Guide des **risques cyber 3.0**

Les questions de l'auditeur et du contrôleur interne

IFACI
IIA France

2025

Le mot du Délégué Général

Après le Guide Cyber et le Guide Cyber V2.0 publié en 2020, vous tenez en mains le troisième opus de notre guide.

Les cyber-risques tiennent une place à part dans l'univers des risques. D'une part, ils sont, à ce jour, toujours en tête de la liste des risques les plus importants du rapport Risk in Focus 2025. D'autre part, les outils et méthodes en la matière ont beaucoup évolué depuis les derniers travaux effectués à l'IFACI.

C'est ainsi que, toujours supervisés par Guy-Philippe Goldstein, nos adhérents se sont à nouveau penchés sur ce Guide Cyber V3.0 qui, je l'espère, vous apportera une vision complétée des dernières avancées et mises à jour sur les risques eux-mêmes, ainsi que sur les moyens de les maîtriser.

Je remercie tous les adhérents contributeurs de cet ouvrage, Mathieu Couturier et Fabien Renaudin de l'ANSSI, Vincent Maret de KPMG, Jamal Basrire de PWC ainsi que Maxime Cartan et ses équipes chez Citalid pour la qualité de leurs apports.

Philippe Mocquard

Délégué Général

TABLE DES MATIERES (*cliquez sur une rubrique pour y accéder*)

Introduction

L'objectif

En 2020, un premier guide de l'IFACI des cyber-risques, démarré un an plus tôt, avait été publié avec l'objectif de pouvoir servir de point de départ pour l'auditeur et le contrôleur interne dans leur visions respectives sur ces risques nouveaux et particuliers du point de vue de la 3ième ou de la 2ième ligne de défense de l'entreprise. Trois constats importants ont amené l'IFACI à reprendre cet exercice quatre ans plus tard.

- D'une part, le risque cyber s'est vu confirmé depuis 2020 et la crise Covid comme l'un des tous premiers risques de l'entreprise. C'est ce que démontre années après années depuis 4 ans « Risk in Focus » de l'ECIIA, qui fait du risque cyber le 1er risque transverse de l'entreprise (hors risque métier) auquel est confronté l'entreprise et par là-même, sa 2ième et 3ième ligne de défense. « Risk in Focus » n'est d'ailleurs pas la seule source à évaluer le risque cyber à un tel niveau. Cette nouvelle importance du risque cyber se retrouve dans les résultats du questionnaire de France Assureurs depuis 2023 ; ou également dans ceux du PwC CEO Survey sur la France en 2024. En outre ce risque occuperait désormais de 15% à 30% des effectifs des auditeurs et des contrôleurs internes, selon les organisations, avec des applications de plus en plus systématiques dans les plans d'audit (à l'instar par exemple, du risque de fraude financière).

- Pour autant, le cyber-risque continue à être à la fois mal perçu, voire rebutant pour certains (vu comme « trop technique »). En outre, différentes évolutions technologiques de fond (ex: cloud, IA..) sont capables de faire profondément évoluer sa pratique alors que les évolutions sociologiques (ex: « tous codeurs avec l'IA »), régulatoires (ex: NIS2, régulation post quantique) ou géopolitiques (chocs mondiaux) vont probablement continuer à le maintenir dans le TOP1 1/ TOP 2 des risques de l'entreprise. La rapidité de son évolution, ainsi que son maintien au premier rang des risques de l'entreprise, laissent penser que ce risque n'est pas encore totalement maîtrisé par l'entreprise.

- Cependant, cinq ans après la publication du Guide des Cyber-Risques pour et par les Auditeurs & les Contrôleurs Internes, les organisations sont désormais plus aguerries. Les approches se sont affinées ; des outils ont commencées à apparaître ; et dans de nombreuses organisations d'audit et de contrôle interne, un renforcement des méthodologies tout autant des bonnes pratiques a pu avoir lieu, éprouvées au fil du temps et des retours d'expérience. Pour l'IFACI, le moment est donc apparu comme propice de revisiter l'ensemble des réflexions du guide de 2020.

