ses missions ainsi que par la diffusion des retours d'expérience et des bonnes pratiques.

Recommandation : instaurer un volet de sensibilisation dans chaque mission d'audit interne, adapté aux opérationnels concernés et relayer les constats auprès du comité d'audit pour assurer une diffusion au plus haut niveau.

Enfin, le sixième axe concerne l'émergence d'un modèle d'audit intégré. Tous les entretiens convergent vers l'idée qu'il est nécessaire de renforcer la collaboration entre l'audit interne et les équipes cyber. Guillaume Cécile rappelle que l'audit interne est un « levier puissant » car il donne du poids aux équipes cyber face au top management (Entretien n°5). André Antunes plaide pour des binômes audit–expert IT afin de renforcer les diagnostics sur des sujets techniques mais stratégiques (Entretien n°3). Chez Amadeus, le département CISO réalise déjà des audits de conformité sans l'aide de l'audit interne (Entretien n°6). Cependant, le département n'est pas contre une collaboration entre les deux services. L'avenir réside donc dans un modèle de complémentarité entre ces fonctions, où l'audit n'essaie pas de se substituer aux experts mais s'appuie sur eux pour enrichir son regard. EY anticipe même l'émergence de « commissaires aux comptes cyber » qui seraient capables de certifier la robustesse numérique des entreprises au même titre que les CAC pour les états financiers (Entretien n°7).

Recommandation : créer des comités conjoints audit–cyber, ritualiser des missions intégrées et envisager, à moyen terme, la constitution d'équipes mixtes associant auditeurs internes et experts techniques. Ce modèle renforcerait la crédibilité de la fonction ainsi que sa valeur ajoutée stratégique.

En conclusion, l'avenir de l'audit interne face au risque cyber se dessine autour d'une intégration croissante mais très exigeante. Les défis restent cependant clairs et passent par un renforcement des compétences, l'obtention des budgets dédiés, l'anticipation des nouvelles régulations, la sensibilisation de l'ensemble des parties prenantes ou encore l'instauration d'une collaboration structurée avec les experts cyber. Les recommandations formulées ici ne visent pas à proposer une recette universelle mais plutôt à identifier des leviers concrets pour réduire l'écart entre théorie et pratique. L'audit interne a déjà démontré sa capacité à être un accélérateur de prise de conscience. Son futur dépendra donc de sa faculté à aller plus loin en devenant un acteur proactif et crédible de l'atténuation du risque cyber. Ces perspectives ouvrent directement sur la conclusion générale de ce mémoire, qui reviendra sur les principaux

enseignements de l'étude et sur les apports professionnels que ces résultats peuvent offrir à la fonction d'audit interne.

Conclusion

La problématique de cette thèse professionnelle posait une question centrale : de quelle manière les exigences croissantes en matière de cybersécurité transforment-elles les approches et les outils de l'audit interne pour gérer les risques organisationnels et technologiques ? Après avoir croisé la littérature académique et professionnelle avec les entretiens menés auprès de praticiens issus de secteurs variés comme la grande distribution, l'hôtellerie, l'agroalimentaire, le conseil ou encore le service, il est désormais possible de tirer un ensemble de conclusions.

Premièrement, les entretiens montrent de manière indiscutable que la cybersécurité a cessé d'être un sujet périphérique pour devenir un enjeu stratégique. Même si ce changement de perception n'a pas été uniforme selon les secteurs d'activités. Dans des entreprises industrielles ou d'agroalimentaire comme Cité Marine, la priorité demeure la qualité et la sécurité alimentaire. En effet, la cybersécurité n'apparaît pour le moment que comme un risque secondaire pouvant perturber la production sans remettre en cause l'existence de l'entreprise. À l'opposé, pour d'autres entreprises fortement digitalisées comme Carrefour ou Amadeus, la menace est pleinement reconnue et intégrée dans le plan d'audit et dans la stratégie de gouvernance. Cela est le cas car ces entreprises sont conscientes qu'une attaque pourrait paralyser l'ensemble du groupe ou encore compromettre les données sensibles des clients. Cette évolution traduit un basculement général, la menace n'est plus seulement technique mais touche directement la continuité d'activité ainsi que la réputation des organisations. Elle est d'autant plus préoccupante que les formes d'attaques se sont transformées depuis quelques années. Là où l'on parlait dans le passé de défaçage de sites internet et d'intrusions à finalité destructrice, on observe désormais la multiplication d'attaques par ransomware combinées à l'exfiltration de données, comme l'explique Guillaume Cécile chez Carrefour. Mathieu Gras et Nabil Babaci d'EY confirment ce point. Ces derniers décrivent une « ubérisation du crime », où des acteurs spécialisés se coordonnent via des messageries chiffrées pour revendre des données, parfois plusieurs mois après les avoir exfiltrées. Le cybercrime est devenu une industrie structurée obligeant les entreprises à repenser leur protection contre ces criminels.

Deuxièmement, les exigences croissantes de cybersécurité se traduisent par une transformation des pratiques de contrôle ainsi que de gouvernance au sein des organisations. Les référentiels internationaux, qu'il s'agisse du NIST, de l'ISO 27001 ou de COBIT, constituent des socles incontournables et robustes. Néanmoins, leur mise en œuvre diffère beaucoup selon les

contextes d'activités. Carrefour pratique des audits NIST annuels sur l'ensemble de ses Business Units, Amadeus doit jongler entre ISO 27001, NIS2 et PCI-DSS en fonction de ses obligations internationales, tandis que Louvre Hôtels Group s'appuie sur ISO 27001 et les recommandations de la CNIL pour encadrer des pratiques très concrètes comme le contrôle des mots de passe. Dans d'autres environnements, comme Cité Marine, ce sont plutôt des référentiels qualité tels qu'ISO 22000 ou IFS Food qui structurent les démarches, avec quelques transpositions cyber. On retrouve donc une logique d'adaptation pragmatique dans laquelle les standards sont modulés et « tailored » pour correspondre à la taille et aux priorités de l'organisation. Les pratiques d'outillage suivent cette même logique progressive. Carrefour illustre parfaitement l'approche « test and scale ». En effet, à partir d'outils open source comme le CNAPP ou le SOAR, ils testent leur pertinence, les industrialisent et ensuite passent à des versions premium plus robustes une fois la preuve de valeur démontrée. Cette démarche permet de concilier contraintes budgétaires et efficacité opérationnelle. Les tests d'intrusion, contrôles d'accès ou encore simulations OSINT décrites par EY peuvent compléter ces dispositifs. Mais derrière ces méthodes, la gouvernance reste décisive et cruciale. Comme le rappelle Guillaume Litvak, la séparation des rôles entre CISO et DSI, avec un double rattachement, a constitué un « levier de maturité » majeur chez Carrefour. Chez Amadeus, la sensibilisation du Board à la réalité des pertes massives de données subies par d'autres entreprises a également joué un rôle clé pour inscrire la cybersécurité dans la gouvernance stratégique.

Troisièmement, l'analyse fait apparaître un écart persistant entre la théorie et la réalité du terrain. Si la littérature et les référentiels insistent sur l'exemplarité du « tone at the top », plusieurs interlocuteurs soulignent l'insuffisante implication concrète des dirigeants. André Antunes raconte par exemple que certains membres du Comex n'utilisent pas eux-mêmes la double authentification, ce qui affaiblit les efforts de diffusion d'une culture cyber. De même, Guillaume Cécile constate que les dirigeants comprennent l'impact financier des menaces mais jugent les mesures opérationnelles trop terre-à-terre pour s'y investir pleinement. Cet écart se retrouve dans l'adéquation des normes : ISO 27001 est jugée trop lourde pour le retail. Les contraintes budgétaires renforcent ce décalage, comme l'explique Guillaume Cécile, il faut souvent comparer le coût d'une assurance et celui d'un outil pour convaincre le top management, signe que la logique reste court-termiste. Enfin, la rapidité d'évolution de ces menaces rend difficile toute transposition stricte des référentiels. Ces deniers peuvent paraître

statiques face à un « feu d'artifice de vulnérabilités » en constante mutation, comme le rappellent les experts d'EY.

Quatrièmement, se pose la question de l'évolution du rôle de l'audit interne et de sa capacité à devenir un acteur clé de son atténuation du risque cyber. Les entretiens révèlent des perceptions contrastées en fonction des secteurs. Chez Carrefour, l'audit est reconnu comme un catalyseur. En effet, en formalisant les constats et en les intégrant dans les plans d'action, il donne du poids aux équipes cyber dans leurs discussions avec le top management. Guillaume Cécile explique qu'il est parfois perçu comme contraignant mais qu'il reste un levier puissant pour faire avancer certains dossiers sensibles. A l'inverse, dans des entreprises comme Cité Marine, l'audit interne se limite à un rôle secondaire. Se cantonnant à un simple relai des constats, mais laissant la maîtrise à la DSI et au prestataire externe. Dans des organisations comme Amadeus, l'audit interne reste encore très peu impliqué, les audits cyber étant menés directement par le département CISO. Ces différences tiennent largement au déficit de compétences. En effet, tous les interlocuteurs s'accordent à dire que la marche est haute pour des auditeurs traditionnels. Comme le souligne André Antunes, « former un auditeur à la cyber, ça marche rarement, il vaut mieux former un expert cyber à l'audit ». Ce manque de compétences transverses empêche l'audit d'évaluer pleinement les dispositifs digitalisés. Pourtant, les attentes évoluent car des missions intégrant des volets IT et cyber apparaissent. Dans ce contexte, l'avenir de la fonction d'audit interne repose sur trois leviers principaux : le renforcement des compétences des auditeurs par un aspect RH ; la formation et le recrutement de profils hybrides ainsi qu'un aspect financier ; l'obtention de budgets dédiés et une meilleure articulation avec les experts techniques. Les expériences de Carrefour, avec ses formations mensuelles, et d'EY, qui plaide pour un budget de 200 000 € afin de créer une équipe d'audit cyber, illustrent ces pistes.

Cinquièmement, il convient d'ouvrir la réflexion sur les perspectives plus larges que dessine cette évolution. La montée en puissance des régulations, qu'il s'agisse du RGPD, de NIS2 ou de la CSRD, montre que la cybersécurité ne sera plus une option dans le futur mais un impératif inscrit dans la gouvernance et la transparence des entreprises. Cela oblige l'audit interne à développer une veille réglementaire et à travailler main dans la main avec les services juridiques et conformité. La sensibilisation de l'ensemble des parties prenantes apparaît aussi comme un chantier prioritaire. Les témoignages de Cité Marine, de LHG ou encore le test de

phishing relaté par EY montrent que les failles humaines demeurent le maillon le plus fragile. L'audit interne a donc un rôle clé de relais de sensibilisation et de diffusion d'une culture cyber auprès de toutes les populations de l'entreprise. Enfin, le modèle d'audit intégré, combinant auditeurs internes et experts techniques, représente sans doute l'une des pistes les plus prometteuses. Qu'il s'agisse des binômes audit–cyber expérimentés à la banque Carrefour Brésil par André Antunes ou aussi de la symbiose décrite par Carrefour entre audit et équipes cyber, ces expériences convergent vers l'idée que l'indépendance de l'audit ne doit pas exclure la collaboration technique mais au contraire s'en nourrir et en tirer les avantages nécessaires. En définitive, cette thèse montre que les exigences croissantes en matière de cybersécurité transforment profondément les approches et outils de l'audit interne. Ce dernier passe d'un rôle de contrôle a posteriori à une fonction plus proactive et intégrée dans la gouvernance pour renforcer sa crédibilité face aux dirigeants. La mutation n'est pas achevée et reste marquée par des écarts importants selon les secteurs et les organisations. Néanmoins, les trajectoires observées convergent toutes vers une hybridation croissante des compétences, des méthodes et des rôles. Cette évolution reflète le lien désormais indissociable entre performance organisationnelle et résilience numérique.

Pour conclure, il est possible d'ouvrir deux pistes de réflexion. La première concerne la nécessité d'élargir la recherche académique sur les conditions concrètes d'émergence d'auditeurs hybrides, capables de conjuguer expertise technique et compétence de gouvernance. La seconde touche à la perspective d'une certification externe du risque cyber, comparable au rôle des commissaires aux comptes, qui pourrait constituer une avancée décisive dans la reconnaissance du cyber comme un enjeu de confiance sociétale. Ainsi, cette étude contribue à éclairer un mouvement en cours : celui d'une fonction d'audit interne en transformation, confrontée à la montée inexorable du risque cyber et appelée à devenir l'un de ses leviers les plus crédibles d'atténuation.

Annexes

A - Entretien n°1

Participants : Auditrice interne (Entreprise Cité Marine – 10 ans d'expérience dans le secteur agroalimentaire industriel) et Titouan Boyard

Date : 10 août 2025

Durée : 45 minutes

Lieu : Cadre privé

Introduction

Dans le cadre de notre étude sur l'intégration de la cybersécurité dans les missions d'audit interne, nous avons échangé avec une auditrice interne de Cité Marine, entreprise spécialisée dans les plats à base de poisson et de légumes cuisinés, en frais et surgelé. Cet entretien a été réalisé en présentiel par Titouan Boyard. Ce dernier visait à comprendre comment une entreprise industrielle, dont les priorités sont historiquement centrées sur la qualité et la sécurité alimentaire, aborde aujourd'hui le risque cyber dans ses processus de gouvernance et de contrôle interne.

Perception et évolution de la cybersécurité dans un contexte industriel

L'auditrice explique que, sur la dernière décennie, la cybersécurité a connu une progression mesurable depuis plusieurs années, notamment après le COVID-19. Mais qu'elle n'a jamais constitué une priorité stratégique au même titre que dans les secteurs bancaires ou purement digitaux. Chez Cité Marine, les efforts se sont concentrés sur d'autres aspects IT comme la modernisation de l'ERP, la mise en place de pare-feu, la protection contre le phishing et quelques campagnes de sensibilisation des salariés. En fait, la direction voit dans le risque cyber une menace sérieuse mais secondaire par rapport aux enjeux sanitaires : une attaque pourrait perturber la production ou retarder les livraisons mais elle n'aurait pas le même impact structurel que dans d'autres secteurs fortement numérisés.

Rôle et positionnement de l'audit interne sur le risque cyber

L'audit interne n'est pas trop perçu comme un acteur central de la maîtrise du risque cyber. Le rôle de pilotage incombe à la DSI et à un prestataire externe spécialisé (ACCEIS), l'audit jouant

un rôle ponctuel de ”regard tiers” ou de relais pour faire passer des informations du ”top management” aux opérationnels. Les attentes de la direction sur ce sujet ont donc évolué de manière indirecte : lors de missions opérationnelles, Cité Marine intégre parfois des vérifications liées aux accès et à l'ERP. L'auditrice illustre cela par un cas concret où un employé, pourtant rattaché à la Supply Chain, disposait de droits lui permettant de modifier les montants des bons de commande ; un ajustement de la configuration ERP a été demandé à la DSI pour y remédier.

Outils, référentiels et bonnes pratiques

Dans le contexte de l'activité de Cité Marine, aucun référentiel purement cyber tel que COBIT ou ISO 27001 n'est utilisé. Les audits reposent sur des référentiels qualité comme ISO 22000 ou IFS Food, avec quelques contrôles transposables à la cybersécurité (gestion des accès, sauvegardes). L'auditrice souligne qu'elle n'a pas accès en autonomie aux indicateurs cyber : toute information est obtenue via la DSI sur demande. Elle insiste sur l'intérêt de continuer à intégrer des points cyber dans les audits existants plutôt que de créer des missions entièrement dédiées. Pour elle, il existe aussi une forte nécessité de former les auditeurs aux menaces les plus courantes (phishing, gestion des accès).

Freins, limites et perspectives d'amélioration

Les principales limites résident dans le manque de formation technique des auditeurs. En effet la complexité du langage IT et un cloisonnement persistant entre audit interne et DSI rend compliqué la possibilité de formation en interne et donc la montée en compétence des équipes sur des sujets clefs comme ceux-là. L'entreprise applique des pratiques ”sur mesure” plutôt qu'une conformité stricte aux standards internationaux car ces derniers sont jugés trop lourds pour une structure de cette taille et de ce secteur. L'auditrice recommande notamment la mise en place d'un comité régulier (tous les quatre à six mois) entre la DSI et l'audit pour partager incidents et bonnes pratiques, tout en évitant de surcharger les équipes IT. Elle estime qu'un modèle plus intégré audit–cyber est envisageable chez Cité Marine mais seulement si proportionné à l'activité et impulsé par la direction générale («tone at the top ”), avec une implication de l'audit en amont de certains projets IT.

Conclusion

Cet entretien met en lumière la réalité d'une entreprise industrielle où la cybersécurité est

présente comme dans tous les secteurs en 2025 mais pas prioritaire. Les actions menées sont pragmatiques et proportionnées au risque perçu, la DSI et le prestataire externe de cybersécurité portant l'essentiel de la responsabilité. L'audit interne y contribue de manière ciblée, principalement via des audits métiers intégrant ponctuellement des points cyber. Les pistes d'évolution identifiées concernent la formation des auditeurs, l'amélioration de la communication avec l'IT ou encore l'instauration d'une gouvernance partagée sur le risque cyber, adaptée à la culture et aux moyens de l'entreprise.

B - Entretien n°2

Participants : Guillaume Litvak - Directeur Exécutif Audit Interne et Risques Groupe Carrefour et Titouan Boyard

Date : 30 juin 2025

Durée : 45 minutes

Lieu : Siège du Groupe Carrefour – Massy (91)

Introduction

Dans la continuité de nos travaux de recherches, nous avons échangé avec le Directeur Exécutif Audit Interne et Risques Groupe interne de Carrefour, Guillaume Litvak. Carrefour étant acteur majeur de la grande distribution en France et à l'international, il nous semblait pertinent de pouvoir discuter avec un professionnel expérimenté comme Guillaume. Cet entretien, conduit par Titouan Boyard, visait à comprendre donc comment une organisation de cette ampleur aborde le risque cyber, perçu comme stratégique. L'objectif était aussi de comprendre comment l'audit interne adapte ses pratiques face à cette menace croissante. L'entretien a également permis d'explorer les liens entre les acteurs clefs de l'atténuation des risques comme la cybersécurité Groupe et la manière dont la structuration des lignes de défense est faite chez Carrefour.

Un risque croissant et intégré dans la stratégie d'audit

Guillaume souligne que le risque cyber n'a cessé de croître ces dernières années, jusqu'à devenir un axe incontournable du plan d'audit chez Carrefour. Face à cette menace carrefour a fait le choix de renforcer ses équipes en allant chercher des experts dédiés et notamment à l'étranger. Carrefour étant un groupe international, il est coutume de recruter des profils talentueux dans les pays pour les faire monter au niveau du Groupe en France. Ces profils doivent être capables de bâtir un véritable plan d'audit cyber. Ce dernier repose sur l'identification de thématiques clés et sur une approche dynamique : chaque année, des sous-thématiques sont explorées en fonction de l'évolution des menaces. Les attaques par phishing, considérées comme critiques chez Carrefour, ou encore les fraudes au président déjà rencontrées dans l'organisation, constituent des exemples concrets de la matérialisation du risque. Guillaume souligne également l'émergence de menaces plus sophistiquées, comme

l'imitation de la voix et de l'image, qui renforcent la nécessité d'une vigilance accrue. Ces menaces se caractérisent aussi et surtout par l'utilisation de l'intelligence artificielle qui rebat toutes les cartes du jeu de protection contre ces risques.

Renforcement des lignes de défense et intégration du "cyber by design"
L'entretien a mis en évidence l'importance de la structuration des lignes de défense pour mieux adresser le risque. La deuxième ligne de contrôle (Contrôle interne Groupe et entités) s'appuie notamment sur les cadres NIST et NIS2, avec un dispositif extrêmement mature qui combine auto-évaluations et tests d'intrusion. Ce dispositif est animé par le CISO du Groupe, en lien avec les RSSI locaux et les référents cybersécurité dans les différentes entités. L'audit interne vient compléter ce mécanisme en assurant la cohérence et l'efficacité des travaux, s'inscrivant dans une logique de coordination. L'intégration de la cybersécurité «by design ", c'est-à-dire dès les phases amont des projets IT, est également présentée comme une priorité. Cela est de plus en plus fait au sein du Groupe et permet de s'assurer d'une certaine protection contre ces risques. Cela permet aussi d'éviter que la sécurité ne soit perçue comme un frein mais plutôt comme une composante naturelle du développement et de la transformation numérique d'un groupe comme Carrefour.