La démarche

Tout comme pour le Guide 2.0 paru en 2020, le Guide 3.0 a pour objectif d'être directement utile aux auditeurs et aux contrôleurs internes. Dans ce contexte, l'IFACI est parti de principes simples :

1. Demander directement aux auditeurs et contrôleurs internes, via une enquête en ligne, les questions identifiés comme les plus importantes concernant les risques cyber (voir ci-dessous les résultats) ;

2. Dans le contexte toujours évolutif du cyberespace, se concentrer sur les points les plus prioritaires plutôt qu'essayer d'apporter des réponses exhaustives ;

3. Créer pour chaque question de petites équipes de travail, constituées des auditeurs et des contrôleurs externes : ces équipes de professionnels seront les mieux à même de répondre aux questions de leurs propres confrères.

Ces volontaires, dont on pourra retrouver une biographie à la fin de ce guide, ont également été épaulés par des experts externes –Vincent Maret de KPMG, Jamal Basrire de PwC et également des experts de Citalid avec l'aide de son dirigeant, Maxime Cartan. Enfin, des experts de l'ANSSI, Fabien Renaudin et Mathieu Couturier, ont bien voulu accompagner la démarche à son initiation. Qu'ils trouvent ici l'expression de nos remerciements.

Les sujets prioritaires

Une enquête en ligne sur les questions les plus importantes que se posaient les auditeurs et les contrôleurs internes au sujet des cyber-risques a été soumise aux membres de la communauté de l'IFACI. 64 participants y ont répondu. La population des répondants a été constitué pour 73% d'auditeurs et pour 27% de contrôleurs internes et de consultants. Les répondants venaient principalement d'organisations de plus de de mille employés (56%) suivi d'une représentation significative de PME et ETI entre 100 et 1000 employés (37%).

Toutes les questions sélectionnées ont dépassé les 50% de réponse de type « oui, très intéressé.e », un très haut niveau. Elles ont toutes atteint un niveau supérieur à 80% d'intérêt si l'on cumule les réponses « oui, interessé.e » et « oui, très intéressé.e ».

On note certaines évolutions sur l'importance respective de chacune des questions, comparé à l'enquête de 2020. La question des impacts opérationnels concrets (Q1) est identifiée en 2024 comme la plus importante. Cela reflète peut-être la nécessité d'être capable de désormais mieux caractériser ce risque afin d'être plus précis dans sa gestion et son contrôle. Ce point fait écho à la question suivante – celle de sensibiliser le top management (Q2). La question des fondamentaux techniques/ contrôles de base à connaitre à minima pour les équipes audit et contrôle internes (Q4), la première en 2020, demeure néanmoins dans le top 5 : s'il y a plus de maturité générale qu'en 2020, de nombreuses organisations continuent à se demander encore quel est le « bon » point de départ pour gérer ce risque. Pour les auditeurs et pour les contrôleurs internes généralistes, il demeure aussi une question de positionnement face aux autres experts internes et externes, un point également abordé dans la question du rôle de l'audit et de contrôle interne (Q3).

L'ensemble des autres questions font aussi écho à l'environnement toujours en évolution de l'entreprise de ses systèmes informatiques, qu'il s'agisse des impacts liés à des transformations technologiques telles que l'IA, le Cloud ou le low-code (Q9) ; la réalité d'une entreprise vivant dans un écosystème établi en réseau (Q10) ; des chocs géopolitiques et une veille générale nécessaire (Q7) ; des changements de régulation toujours plus rapides qu'il faut anticiper (Q6). Toutes ces évolutions posent la question de la mesure à un instant t de la maturité de l'organisation (Q5) – alors même que demeure un des invariants les plus profonds et les plus importants du risque cyber : celle du facteur humain (Q8).

Questions-clés retenues pour étude pour le Guide 3.0

Questions		Oui, très intéressé.e
Q1	Les impacts opérationnels concrets du risque cyber	80%
Q2	Sensibiliser le top management, et avec quels types de tableau de bord	70%
Q3	Le rôle de l'audit et du contrôle interne face aux autres experts internes en cybersécurité	70%
Q4	Les fondamentaux techniques/ contrôles de base à connaitre à minima pour les équipes audit et contrôle internes	69%
Q5	Mesurer la maturité de l'organisation et son niveau d'exposition au risque cyber	63%
Q6	Prendre en compte et intégrer les régulations à venir (Ex : NIS2, DORA, AI act, Cyber-Résilience Act, Cyber Security act, etc…), incluant les nouvelles responsabilités civiles voir pénales des dirigeants	60%
Q7	Se tenir au courant de l'évolution du risque cyber – y compris au niveau géopolitique ?	58%
Q8	Sensibiliser les collaborateurs, et développer une « cyber-hygiène » et mieux contrôler le facteur humain	58%
Q9	Le risque cyber dans les projets informatiques, y compris avec l'accélération & la démocratisation du code en entreprise (via cloud, low-code, IA…) ?	56%
Q10	Vérifier et contrôler l'état des risques-cyber des fournisseurs clés de l'entreprise ou des entités cible d'opérations d'acquisition.	53%