Positionnement organisationnel et enjeux de gouvernance
Guillaume insiste sur le positionnement institutionnel de la fonction cybersécurité. Une avancée importante a été la séparation des rôles entre la DSI et le CISO, garantissant une indépendance et étant en lien avec les recommandations des standards internationaux de gouvernance. Le CISO bénéficie donc d'un double rattachement, à la fois auprès de la direction générale (hiérarchique) et de la DSI (fonctionnel), afin d'assurer un reporting équilibré. L'audit interne a joué un rôle clé pour pousser cette clarification, considérée comme un levier de maturité. Par ailleurs, Guillaume souligne que la réglementation (notamment DORA pour les activités bancaires) impose désormais un renforcement de la gouvernance cyber, ce qui accélère la mise en place de ces dispositifs.

Compétences et perspectives d'évolution
L'audit interne, pour être crédible sur ces sujets, doit impérativement disposer de compétences spécifiques en cybersécurité comme le recommandent d'ailleurs les normes internationales. Carrefour a fait le choix d'investir dans la montée en compétences de ses collaborateurs, avec

un dispositif de formation continue (par exemple, une heure par mois consacrée à la cyber, ou parfois des journées de formation banalisées). La population relativement jeune des équipes d'audit interne facilite aussi cette dynamique d'apprentissage, même si la complexité technique reste un frein. L'approche consiste à compléter les compétences généralistes des auditeurs par des "briques cyber", afin de garantir un niveau minimal de maîtrise pour pouvoir réaliser efficacement les missions. Néanmoins, l'appuie sur des experts, notamment externes reste nécessaire pour les points les plus techniques.

Conclusion

Cet entretien montre que Carrefour a pleinement intégré la cybersécurité comme un risque stratégique. Ce risque nécessite une réponse organisationnelle et technique adaptée. Le rôle de l'audit interne est donc double : d'une part, accompagner et challenger la mise en œuvre des dispositifs (plans d'audit, questionnaire d'auto-évaluations, tests) et d'autre part, s'assurer que les compétences internes évoluent en cohérence avec les attentes. La clarification des rôles entre la DSI et le CISO, ainsi que l'intégration de la sécurité «by design" dans les projets IT, illustrent une maturité croissante et performante. Les perspectives futures reposent sur un équilibre entre expertise technique spécialisée et acculturation progressive de l'ensemble des auditeurs internes.

C - Entretien n°3

Participants : André Luis Antunes - Directeur Audit IT, data et cyber Groupe Carrefour et Titouan Boyard

Date : 24 juillet 2025

Durée : 45 minutes

Lieu : Siège du Groupe Carrefour – Massy (91)

Titouan. – Bonjour André, comment vas-tu ?

André. – Hello Titouan, ça va super et toi ?

Titouan. – Nickel. Merci de m'accorder un peu de temps aujourd'hui. Je vais te poser quelques questions afin d'avoir ta réflexion sur la cyber chez Carrefour et les liens avec l'audit.

André. – Ca marche, je t'écoute.

Titouan. – Pour commencer, est-ce que tu pourrais me dire comment la cybersécurité a évolué dans ton organisation au cours des dix dernières années ?

André. – Franchement, ça a été un chemin assez particulier. Quand j'étais à Carrefour Brésil, la cybersécurité n'était pas du tout au centre des priorités. Au niveau du Comex, ce n'était pas un sujet qui faisait vibrer, c'était un peu relégué au second plan derrière les problématiques purement opérationnelles. Mais il y a quand même eu un déclic quand l'audit interne a mis en place une évaluation basée sur le référentiel NIST. Là, ça a forcé les dirigeants à regarder le sujet de plus près, à se rendre compte qu'il y avait de vraies failles et qu'il fallait se mettre à niveau.

Ensuite, en arrivant au sein du Groupe, je pensais que la situation serait radicalement différente mais en fait… pas tant que ça. Dans la grande distribution, on reste focalisés sur la logistique, la supply chain et la satisfaction client. La cybersécurité n'est pas perçue comme un risque vital, contrairement à ce que tu peux voir dans le secteur bancaire par exemple. Alors, bien sûr, de temps en temps, quand on remonte des vulnérabilités ou qu'il y a un incident un peu visible, le sujet revient sur la table. Mais c'est très fluctuant : tu as des périodes où ça monte très haut

dans les priorités, puis ça retombe aussitôt. Et puis il y a cette difficulté : comme le risque cyber est rarement concret pour les dirigeants – ça ne se matérialise pas comme un incendie ou un problème sanitaire – et bien c'est compliqué de leur faire prendre conscience de son importance et surtout de leur faire comprendre qu'il faut dépenser de l'argent pour se prémunir d'une menace invisible.

Titouan. – Donc pour toi, ça reste quand même un risque stratégique ?

André. – Pour moi, oui, clairement. Tu prends le phishing, les ransomwares… ce sont des menaces qui peuvent paralyser les opérations en un rien de temps. On a déjà eu un cas de fraude au président, ce n'est pas courant mais ça prouve que ça peut arriver. Le problème, c'est que les instances dirigeantes n'ont pas ce niveau de lecture. Je te donne un exemple concret : aujourd'hui, si un membre du Comex n'utilise toujours pas de double authentification, ça comporte un risque très très critique pour nous. Et la politique de changement de mots de passe n'est pas appliquée comme elle devrait l'être, à la même échelle à travers le Groupe. Ça montre bien qu'il n'y a pas de "tone at the top" ou en tout cas un manque dans cette impulsion du "top management". Tant que le message n'est pas impulsé au sommet, les bonnes pratiques ne descendent pas.

Titouan. – Oui, je comprends, c'est un peu comme si l'exemple ne venait pas d'en haut.

André. – Exactement. Tu peux avoir les meilleures politiques écrites mais si le dirigeant lui-même ne s'impose pas ces règles, le reste de l'organisation ne va pas les suivre non plus.

Titouan. – Et l'audit interne, dans tout ça, a-t-il vu ses attentes évoluer de la part du management ?

André. – Pas énormément, à vrai dire. On est souvent dans une posture réactive plutôt que proactive. Je prends l'exemple du projet SmartPOS (projet de logiciel pour les systèmes de caisses des magasins, développé en interne par Carrefour) : la cybersécurité n'a pas été intégrée dès la conception. Résultat : certains systèmes de caisse tournaient avec un mot de passe identique. Tu imagines l'ampleur du risque ? Et pourtant, ce n'était pas un sujet pour la direction. L'audit interne a été consulté mais trop tard, un peu comme si on venait chercher un avis extérieur sans nous inclure vraiment et surtout à posteriori. C'est ce que j'appelle la logique du "poulet et du cochon" : on consulte le poulet mais ce n'est pas lui qui est impliqué. Le

problème, c'est que ni la première ligne, ni la deuxième ligne ne prennent suffisamment conscience de la gravité des enjeux cyber. Et du coup, on se retrouve sans contrôle via les questionnaires d'auto-évaluation, avec des DRP qui existent sur le papier mais dont on ne sait pas vraiment évaluer l'efficacité.

Titouan. – D'accord. Et quand vous réalisez des audits, quels sont les référentiels ou outils que vous utilisez concrètement ?

André. – On s'appuie beaucoup sur le NIST mais aussi sur des référentiels comme MITRE et OWASP.

Titouan. – Excuse-moi, tu peux me rappeler ce que c'est, MITRE ?

André. – Bien sûr, c'est ce que j'avais présenté à Skema durant la conférence avec Mathieu Gras. MITRE, c'est une organisation américaine qui a développé le cadre ATT&CK. C'est une sorte de matrice qui répertorie toutes les techniques connues d'attaque utilisées par les cybercriminels. Ca permet aux organisations de se situer par rapport à ces scénarios et de voir si elles ont mis en place les défenses adaptées. C'est hyper concret parce que ça s'appuie sur l'observation des menaces réelles.

Titouan. – D'accord et OWASP alors ?

André. – OWASP, c'est l'Open Web Application Security Project. C'est une communauté mondiale qui publie notamment le fameux "Top 10", une liste des dix vulnérabilités applicatives les plus critiques. C'est devenu une référence pour tous ceux qui développent ou auditent des applications web, parce que ça permet d'identifier les failles les plus courantes et de les corriger.

Titouan. – Ok, je vois mieux, merci.

André. – Après, on utilise aussi des outils open source, parfois même PowerBI pour faire des analyses rapides. Et puis, on a un logiciel de gestion des accès qui nous permet d'identifier très précisément qui a le droit d'accéder à quoi. Par exemple, sur les données personnelles, on met en place des niveaux de chiffrement et des droits spécifiques pour le déchiffrement. Donc oui, on a une certaine visibilité mais c'est très dépendant des ressources qu'on y met.

Titouan. – Et les outils d'automatisation, vous en utilisez aussi ?

André. – Oui mais à petite échelle. On fait des scripts en Powershell, parfois en utilisant l'IA générative pour accélérer le développement. Et encore une fois, beaucoup d'outils open source. Le problème, c'est que tu peux avoir les bons outils, si tu n'as pas les bonnes compétences derrière, ça ne sert à rien. Et c'est là qu'on voit les limites de l'audit interne classique. Former un auditeur à la cyber, ça marche rarement : c'est trop complexe. Par contre, quand tu prends un expert cyber et que tu le formes à l'audit, ça fonctionne beaucoup mieux. Au Brésil, on avait fait ça et ça donnait des résultats.

Titouan. – Donc en gros, la marche est trop haute dans un sens mais pas dans l'autre.

André. – Exactement. Et du coup, ce qui arrive souvent, c'est qu'on sous-estime le risque. On sort un rapport avec un "risque moyen" alors que c'est clairement un risque élevé. Et si derrière, le Comex n'est pas aligné, ça ne change rien.

Titouan. – Et par rapport aux référentiels comme ISO 27001 ou COBIT, est-ce que vous êtes en ligne ?

André. – Sur le papier, oui. Les procédures sont carrées. Mais quand tu les compares vraiment aux standards, tu vois vite l'écart. C'est un peu le jour et la nuit entre la théorie et la réalité.

Titouan. – Et si on se projette, est-ce qu'un modèle d'audit plus intégré avec la cybersécurité est possible selon toi ?