Résultats et conclusions intermédiaires

L'ensemble des travaux réalisés par les différentes équipes de travail a été présenté en session plénière et ont donné lieux à des fiches de synthèse ici présentes. Ces fiches doivent être lues comme une introduction à chacune de ces questions clés, et doivent permettre aux auditeurs et contrôleurs internes une première orientation.

Ces fiches sont donc l'expression de la réflexion des différentes équipes. Epaulés par les conseils listés plus haut, les équipes d'auditeurs & contrôleurs internes ont néanmoins gardé jusqu'au bout le contrôle rédactionnel et donc sont seules responsables des éléments posés ici. Il s'agit d'un parti pris.

Comme en 2020, face à une matière technologique terriblement large et changeante, embrassant des entreprises de tout type et conditions, il serait à nouveau illusoire d'écrire dans le marbre ce qui pourrait être nuancé, ou changé, dans 24-36 mois. Comme pour son prédécesseur (le Guide 2.0 publié en 2020), ce présent guide se veut donc lui aussi le reflet volontaire d'une réflexion collective. Il reflète aussi une démarche particulière : il est un appel au questionnement et à la réflexion de tous, qu'ils convergent avec les idées présentées ici, ou bien au contraire qu'ils en divergent. Car, à la mesure de la matière qu'il essaie de traiter, ce guide doit être vivant et devra évoluer.

Avis, exemples, réflexions sont donc les bienvenues de la part de l'ensemble des auditeurs et contrôleurs internes. Tout apport constructif permettra de faire progresser la communauté des membres de l'IFACI, tant le sujet, important et riche, doit encore incorporer variations, compléments ou même situations éventuelles de contre-indication. Au-delà de ce guide et de son matériel, c'est cette conversation qui permettra à la communauté des auditeurs et des contrôleurs internes de contribuer de manière efficace et dynamique à un risque en perpétuelle évolution, qui menace les entreprises et même, parfois, les nations derrière les organisations qui la composent.

Profitons enfin de cette introduction pour remercier et saluer les 33 contributeurs auditeurs et contrôleurs internes, adhérents de l'IFACI, qui par leurs efforts ont réussi à faire naitre ce Guide 3.0. Une petite biographie de chacun d'entre eux est présente à la fin de cet ouvrage.

Comme l'a rappelé le Délégué Général en avant-propos, L'IFACI remercie également pour leur aide Mathieu Couturier et Fabien Renaudin de l'ANSSI, Vincent Maret de KPMG, Jamal Basrire de PWC ainsi que Maxime Cartan, Pouya Canet et Léo Coquebelin de Citalid. Leur soutien et la qualité de leurs apports ont été précieux pour les contributeurs de ce Guide 3.0.

Partie I

Vision d'experts

Mathieu Couturier,

Chef de la division Management de la Sécurité du Numérique de la sous-direction Stratégie de l'ANSSI.

Dans un monde de plus en plus connecté et numérisé, la maitrise des risques cyber est devenue un enjeu incontournable pour les organisations, qu'elles soient publiques ou privées. Face à l'intensification des menaces, qui touchent désormais tout le monde, et à l'évolution rapide des technologies, il est essentiel que les entreprises adoptent une approche proactive, intégrée et systémique de la gestion des risques numériques. Le **Guide des Cyber Risques 3.0 de l'IFACI**, fruit de l'expertise collective des professionnels de l'Audit et du Contrôle Interne, constitue une réponse essentielle pour renforcer la résilience des organisations face aux défis de la cybersécurité.

Les ruptures technologiques portées notamment par la cryptographie post-quantique (PQC) ou l'intelligence artificielle (IA) renforcent les risques cyber actuels, en fournissant de nouvelles capacités aux attaquants, et créent de nouveaux domaines de risques, notamment avec le déploiement, encore mal maitrisé, de systèmes d'intelligence artificielle dans les processus métiers. La prise de conscience des enjeux associés à ces technologies est nécessaire afin de sécuriser les usages et en tirer pleinement les bénéfices. L'Audit et le Contrôle Interne ont un rôle tout particulier à jouer pour accompagner les directions générales et les directions métiers dans la bonne prise en compte de ces nouveaux enjeux.

Les (re)évolutions réglementaires à venir dans le domaine de la cybersécurité, en particulier avec la Directive *Network Information Security 2 (NIS2) et* le Règlement *Cyber Résilience Act (CRA),* vont également inciter les plus hauts niveaux de l'organisation à prendre en compte la cybersécurité avec une approche qui se veut désormais globale. Dans ce contexte, la gestion des risques devient un outil essentiel pour les dirigeants afin de les guider et s'assurer de la bonne mise en œuvre des mesures d'hygiène de cybersécurité permettant de se protéger contre la menace cybercriminelle de masse.

Ce guide se veut pragmatique et propose des axes de réflexions, des outils et des bonnes pratiques, des méthodologies éprouvées et des référentiels adaptés aux réalités actuelles, permettant aux organisations de mieux évaluer, maîtriser et atténuer les risques numériques dans un environnement en perpétuelle évolution. Il est essentiel que les dirigeants et responsables métiers comprennent ces risques, et intègrent leur maitrise dans leurs priorités. Ce guide s'inscrit également dans un contexte où la cybersécurité ne se limite plus uniquement à une simple question technique, mais devient un enjeu stratégique pour les entreprises, touchant tous les aspects de leur fonctionnement.

Nous encourageons les professionnels de l'Audit et du Contrôle Interne à utiliser ce guide comme un outil intégrant les bonnes pratiques indispensables pour renforcer la maitrise des risques cyber, tout en tenant compte de l'évolution rapide des menaces et des technologies, afin de garantir une gouvernance de la sécurité numérique efficace.

Vincent Maret,

Associé KPMG, en charge des activités de conseil en Cybersécurité, Protection des données personnelles et IA de confiance

La cybersécurité est plus que jamais une priorité stratégique pour les directions générales et les conseils d'administration. Les dirigeants ont pleinement conscience des impacts dévastateurs que les cyber attaques peuvent avoir sur la continuité des activités, la réputation de l'entreprise ou la confiance des clients. À cela s'ajoute un cadre réglementaire de plus en plus contraignant, avec notamment le RGPD, DORA, NIS2, l'AI Act et demain le Cyber Resilience Act. En réponse à ces évolutions, on a assisté depuis une dizaine d'années, à une montée en puissance des moyens humains et budgétaires consacrés par les entreprises à la protection contre les cyber menaces. Et ce sujet de la cybersécurité a été intégré dans tous les plans d'audit.

Mais les entreprises sont confrontées à une extension constante de la surface d'exposition aux menaces cyber. Là où les menaces visaient hier principalement les systèmes d'information de gestion, elles portent aujourd'hui en plus sur les systèmes industriels ainsi que les produits et les services vendus par les entreprises. Les tensions géopolitiques exacerbent les risques d'impacts directs ou indirects de cyberattaques étatiques et d'espionnage industriel. Les innovations technologiques telles que l'IA, le Web3 et l'Internet des objets offrent de nouvelles opportunités, mais introduisent également des risques inédits, renforçant la nécessité d'une vigilance accrue. La dépendance croissante des entreprises à leurs sous-traitants technologiques engendre des risques accrus de fuites de données ou d'arrêts d'activité.

Face à ces enjeux, le rôle de l'auditeur interne évolue. Il s'agit d'adapter son positionnement et de renforcer ses collaborations avec les équipes opérationnelles, les experts technologiques et les fonctions de contrôle pour appréhender les risques de manière transversale, systémique et dynamique. En travaillant main dans la main avec ces parties prenantes, tout en assurant son indépendance, l'auditeur interne peut fournir aux directions générales et aux comités d'audit une vue d'ensemble des risques cyber et des leviers d'action envisageables, leur permettant de prendre des décisions éclairées. Les décideurs doivent pouvoir trouver le juste équilibre entre agilité et maîtrise des risques, afin de protéger le présent tout en préparant l'avenir. L'auditeur interne joue ainsi un rôle clé en apportant des recommandations pragmatiques qui permettent non seulement de renforcer la résilience face aux menaces actuelles, mais aussi de positionner la cybersécurité comme un levier pour l'entreprise.