André. – Oui, je pense. Mais il faut le construire intelligemment. Avec des partenariats, par exemple avec des fournisseurs comme IBM, tu peux aller beaucoup plus loin. Mais il y a aussi une dimension éthique. Aujourd'hui, dans certaines missions menées par les Big Four, tu te retrouves avec des stagiaires qui gèrent des sujets critiques. Tu vois le paradoxe. Ce n'est pas seulement une question de budget, c'est aussi une question de volonté d'évoluer et d'éthique professionnelle. Et ça, pour moi, c'est le vrai frein. Tu vois bien le niveau de risque… Pour moi, ce n'est pas qu'une question d'argent, c'est aussi une question humaine : on est réticents au changement, on n'a pas envie de s'adapter. Et tant qu'on ne règle pas ça, ça restera compliqué.

Titouan. – Donc pour toi, le frein, c'est moins la technologie que la culture ?

André. – Complètement. La techno, tu la trouves. Mais la volonté de changer… c'est une autre histoire.

Titouan. – Ecoute André, je n'ai pas plus de questions. Merci beaucoup pour ton temps et tes réponses !

André. – Merci à toi c'était très intéressant de discuter de ces sujets là avec toi.

Titouan. – Bonne fin de journée.

André. – Merci à toi aussi !

D - Entretien n°4

Participants : Christophe Pernot - Délégué à la protection des données Louvre Hôtels Group (LHG) et Violette Blanchard

Date : 28 juillet 2025

Durée : 45 minutes

Lieu : Teams

Introduction

Dans la continuité de nos travaux de recherche, nous avons échangé avec le Délégué à la protection des données de LHG, Christophe Pernot. Louvre Hôtels Group étant acteur majeur de l'hôtellerie en France et en Europe, il nous semblait pertinent de pouvoir discuter avec un professionnel expérimenté comme Christophe. Cet entretien, conduit par Violette Blanchard, visait à comprendre donc comment une organisation de cette ampleur aborde le risque cyber, perçu comme stratégique. L'objectif était aussi de comprendre comment une entreprise en contact constant avec des données clients adapte ses pratiques face à cette menace croissante. L'entretien a également permis d'explorer comment l'audit interne et la délégation de la protection de données collaborent.

Perception et évolution de la cybersécurité dans un contexte de service

Christophe indique que le groupe a rapidement pris au sérieux les menaces cyber auxquelles le groupe pouvait faire face. Le groupe n'a pas attendu la réglementation sur le RGPD pour mettre en place des contrôles et une équipe pour évaluer les risques cyber de l'entreprise. Selon Christophe, cela a du sens et car si le LHG venait à être attaqué, cela créerait une grosse interruption de l'activité du groupe, comme le COVID a pu l'être. Les enjeux auxquels le groupe doit faire face ont évolué avec la diversité des attaques dont les équipes pouvaient entendre parler et avec l'utilisation de certains logiciels. Les attentes sur le sujet de la cybersécurité sont élevées au sein du Top Management car l'un des membres du COMEX fait partie des équipes IT. Christophe est régulièrement consulté pour donner son opinion avant la mise en place de projets ou de nouveaux outils, par tous services confondus. Cela montre l'importance du sujet au sein du siège.

Les attaques au président, ransomware, phishing ou APT sont aujourd'hui plus que jamais des risques stratégiques pour le groupe qui traite énormément de données chaque jour. Cela représente un risque pour la réputation du groupe, pour l'actionnaire et parfois même pour les assurances. Christophe évoque notamment que les personnes qui ne travaillent pas dans le secteur de l'hospitalité connaissent mal Louvre Hôtels Group mais plutôt les marques d'hôtels. Cela peut être un avantage car en cas d'une attaque cyber importante, cela peut protéger la réputation du groupe.

Evaluation du niveau de sécurité informatique

L'entretien a mis en évidence que le groupe ne fait pas appel à l'audit interne pour évaluer la sécurité informatique ni même pour l'évaluation des risques. Ces deux éléments sont réalisés directement au sein des équipes IT et de la délégation de la protection de données. Néanmoins, des personnes au sein des équipes IT sont dédiées à évaluer les processus liés à la cybersécurité au sein du siège. ISO 27001 est la norme utilisée au siège pour évaluer les processus liés à la cybersécurité. Des outils sont également utilisés au siège en cas de défaillance. Christophe mène de son côté des audits sur ces sujets au sein des hôtels.

Christophe indique que l'entreprise utilise un outil afin d'assurer que les comptes ne soient pas partagés par plusieurs personnes dans l'entreprise et ne sont pas connectés sur plusieurs postes de travail. Cet outil permet d'assurer un certain niveau de sécurité informatique car les employés n'ont pas les mêmes niveaux d'accréditations en fonction de leur poste. De ce fait, l'outil permet de savoir si des comptes sont connectés sur plusieurs postes. Également, les outils utilisés permettent de bloquer les mots de passe non conformes aux recommandations de la CNIL.

Freins ou limites rencontrés

Christophe explique qu'il y a plusieurs freins comme le manque de formation, le cloisonnement avec les équipes IT. Ces freins font que lors des audits qu'il réalise dans les hôtels, il passe du temps à éduquer les membres du personnel pour éviter d'avoir des faiblesses humaines dans la protection des données mais également de manière générale pour les risques cyber. Il a su avec les années casser les silos entre la délégation de la protection des données, dont il fait partie et les équipes IT avec qui il travaille aujourd'hui pour gérer les risques cyber. L'autre frein auquel

l'entreprise fait face est le manque de temps au quotidien, qui fait que de temps en temps des contrôles sont faits moins régulièrement.

Cependant, selon Christophe, les recommandations des référentiels et les standards ne sont pas des freins ou une limite. La réalité terrain s'accorde bien avec les demandes réglementaires. Typiquement, il a pris le temps de faire une fausse communication en interne afin d'éveiller les consciences lorsqu'il a fallu mettre en place les RPA et les PCA au sein des entreprises. Cela a permis de répondre aux réglementations tout en poussant l'ensemble des personnes concernées à s'engager et à le faire correctement et rapidement.

Compétences et perspectives d'évolution

Afin d'être un acteur crédible sur les sujets cyber, les auditeurs internes doivent combler le manque de connaissances sur les normes, réglementations et compréhension des sujets cyber. Selon Christophe, ce qui manque le plus aux auditeurs internes est souvent la connaissance technique des structures informatiques, comment les informations sont protégées, comment elles passent d'un outil à un autre. Il considère que les équipes doivent se former sur le terrain et pas uniquement dans les réglementations car avant de vouloir évaluer/auditer, il faut comprendre ce qui est en face de nous.

En plus de la compréhension des systèmes informatiques, il faut créer une cohésion, une confiance entre les équipes IT et d'audit interne avant d'envisager une collaboration. Il considère toutefois qu'un auditeur IT qui a une vraie compréhension des enjeux informatiques et pas uniquement des structures de systèmes serait l'idéal. Aujourd'hui il considère qu'une collaboration entre les équipes IT et d'audit interne serait trop difficile pour plusieurs raisons comme le manque de temps et de personnes.

Conclusion

Cet entretien montre que Louvre Hôtels Group a pleinement intégré la cybersécurité comme un risque stratégique. Ce risque nécessite une réponse organisationnelle et technique adaptée. Le rôle de Christophe en tant que DPO est donc double : d'une part, accompagner et challenger la mise en œuvre des dispositifs réglementaires au sein des hôtels du groupe et d'autre part, faire la passerelle entre les équipes IT et les autres services au sein du siège. Il est également un soutien des équipes IT pour les études de faisabilité des projets internes. Les perspectives futures reposent sur une éducation des employés et de l'équipe d'audit interne sur les sujets

cyber et une collaboration progressive entre les équipes IT en charge des risques cyber et l'équipe audit interne qui a la rigueur et les méthodes d'audit, afin de créer un équilibre entre expertise technique et rigueur d'audit et de gestion des risques.

E - Entretien n°5

Participants : Guillaume Cécile - Chief Information Security Officer Groupe Carrefour et Titouan Boyard

Date : 21 août 2025

Durée : 1h

Lieu : Siège du Groupe Carrefour – Massy (91)

Introduction

Guillaume est l'un des Chief Information Security Officers (CISO) du Groupe Carrefour. Il est en charge des opérations de sécurité à l'échelle du groupe, ce qui implique un rôle central dans le maintien en condition opérationnelle des outils de cybersécurité ainsi qu'une supervision globale sur ce qui se passe derrière ces dispositifs. Sa mission s'appuie sur trois équipes distinctes : l'une dédiée au fonctionnement quotidien des outils, une autre à la protection des données et la dernière à la gestion des vulnérabilités cyber. Fort de plus de vingt ans d'expérience dans le secteur du retail, d'abord sur les infrastructures IT puis sur la cybersécurité, Guillaume a également assuré par intérim la fonction de chef des CISO Groupe pendant plusieurs mois en 2025. Son expertise lui confère donc une vision stratégique et opérationnelle des enjeux cyber dans un environnement aussi vaste et complexe que celui de Carrefour.

Évolution des menaces et perception stratégique

Selon Guillaume, les menaces auxquelles Carrefour fait face ont considérablement évolué au cours des dix dernières années. Il y a cinq ou six ans, les principaux risques concernaient des attaques de type défaçage (prise de contrôle d'un site internet pour en modifier l'apparence) ou encore des intrusions dans les réseaux avec parfois pour objectif la destruction de données. Ces menaces étaient d'une nature différente de celles observées aujourd'hui car désormais, l'extorsion de fonds et les attaques par ransomware représentent la menace principale. Le scénario craint est clair : extraction massive de données sensibles, paralysie du réseau et arrêt des activités, comme cela a déjà frappé de nombreuses entreprises en France et en Europe. Ces attaques peuvent compromettre durablement la continuité de l'activité et entraîner des pertes

financières colossales ainsi que de nuire à la réputation du Groupe. A l'inverse, les attaques au président ou les tentatives de phishing sont considérées comme des risques secondaires. Elles existent mais leur gravité est jugée moindre et la réponse à ces risques repose surtout sur de l'information et de la prévention auprès des équipes.

Perception et attentes des dirigeants

Chez Carrefour, le "top management" a conscience de l'importance des menaces cyber mais cette compréhension reste en grande partie liée au langage financier. Les impacts potentiels d'une attaque sont entendus et pris au sérieux. En revanche, les aspects plus techniques, apparaissent trop terre-à-terre pour une partie des dirigeants qui n'ont pas de bagage technique.

Guillaume explique donc que les arbitrages budgétaires constituent un défi majeur. Le discours récurrent est celui du "trop d'outils" en cybersécurité, avec la difficulté pour les équipes cyber de démontrer un retour sur investissement clair. La menace étant diffuse et évolutive, il est complexe de convaincre les instances dirigeantes de financer de nouveaux projets. Pour parvenir à se faire entendre, Guillaume et les équipes de cyber illustrent souvent les menaces par des exemples concrets : en comparant le coût d'une assurance pour les risques cyber avec celui d'un nouvel outil, il devient plus simple de convaincre le management. Si l'implémentation de ce nouvel outil permet de réduire le montant de l'assurance, le gain est tangible et justifie donc la dépense. Cette logique de compromis montre bien la nécessité de parler le langage des décideurs.

Rôle et perception de l'audit interne

L'audit interne n'est pas perçu comme un acteur central de la cybersécurité par les équipes cyber mais plutôt comme un facilitateur. Guillaume explique qu'il joue un rôle d'aidant dans la formalisation de certains processus. L'audit est parfois perçu comme contraignant car il peut pointer du doigt des défaillances sensibles ou consommer trop de temps, il constitue quand même pour lui un levier puissant. Sa capacité à mettre en lumière des risques et à formuler des recommandations donne du poids aux équipes cybersécurité lorsqu'elles cherchent à faire avancer des sujets auprès des instances dirigeantes. L'audit interne permet ainsi de débloquer certaines discussions avec ces dernières en ajoutant un poids supplémentaire aux arguments déjà portés par la cyber, notamment via des plans d'actions qui sont un signal d'alarme.

Outils et référentiels

Carrefour adopte une stratégie pragmatique vis-à-vis de ses outils. L'approche privilégiée consiste à tester en premier lieu des solutions open source pour en évaluer la pertinence et l'efficacité. Puis si cela est concluant de passer à des versions premium plus robustes. Guillaume cite l'exemple du CNAPP (Cloud-Native Application Protection Platform), utilisé initialement dans une version open source pour vérifier la conformité des configurations cloud. Après centralisation et industrialisation, l'outil a été remplacé par une solution premium offrant une meilleure couverture des vulnérabilités (90 % contre 20 % auparavant). Un processus similaire a été suivi avec le SOAR (Security Orchestration, Automation and Response), qui permet de catégoriser les alertes et de gérer les faux positifs avant de les transmettre au SOC (Security Operation Center). Là encore carrefour a commencé par une solution open source avant de migrer vers un outil premium plus complet.

En matière de référentiels, le groupe se base principalement sur le NIST, utilisé chaque année pour auditer l'ensemble des Business Units (BU). Ce cadre est apprécié pour sa flexibilité et son caractère international. NIST permet aussi la comparabilité entre différents concurrents ou partenaires. Les normes ISO sont quant à elles jugées trop théoriques et lourdes pour le quotidien d'un acteur du retail.

Défis opérationnels

Parmi les principaux freins, Guillaume insiste sur le manque d'information et de sensibilisation des opérationnels. Par exemple, les collaborateurs en caisse ne mesurent pas toujours l'impact d'un incident cyber sur l'activité globale de l'entreprise. Cette méconnaissance entraîne parfois un manque de vigilance et augmente le risque d'erreurs humaines. Un autre défi tient aux indicateurs utilisés par l'audit. Les KPIs de l'audit continu, notamment sur le déploiement du MFA (Multi-Factor Authentication) ne reflètent pas forcément la réalité terrain. Même si ces chiffres peuvent être utiles ils ne sont pas exhaustifs. Guillaume rappelle aussi la nécessité de trouver un équilibre entre sécurité et fluidité opérationnelle. L'exemple du MFA est révélateur : imposer une authentification multifacteur trop stricte ralentit les opérationnels dans leurs tâches quotidiennes et les pousse parfois à contourner les règles. Dans un secteur comme la banque, ce niveau d'exigence est justifié mais dans la grande distribution, il peut devenir contre-productif.

Compétences manquantes chez l'audit interne

Pour Guillaume, les audits techniques tels que les pentests doivent rester de la responsabilité des équipes cybersécurité. L'audit interne ne doit pas devenir expert en hacking mais il doit monter en compétence sur les fondamentaux : distinguer un risque d'une menace, comprendre les grands principes de protection, dialoguer avec les experts sur un pied d'égalité. Cette montée en compétence permettrait aux auditeurs de mieux appréhender les enjeux et de challenger plus efficacement. Il rappelle aussi que ses propres équipes sont composées de profils variés : ingénieurs, anciens hackers, auditeurs IT… Cette diversité est un atout et il serait pertinent que l'audit interne développe au minimum une culture cyber afin de renforcer la qualité des échanges et la pertinence des constats lors des missions cyber.

Conclusion

Cet entretien avec Guillaume met en lumière l'évolution rapide et profonde des menaces cyber, passées d'attaques de visibilité à des tentatives d'extorsion massives capables de paralyser un groupe comme Carrefour. Le rôle de l'audit interne apparaît comme essentiel pour donner du poids aux équipes cyber dans leurs discussions avec le top management. Carrefour adopte une approche pragmatique en combinant outils open source et solutions premium et s'appuie sur le NIST comme référentiel structurant. Néanmoins, la sensibilisation des opérationnels et la montée en compétence des auditeurs internes restent des défis majeurs pour la cyber et l'audit. Pour Guillaume, la clé réside dans une collaboration renforcée où chacun joue son rôle : l'un comme garant de l'évaluation indépendante et l'autre comme expert technique. Ce tandem est déjà bien présent chez Carrefour mais gagnerait à être consolidé par une meilleure compréhension de la part de l'audit des spécificités des métiers liés à la cybersécurité.

F - Entretien n°6

Participants : Program manager au département CISO d'Amadeus S.A. et Violette Blanchard

Date : 2 juillet 2025

Durée : 1h

Lieu : Teams

Introduction

Dans le cadre de notre étude sur l'intégration de la cybersécurité dans les missions d'audit interne, nous avons échangé avec un senior program manager d'Amadeus SA, entreprise d'IT dans le secteur du voyage. Cet entretien est réalisé à distance par Violette Blanchard. Ce dernier visait à comprendre comment une entreprise d'envergure internationale appréhende les sujets cyber avec la complexité des différentes normes dans les différentes régions du monde.

Perception et évolution de la cybersécurité dans un contexte international
L'entreprise n'a pas attendu les réglementations pour s'interroger sur la cyber sécurité et comment y faire face. Il a été question de trouver une façon de protéger leurs données et ensuite de quels contrôles ils devaient mettre en place pour assurer une sécurité suffisante au groupe mais aussi aux clients. L'objectif était et est toujours aujourd'hui pour toutes les entreprises de répondre aux menaces qui sont raisonnables en termes de coûts et ensuite de protéger toutes les parties de l'entreprise. Notre interlocuteur évoque l'apparition des standards, normes et recommandations qui les ont aidés à structurer leur approche de la cybersécurité. Les risques cyber se sont multipliés depuis un peu plus de 10 ans aujourd'hui, ce qui a obligé cette entreprise à aller plus vite et plus loin dans la mise en place d'une structure pour protéger ses données. Selon notre interlocuteur, les grandes entreprises ont souvent davantage de facilités à répondre qualitativement aux standards à mettre en place que les plus petites entreprises. Cela vient de la dimension de l'entreprise et des coûts qu'elle est prête à engager pour ces sujets de cybersécurité.

Perception et attentes des dirigeants
Notre interlocuteur indique qu'une prise de conscience au plus haut niveau de l'entreprise est nécessaire. Cela s'est fait avec la réalité des choses dans les autres entreprises et avec les

standards et règlementations imposés aux entreprises. Les membres du Board ont des attentes importantes face à la cybersécurité car il s'agit de pouvoir livrer leurs services tout en protégeant les données des clients. Notre interlocuteur rappelle que plusieurs années en arrière, des entreprises ont été très florissantes jusqu'à une perte massive de leurs données, ce qui a fait souffrir ces entreprises, voire les faire disparaître. De ce fait, la prise de conscience est faite et il n'est pas question pour une entreprise telle qu'Amadeus d'avoir une perte de données car il en va de la confiance de ses clients et de leur réputation. La confiance de ces clients étant capitale pour l'entreprise, il est clair que le top management fait des choix permettant de mettre en place tout ce qui est possible pour assurer une cybersécurité solide.

Application des référentiels et normes

Amadeus a décidé d'être conforme à certains standards comme ISO 27001, NIS 2 mais aussi à PCIDCS qui est un peu plus spécifique à leur cœur de métiers. Ce deuxième standard a été créé par VISA et Mastercard ; c'est un standard de cybersécurité pour la protection des données de carte de crédit. Notre interlocuteur souligne la différence entre les standards et les réglementations imposées aux entreprises. Les réglementations les plus connues mises en place sont le RGPD et le CER. Le cadre réglementaire CER est axé sur la continuité d'activité, notamment en cas de cyberattaques mais également de pandémies comme le COVID, par exemple. L'entretien nous a permis également de comprendre que chaque pays ou région du monde a ses règlementations et standards, ce qui est parfois complexe pour les entreprises internationales comme Amadeus. L'entreprise étant espagnole, doit être conforme aux versions espagnoles des réglementations européennes comme le RGPD. Après la divulgation des réglementations européennes, les pays doivent ensuite traduire le texte en quelque sorte pour le faire appliquer dans leur pays. C'est pourquoi Amadeus est conforme à la version espagnole du RGPD, qui n'est pas très différente de la version française. L'application des normes demande parfois un travail de mapping pour assurer aux entreprises de bien répondre à tout ce qui leur est demandé dans chaque pays. Parfois, seuls les documents prouvant la conformité sont différents d'un pays à un autre.

Freins et limites

Il y a, selon notre interlocuteur, un manque d'accompagnement dans la mise en place des standards et réglementations, une potentielle distorsion sur le marché européen car certains pays s'autorisent des aménagements dans la transposition des lois. Le manque

d'accompagnement vient des autorités qui promulguent des lois parfois de haut niveau qui ne sont pas toujours simples à comprendre et qui nécessitent par la suite l'aide de certains cabinets pour mettre en place ces réglementations. La distorsion peut venir du fait que certains États européens vont simplement imposer dans leur pays le strict minimum pour appliquer la loi, quand certains pays vont ajouter des complexités. Il y a aussi des complexités techniques de mise en place des réglementations. Ce qui crée le laps de temps entre la publication d'une loi et sa mise en place. Tous ces éléments constituent des freins ou limites pour les entreprises dans leur conformité aux réglementations.