C'est toute l'ambition de cette version 3.0 du guide des Cyber-Risques de l'IFACI : accompagner les auditeurs internes dans cette mission, en leur fournissant des outils et des méthodes pour analyser les enjeux, évaluer les risques et contribuer à la prise de décisions.

Jamal Basrire,

Associé en charge des activités Cybersécurité chez PwC France et Maghreb

L'ère numérique, en constante évolution, a ouvert des perspectives incroyables pour les organisations du monde entier. Cependant, avec ces opportunités viennent également des défis inédits.

La cybersécurité plus que jamais érigée comme une priorité stratégique des dirigeants d'entreprise.

La menace cyber continue de croitre et constitue pour les dirigeants d'entreprise la priorité numéro 1 devant les risques environnementaux, géopolitiques ou sociétaux selon l'enquête « Global Digital Trust Insights (DTI) 2025 » de PwC.

Il ne suffit plus de considérer la cybersécurité comme une simple fonction technique. Elle doit être intégrée au cœur de la stratégie d'entreprise, avec une gouvernance claire et des ressources dédiées. A titre d'exemple le modèle des 3 lignes de défense permet de poser un cadre de responsabilité efficace devant être décliné au contexte de chacune des organisations. La sensibilisation des collaborateurs et le développement d'une cyber-hygiène sont 2 facteurs clés pour établir des fondations solides.

L'accélération technologique nécessite une adaptation de l'approche cyber.

Les avancées technologiques telles que l'IA, le développement low-code – no code et l'usage du Cloud apportent leur lot de défis en matière de sécurité. Une gouvernance éthique et une vigilance particulière sont nécessaires pour tirer parti de ces technologies tout en garantissant la sécurité des systèmes.

Parmi ces tendances technologiques, l'adoption de l'IA générative apparait comme un enjeu prenant de l'ampleur. Face à une donnée jouant un rôle de plus en plus central et dans le même temps de plus en plus accessible, 51% des répondants positionnent la protection des données comme la priorité no. 1 des investissements cyber (source : Digital Trust Insights 2025, PwC) ?

La réglementation un accélérateur pour mettre à niveau les entreprises dans leur gestion du risque cyber ?

La conformité aux réglementations en matière de cybersécurité est un impératif pour les organisations compte tenu des sanctions financières et administratives en jeu.

Jusqu'à présent, des cadres législatifs comme le règlement général de protection des données (RGPD) en Europe ou la loi de programmation militaire (LPM) en France imposaient déjà des standards stricts de protection des données ou plus globalement de sécurité des systèmes sensibles.

Face à l'accélération technologique, les états continuent de légiférer recherchant ainsi la préservation de la souveraineté et la réduction de la probabilité de survenance d'un incident systémique touchant une industrie sensible tels que : services financiers, santé, transport, énergie, eau, télécommunications / services des technologies de l'information et de la communication…

Selon la DTI 2025 de PwC, seulement 16% des entreprises indiquent être totalement confiant dans leur capacité à être en conformité réglementaire (NIS2 et DORA notamment). Seuls 2% indiquent avoir mis en œuvre une cyber résilience couvrant l'ensemble de leur organisation. Ces statistiques montrent ainsi l'ampleur du travail à encore réaliser dans un contexte où les entreprises chercheront à améliorer la performance de leur fonction cyber compte tenu de l'attention particulière des dirigeants sur les dépenses. 77% des répondants à notre enquête indiquent que leurs budgets cyber augmenteront en 2025…

Les entreprises ne disposant pas toutes des mêmes moyens et des mêmes dispositifs, celles-ci se questionnent actuellement sur leur modèle opérationnel avec un recours croissant au « services managés » pour compléter leur dispositif actuel voire parfois pour challenger le dispositif établi qui ne répond pas aux exigences de qualité et d'efficacité attendu par les entreprises.