Collaboration entre l'audit interne et les équipes CISO

Aujourd'hui, les sujets de cybersécurité sont traités par les équipes CISO sans l'aide de l'audit interne. Les audits sont réalisés directement par les CISO qui ont leur propre gouvernance. Néanmoins, il arrive que ces deux corps de métiers travaillent ensemble dans le cadre d'une mission d'audit interne qui doit couvrir des volets cyber et qui se tourne donc vers les équipes CISO. Les auditeurs demandent donc une opinion ou de l'aide pour certains sujets. La collaboration se passe très bien entre ces deux services mais il n'est pas arrivé que les équipes CISO fassent appel à l'audit interne. L'équipe d'audit interne n'est pas assez au fait des notions de cybersécurité pour aujourd'hui faire des audits de conformité par exemple. Cependant, le département CISO réalise des audits de conformité, de manière continue pour couvrir les risques.

Conclusion

Cet entretien avec notre interlocuteur met en lumière l'évolution rapide et profonde de la cybersécurité. L'entretien nous permet également de saisir la complexité de la dimension internationale pour les entreprises qui doivent répondre aux réglementations de chaque pays dans lequel elles opèrent. La mise en place de certains standards est propre à l'industrie dans laquelle se trouve Amadeus, lorsque d'autres concernent simplement la cybersécurité. Ce qui ressort également est une collaboration relativement faible entre les équipes CISO et l'audit interne, bien que lorsque nécessaire tout se passe parfaitement.

G - Entretien n°7

Participants : Mathieu Gras Associé, Forensic & Integrity Services, France chez EY, Nabil Babaci Senior Manager Forensic & Integrity Services chez EY, Titouan Boyard et Violette Blanchard

Date : 18 juillet 2025

Durée : 1h

Lieu : Teams

Introduction

Mathieu et Nabil travaillent tous deux chez EY sur des sujets liés au forensic et à la cybersécurité. Mathieu, ingénieur télécom de formation, a passé seize ans dans le domaine des télécoms. Après avoir rejoint EY, il s'est progressivement orienté vers la fraude en raison de la volumétrie croissante des données à analyser. Il a également travaillé deux ans pour Roland Garros avant de rejoindre EY. Nabil a intégré EY en 2013, après une expérience en contrôle de gestion et en audit IT chez Deloitte. Spécialisé en forensic orienté fraude, il a développé une expertise solide dans la mise en place de reporting data et dans l'accompagnement des entreprises face aux enjeux de cybersécurité. Avec plus de douze ans d'expérience, il est un acteur majeur sur l'offre cyber et forensic du cabinet.

Évolution de la cybersécurité ces dix dernières années

Les deux experts soulignent à quel point la cybersécurité a profondément évolué. Pendant longtemps, elle était perçue comme un risque périphérique. L'objectif principal était de "construire la meilleure muraille" possible pour empêcher toute intrusion. Mais les mentalités ont changé : aujourd'hui, tout le monde sait que les attaques réussissent tôt ou tard et la question n'est plus de savoir si elles auront lieu mais plutôt quel en sera l'impact réel sur l'organisation.

Nabil insiste particulièrement sur la professionnalisation croissante du domaine, avec une structuration claire entre la blue team (les défenseurs) et la red team (les attaquants) au sein des organisations et des cabinets. Ces équipes se spécialisent dans des techniques précises, comme le vol de données ou la mise en place de "command & control" après une intrusion. Le

ransomware reste une menace importante mais il illustre surtout une tendance plus large : l'ubérisation du crime. Aujourd'hui, les attaques sont organisées via des messageries chiffrées (Telgram, Signal etc.) avec des acteurs qui se coordonnent pour revendre des données, parfois des mois après les avoir exfiltrées.

Il y a dix ans, la vision dominante en entreprise était centrée sur le hardware et les infrastructures. Désormais, les entreprises ont pris conscience de leur vulnérabilité à travers des attaques beaucoup plus simples : certaines intrusions ont été réalisées uniquement par téléphone portable. Ce changement a marqué un tournant dans la manière d'appréhender la cybersécurité.

Cybermenaces et risques stratégiques

Pour Mathieu et Nabil, le ransomware, autrefois perçu comme la menace majeure, tend à devenir secondaire : les attaquants privilégient désormais la revente de données sur les marchés parallèles comme expliqué plus tôt. Ce qui inquiète davantage, ce sont les vulnérabilités critiques (CVE), en particulier lorsqu'elles concernent des acteurs majeurs comme SAP ou Microsoft qui développent des outils et logiciels utilisés dans le monde entier.

La dimension géopolitique est aussi de plus en plus présente. Certains États peuvent chercher à exploiter ces vulnérabilités pour cibler des entreprises stratégiques. Nabil rappelle l'exemple des États-Unis, où même Donald Trump, qui était initialement sceptique quant à l'importance de financer les CVE, a fini par admettre leur rôle stratégique. Aujourd'hui, on observe un véritable "feu d'artifice de vulnérabilités" et la crainte que des puissances comme la Russie s'en emparent, notamment dans le cadre de guerre hybride avec l'UE. Nabil et Mathieu voit l'intelligence artificielle comme une arme à double tranchant : elle peut renforcer la défense des blue teams mais aussi amplifier la capacité d'attaque des red teams.

Concernant le fishing un exemple marquant partagé par les intervenants est celui d'un test de phishing réalisé auprès d'un Comex d'une grande entreprise. L'attaque simulée prenait la forme d'un lien promettant des chèques cadeaux. Résultat : même le CFO (Chief Financial Officer) de l'entreprise a cliqué, révélant à quel point la sensibilisation reste un défi majeur, même pour les plus hauts niveaux de l'organisation.

Attentes des dirigeants vis-à-vis de l'audit interne

Les attentes des dirigeants dépendent fortement du secteur et de la maturité de l'entreprise. La cybersécurité est désormais intégrée dans les cartographies de risques mais elle reste coûteuse. Les arbitrages budgétaires sont donc fréquents et les décisions de financement parfois difficiles à obtenir. Mathieu constate que les compétences en cybersécurité sont de plus en plus recherchées dans les directions mais que beaucoup restent encore focalisés sur les outils au détriment d'une vision plus globale. Nabil souligne le rôle croissant des réglementations, qui responsabilisent davantage les dirigeants et les engagent directement dans la gouvernance du risque cyber. Cette responsabilisation transforme la perception du risque cyber, en le reliant plus directement à la performance et à la conformité de l'organisation.

Perception de la fonction d'audit interne

Selon Nabil et Mathieu, l'audit interne n'est pas encore considéré comme un acteur central dans la maîtrise du risque cyber. Cette limite s'explique en grande partie par l'absence de compétences spécialisées des auditeurs. Cette incapacité à traduire les enjeux techniques en éléments de gouvernance. Aujourd'hui, la responsabilité opérationnelle demeure largement confiée au RSSI. Pourtant, une évolution se dessine : de plus en plus de missions intègrent des volets IT et cyber en étant appuyées de référentiels comme l'ISO 27001. Pour franchir un cap, il serait nécessaire de développer des fonctions dédiées à l'audit cyber et de créer des comités réunissant auditeurs et responsables de la cybersécurité. Cela permettrait de renforcer à la fois l'indépendance des travaux et le rôle du comité d'audit. Cette montée en puissance suppose aussi un investissement durable : Mathieu et Nabil estiment qu'un budget de l'ordre de 200 000 € par an permettrait de constituer une équipe interne réellement spécialisée, en capacité d'accompagner les entreprises face à l'évolution rapide des menaces et des technologies. Ils estiment que, tout comme les Commissaires aux Comptes (CAC) existent pour assurer la robustesse financière, il pourrait à terme émerger des "CAC IT/Cyber" pour attester de la robustesse numérique des entreprises.

Outils, méthodes et accès aux données

Les auditeurs d'EY s'appuient sur des référentiels comme l'ISO 27001 mais privilégient une approche pragmatique en allant au-delà des normes. Ils vérifient concrètement la gestion des incidents, la pertinence du traitement des alertes et l'efficacité des dispositifs. La plupart des clients disposent déjà d'outils tels que les EDR (Endpoint Detection and Response) ou les SOC

(Security Operation Centers) mais ceux-ci génèrent un volume massif d'alertes. L'enjeu est donc d'évaluer leur véritable efficacité : les alertes sont-elles traitées correctement, par les bonnes personnes et dans des délais adaptés ?

En complément, les auditeurs accèdent à certaines données et systèmes pour tester la robustesse de la sécurité. Sans mener de pentests complets, ils utilisent des techniques d'OSINT (Open Source Intelligence) afin de simuler des scénarios réalistes et repérer les vulnérabilités. Cette démarche, qui croise normes, outils et analyses ciblées, permet d'obtenir une vision opérationnelle et concrète du niveau de sécurité des organisations auditées.

Conclusion

Cet entretien met en évidence l'évolution rapide de la cybersécurité : d'un risque périphérique à une menace stratégique. Si la prise de conscience progresse, les entreprises restent limitées par leurs budgets et par le manque de compétences spécialisées. L'audit interne, encore en retrait, devra évoluer vers une intégration plus forte des enjeux cyber, portée à la fois par la réglementation et par une gouvernance plus impliquée.

H – Guide d'entretien des interviews

1. Synthèse des retours terrain

(Perceptions générales sur la montée en puissance du risque cyber / Évolutions observées dans les missions d'audit)

1) Comment la cybersécurité a-t-elle évolué dans votre organisation ces 10 dernières années ?
2) Diriez-vous que les cybermenaces (attaque au président, ransomware, phishing…) représentent aujourd'hui un risque stratégique pour votre entreprise ? Pourquoi ?
3) Avez-vous constaté une évolution des attentes des fonctions dirigeantes vis-à-vis de l'audit interne concernant les sujets cyber ?
4) Quelles missions d'audit interne menées récemment (dernier plan triennal/3 ans) intégraient directement la cybersécurité ? Quels étaient leurs objectifs et leurs conclusions ?
5) L'audit interne est-il aujourd'hui perçu au sein de votre entreprise comme un acteur clé dans la maîtrise du risque cyber ? Pourquoi (ou pourquoi pas) ?