Une interconnexion croissante amenant les entreprises à chercher à mieux maitriser les risques liés à leurs fournisseurs

Les cybercriminels utilisent des techniques de plus en plus avancées pour infiltrer les systèmes. Chaque organisation, grande ou petite, est une cible potentielle, rendant indispensable une approche de sécurité robuste et proactive.

Les risques cyber ne se limitent pas aux frontières de l'organisation. Les fournisseurs et partenaires peuvent également être des vecteurs de cyberattaques. Il est crucial d'incorporer des clauses d'audit rigoureuses dans les contrats et de vérifier l'état des risques cyber des fournisseurs clés.

Un guide 3.0 visant à poser les fondamentaux d'une approche cyber en 2025

Les 10 grandes questions abordées dans ce guide constituent un outil indispensable pour toutes les organisations pour naviguer les principales clés de succès pour aborder les risques cyber dans le paysage numérique actuel. Ce guide qui a mobilisé 32 auditeurs et contrôleurs internes qui proposent des stratégies pragmatiques et actuelles pour anticiper, prévenir, et réagir face aux cybermenaces. Implication des dirigeants, *dashboarding* cyber, mise en place des fondamentaux techniques, veille sur la menace cyber (cyber threat intelligence) et surveillance de l'exposition, supervision et surveillance du risque cyber des tierces parties sont autant de stratégies qui devront faire partie de l'arsenal des fonctions cyber d'entreprise. A l'ère de l'IA, il conviendra par ailleurs de mettre en œuvre une approcher cyber pour l'IA tout en étudiant les opportunités qu'offre l'IA à la cyber.

Ce guide pose la posture à adopter pour traiter les risques cyber dans l'ère technologique dans laquelle nous entrons. Il constitue un point de départ important à la poursuite des discussions qui amèneront chaque entreprise dans la revue de sa stratégie cyber dans cette nouvelle ère…

Maxime Cartan

Co-fondateur et Président de Citalid

Le risque cyber ne se résume plus à une simple question technique : il a un impact sur chaque facette de l'entreprise, de la continuité opérationnelle à la réputation, en passant par la performance financière. En échangeant chaque jour avec l'ensemble des parties prenantes du risque cyber, nous observons chez Citalid ce défi croissant : la menace devient plus complexe, les cyberattaques plus ciblées, et leurs conséquences plus lourdes. Le pilotage stratégique du risque cyber est donc une priorité pour toute organisation.

Le guide de l'IFACI développe une approche pratique, conçue pour permettre aux auditeurs internes de transformer le risque en levier de résilience. Comment éveiller et maintenir l'intérêt des dirigeants avec des tableaux de bord clairs et actionnables ? Comment briser les silos et permettre une collaboration fluide entre auditeurs, RSSI, comités exécutifs, Risk Managers, assureurs, etc. ? Comment mesurer dynamiquement la maturité cyber d'une organisation dans son intégralité, ainsi que son exposition financière à des scénarios de risque ? Autant de questions cruciales auxquelles ce guide apporte des éléments concrets de réponse.

Avec l'élargissement des menaces et des régulations internationales comme DORA, NIS2 ou les nouvelles règles de la SEC, le risque cyber est enfin pleinement reconnu comme un risque business. Dans ce contexte, les auditeurs internes jouent un rôle clé : garantir une maîtrise solide des risques, en interne comme auprès des partenaires et fournisseurs critiques, sans oublier les processus d'acquisition.

Pourtant, la maturité face au risque cyber reste hétérogène. Or, pour protéger efficacement l'organisation, il ne suffit plus de réagir aux incidents ; il faut anticiper, sensibiliser et assurer une compréhension commune des enjeux. Ce guide aide à combler ce fossé, en fournissant des éléments concrets pour aligner l'organisation et faire sortir la sécurité des systèmes d'information de son isolement. C'est un enjeu business, et sa valeur ajoutée n'est plus à prouver dans un environnement numérique.

L'importance des auditeurs internes dans cette transition ne fait désormais plus de doutes pour nous. Elle nous parait même centrale. En se tenant informées de la menace, des évolutions géopolitiques et des nouvelles technologies, les équipes de contrôle pilotent la résilience organisationnelle, intégrant une approche cyber robuste et adaptable. Nous espérons que ce Guide aidera donc les auditeurs et les contrôleurs internes à mieux exploiter de nouveaux outils et méthodes pour réinventer le rôle de l'audit interne face au cyber.