2. Confrontation aux pratiques

(En quoi les outils et méthodes changent ? / Exemples de bonnes pratiques / Points de friction : compétences, collaboration, périmètre…)

6) Quels types d'outils ou de référentiels utilisez-vous pour auditer les processus liés à la cybersécurité ?
7) Avez-vous accès aux données, aux systèmes ou à des indicateurs spécifiques pour évaluer le niveau de sécurité informatique ?
8) Utilisez-vous des outils d'analyse de données, d'automatisation ou de cybersécurité dans vos missions d'audit ?
9) Quelles sont, selon vous, les bonnes pratiques pour intégrer efficacement la cybersécurité dans les missions d'audit interne ?

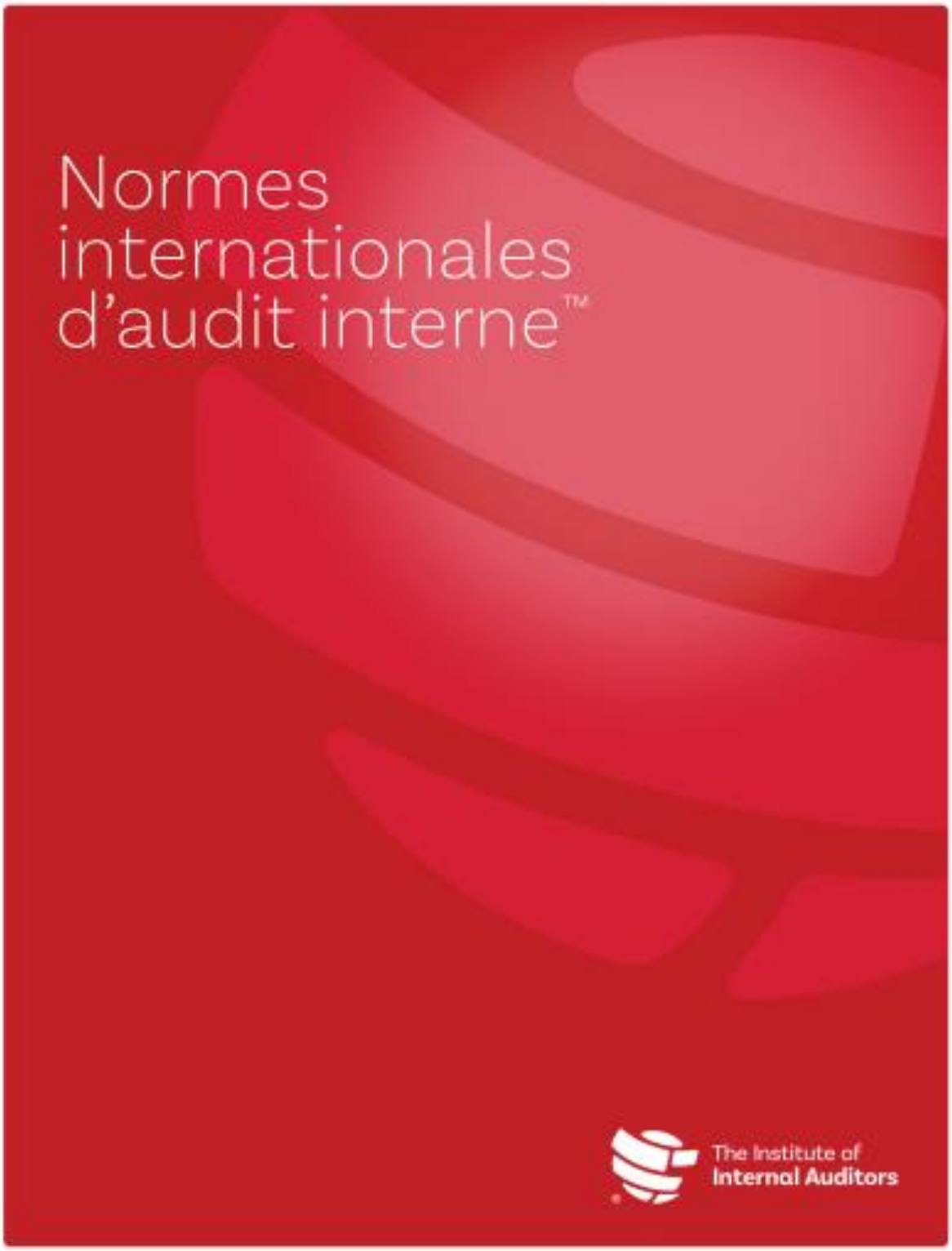
10) Quels sont les principaux freins ou limites que vous avez rencontré ? (Manque de formation, complexité technique, cloisonnement avec les équipes IT…)

3. Discussion croisée

(Analyse des écarts théorie/pratique / Quels leviers pour améliorer l'intégration cyber dans l'audit interne ? / Vers une vision "future-proof" de l'audit interne)

11) Pensez-vous que la réalité de terrain est conforme aux standards ou aux recommandations des référentiels (COBIT, ISO 27001, COSO etc.) ?
12) Y a-t-il un écart entre ce que les normes ou la littérature recommandent et ce que vous pouvez réellement appliquer ? Pourquoi ?
13) Quelles compétences spécifiques en cybersécurité sont, selon vous, les plus manquantes dans les équipes d'audit ?
14) Quelles seraient, selon vous, les évolutions nécessaires pour une meilleure collaboration entre audit interne et cybersécurité ?
15) À moyen terme, imaginez-vous un modèle d'audit plus intégré avec la fonction cybersécurité ? Quelles en seraient les conditions de réussite ?

I – Nouvelles normes d'audit interne (Source : IIA, 2024)



J – COSO 2017 Framework (Source : COSO, 2017)

COSO

Committee of Sponsoring Organizations of the Treadway Commission

Le management des risques de l'entreprise

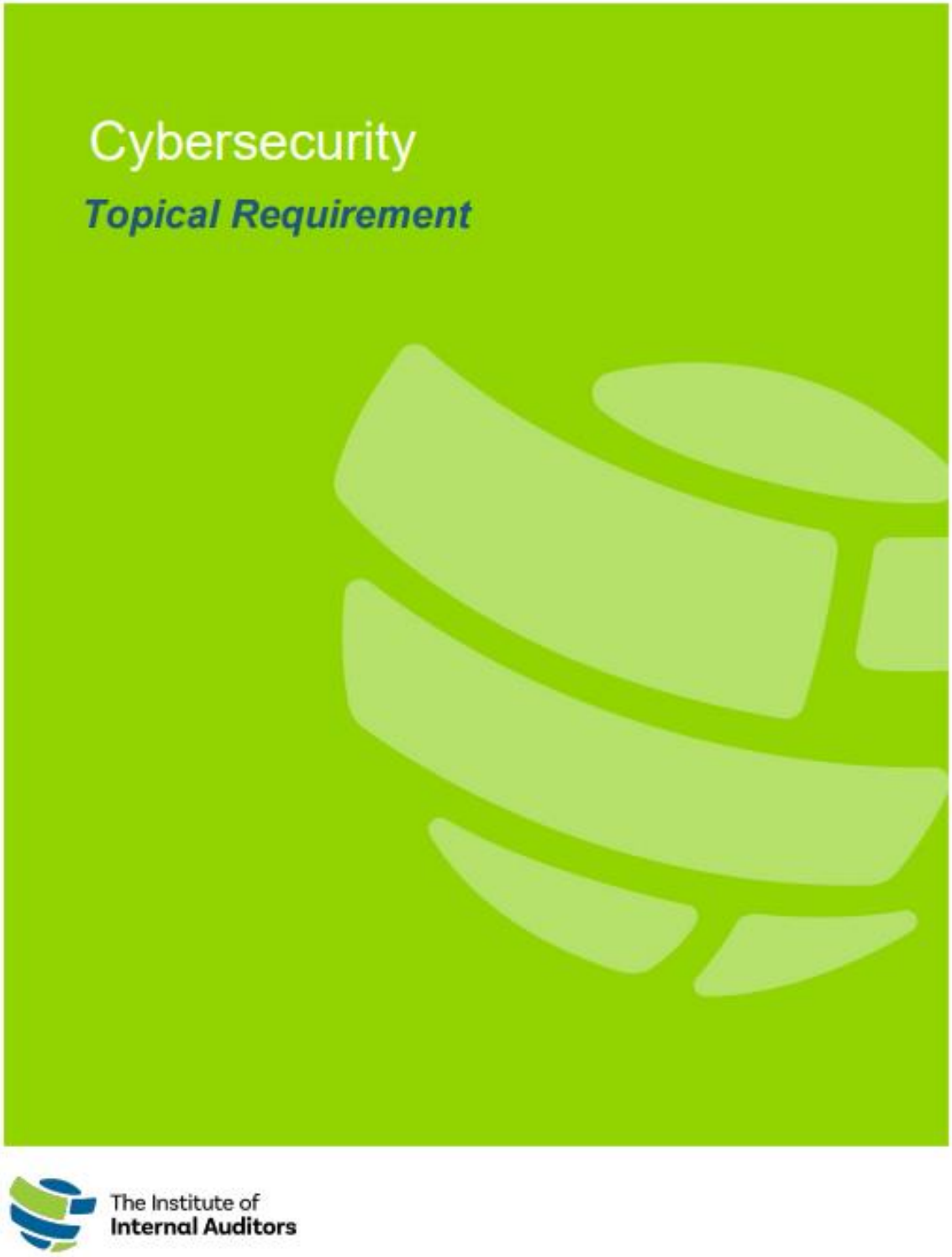
Une démarche intégrée à la stratégie et à la performance

Synthèse

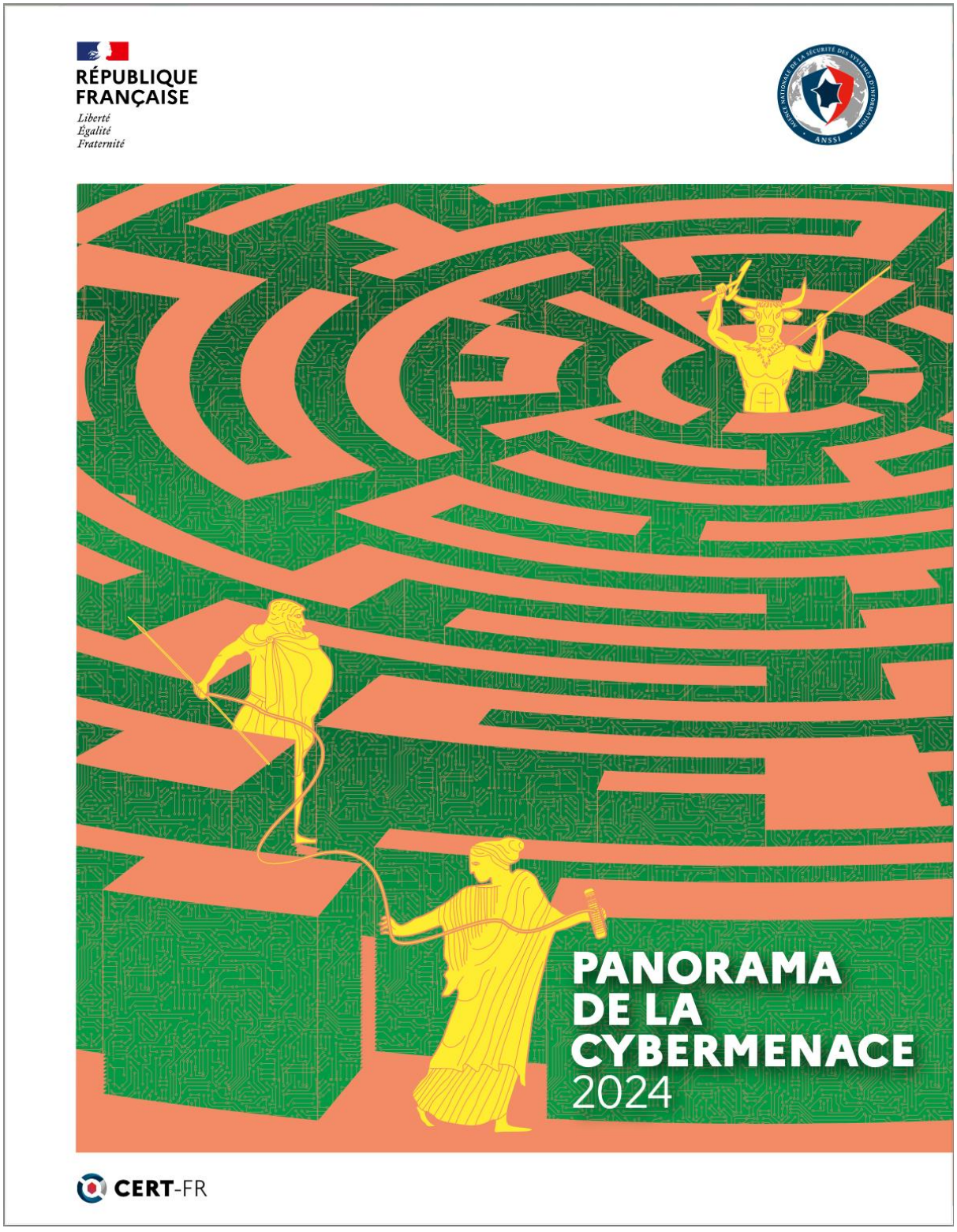
Traduit de l'anglais

Juin 2017

K – Cybersecurity Topical Requirement (Source : IIA, 2025)



L – Panorama de la Cybermenace (Source : CERT-FR, 2024)



Bibliographie

- Alem S., Ben Zekri Z. (2019). L'Impact des technologies de l'information et de la communication sur la prévention et la détection de la fraude dans le contrôle interne
- ANSSI (2025) Panorama de la cybermenace 2024. Récupéré le 28 juillet 2025, de https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf
- ANSSI (2025, 15 avril) Panorama de la cybermenace 2024 : mobilisation et vigilance face aux attaquants. Récupéré le 28 juillet 2025, de https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants
- Berretta E. (2025, 5 janvier) Pourquoi les hôpitaux français restent les cibles privilégiées des cybercriminels. Récupéré le 28 juillet 2025, de https://www.lepoint.fr/sante/pourquoi-les-hopitaux-francais-restent-les-cibles-privilegiees-des-cybercriminels-05-01-2025-2579223_40.php#11
- Bon-Michel B., Cappelletti L. (2025). La CSRD : un atout pour le contrôle interne
- Bubilek, O. (2017). Importance of Internal Audit and Internal Control in an organization - Case Study
- Clapaud, A. (2024). Cybersécurité Au Défi Des Nouvelles Menaces. Silicon, 18, 28–32.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). Internal Control – Integrated Framework.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). Enterprise Risk Management – Integrated Framework.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control – Integrated Framework (updated).
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management – Integrating with Strategy and Performance: Executive Summary.
- Crowe & IIA. (2018). The Future of Cybersecurity in Internal Audit. Internal Audit Foundation.

- Dauphine PSL & Grant Thornton. (2023). Quelle est la place de l'intelligence artificielle dans les pratiques d'audit interne ? Étude Grant Thornton & Université Paris Dauphine.
- Cybersecurity and the role of internal audit. (s. d.). Deloitte United States. https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/risk-advisory/2024/us-risk-cyber-ia-urgent-call-to-action.pdf
- ECIIA. (2018). Hot Topics 2018.
- ECIIA. (2019). 10 sujets incontournables pour le plan d'audit interne 2017.
- ECIIA. (2020). Risk in Focus 2020.
- ECIIA. (2023). Risk in Focus 2024: Hot topics for internal auditors.
- ECIIA. (2024). Risk in Focus 2025: Hot topics for internal auditors
- Explorer les nouveaux horizons technologiques : perspectives mondiales de l'audit interne IT (s. d.). KPMG. https://kpmg.com/fr/fr/insights/it/audit-interne-it-risques-technologiques.html
- Fülöp, M. T., Măgdaș, N., Ionescu, C. A., & Topor, D. I. (2024). Exploratory study on the use of CAAT and on the work environments of small and medium audit entities. Journal of East European Management Studies, 29(4), 696–722. https://doi.org/10.5771/0949-6181-2024-4-696
- Guemas, J. (2022, Janvier 31). AUDIT INTERNE. Récupéré sur Aix-Marseille Université : Explorer pour faire société : https://www.univ-amu.fr/fr/public/audit-interne
- Harisaiprasad K. (2020). COBIT 2019 and COBIT 5 comparison
- IFACI. (2005). Cahier de la recherche – L'auto-évaluation du contrôle interne.
- IFACI. (2025). Référentiel professionnel de l'audit interne – RPAI 2025. Institut Français de l'Audit et du Contrôle Internes.
- IIA. (2020). Modèle des trois lignes – Une mise à jour du modèle des trois lignes de défense (version canadienne-française). Récupéré le 28 juillet 2025, de https://theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-french-canadian.pdf
- IIA. (2024). Normes internationales pour la pratique professionnelle de l'audit interne. Récupéré le 28 juillet 2025, de

https://www.theiia.org/globalassets/documents/fr/documents/guidance/standards/2024/standards-2024-french.pdf

- Institut Français de l'Audit et du Contrôle Interne (IFACI). (2020). Guide des risques cyber IFACI 2.0. IFACI.
- IFACI Certification (2012). Référentiel professionnel de l'audit interne
- IIA (s. d.). Report on the Development and public consultation processes for the cybersecurity topical requirement
- Internal audit: key thematic areas to consider in 2025 (2024). KPMG. Récupéré de : https://assets.kpmg.com/content/dam/kpmg/au/pdf/2024/internal-audit-key-focus-areas-2025.pdf
- Jamison, J., Morris, L., & Wilkinson, C. (2018). The Future of Cybersecurity in Internal Audit. Internal Audit Foundation & Crowe.
- Ligaudan L. I. (2024). RGPD Le guide pratique. Éditions EMS
- Litvak, G., Marks, N., & Allaire, S. (2019). Guide de l'audit interne : Défis en enjeux - Théorie et pratique. Vuibert.
- Orange (2025, 28 juillet) Le groupe Orange annonce avoir déposé plainte lundi 28 juillet pour atteinte à un de ses systèmes d'information. Récupéré le 28 juillet 2025, de https://newsroom.orange.com/le-groupe-orange-annonce-avoir-depose-plainte-lundi-28-juillet-pour-atteinte-a-un-de-ses-systemes-dinformation/?lang=fra
- Ouest-France. (2025, 26 juillet). Naval Group, ciblé par une cyberattaque, évoque une attaque contre sa réputation. Récupéré le 28 juillet 2025, de https://www.ouest-france.fr/economie/economie-de-la-mer/naval-group/naval-group-cible-par-une-cyberattaque-evoque-une-attaque-contre-sa-reputation-7deb3eb0-6a4b-11f0-b8dc-7402ea9fbf6c
- Perez, C. (2023). La Cybersécurité. Studyrama.
- Qu'elle est la place de l'Intelligence Artificielle dans les pratiques d'audit interne ? (2023). Dauphine PSL & Grant Thornton
- Statista Research department (2024, 28 octobre) La cybersécurité – Faits et chiffres. Récupéré le 28 juillet 2025, de https://fr.statista.com/themes/3680/la-cyber-securite/#topFacts
- Verspieren (2025, 4 février) Risques cyber pour les hôpitaux : pourquoi le secteur de la santé doit renforcer sa cybersécurité. Récupéré le 28 juillet 2025, de https://www.verspieren.com/fr/entreprise/article/iard/cybersecurite-

hopitaux#:~:text=La%20fragilité%20des%20infrastructures%20informatiques,augmentant%20la%20surface%20d'attaque.

- Wikipédia. (s.d.). Opérateur d'importance vitale. Récupéré le 28 juillet 2025, de https://fr.wikipedia.org/wiki/Op%C3%A9rateur_d%27importance_vitale
- Wikipédia. (s.d.). Opérateur de services essentiels. Récupéré le 28 juillet 2025, de https://fr.wikipedia.org/wiki/Op%C3%A9rateur_de_services_essentiels
- Wikipédia. (s.d.). Techniques d'audit assistées par ordinateur. Récupéré le 28 juillet 2025, de https://fr.wikipedia.org/wiki/Techniques_d%27audit_assist%C3%A9es_par_ordinateur