Partie II

Les Questions Clés des Auditeurs Et Des Contrôleurs Internes

1 - Les impacts opérationnels concrets du risque cyber

Par Anny SIBONI-ZERBIB, Frédéric VILANOVA et Guillaume MALESPINE

I - Les impacts opérationnels concrets du risque cyber : Enjeux de la question

Quatre objectifs majeurs pour l'organisation et ses auditeurs & contrôleurs internes peuvent être notés autour de cette question, suivis des quelques exemples concrets :

- **Améliorer la prise de décision éclairée** en cyber-risques, domaine récent et complexe pour les Comités de Direction du fait de la nature protéiforme des attaques (externes ou internes) et de leurs impacts souvent très préjudiciables pour les organisations.
- **Réduire les coûts** liés aux pertes et aux dommages **tout en investissant de manière adaptée** à la maturité cyber nécessaire aux métiers.
- **Améliorer la résilience opérationnelle** lors des crises cyber.
- **Protéger la valeur de l'organisation, sa réputation et la confiance des marchés**.

Exemples d'impacts opérationnels par suite d'une cyberattaque :

- **Perturbation ou interruption des activités** : Une cyberattaque peut dégrader ou même arrêter totalement le niveau de service.
- **Fuite d'informations** : La compromission de données sensibles ou personnelles peut résulter d'une attaque discrète ou bruyante.
- **Perte d'intégrité des données :** La corruption des données, notamment par des attaques de rançongiciels, peut être fatale pour certaines organisations.
- **Perte d'un agrément ou d'une certification :** La perte d'un agrément nécessaire à une activité réglementée peut interdire temporairement ou définitivement une activité. La directive NIS2 et la règlementation DORA (secteur banques assurances) abordent cette problématique au niveau européen,
- **Impacts sur les ressources humaines :** Certaines cyberattaques entraînent des problèmes de ressources humaines, comme une augmentation de l'absentéisme ou un refus de collaborer, ou encore une augmentation du stress, qui peut être lié à la gestion de la crise ou à un sentiment de culpabilité.

Tous ces impacts opérationnels des risques cyber entraînent des coûts directs et indirects qui pourront faire l'objet d'une analyse assurantielle par ailleurs. À court terme, l'entreprise doit financer l'analyse de l'attaque, la remédiation des dommages, et les pénalités de retard contractuelles. La temporalité et le niveau de couverture d'une police d'assurance ne garantissent souvent pas une couverture complète et rapide de ces impacts.

II - Grands principes pour une approche des impacts opérationnels du risque cyber

Quels sont les grands principes qui permettent de mieux gérer les impacts opérationnels du risque cyber ?

- **Identifier les principales sources de profitabilité et activités critiques** de la structure est indispensable pour une connaissance transverse, partagée et holistique.
- **Cartographier les processus métiers** qui sous-tendent ces activités : Comprendre les processus métiers afin de mieux identifier la répercussion d'un incident cyber sur l'ensemble de la chaîne de production, les clients et la profitabilité.
- **Analyser les risques :** Maîtriser une méthodologie d'analyse des risques cyber adaptée à l'organisation (en empruntant, si cela est pertinent, au référentiel FR EBIOS RM ou à la norme internationale ISO IEC 27005) ; la méthodologie doit être comprise par l'ensemble des métiers. Relier les risques cyber aux processus métiers et aux actifs (infrastructure et SI) qui les supportent.
- **Collaborer transversalement :** l'auditeur, la fonction contrôle interne, la fonction conformité (fraude ; DPO), le RSSI, et les responsables des services de sécurité IT afin de définir des scénarii d'attaque et des chemins d'attaque techniques pertinents dans le contexte de l'organisation.
- **Développer une culture des enjeux cyber :** Maintenir une sensibilisation constante aux enjeux opérationnels liés aux risques cyber de l'organisation.
- **Adapter les politiques et procédures de sécurité** aux exigences de continuité et de sécurité dictées par les activités critiques : mettre en place un processus de management de la sécurité et de la continuité de l'information et des systèmes conforme aux exigences des règlementations et directives en vigueur
- **Améliorer la maturité de la structure en matière de cybersécurité** en s'appuyant sur les principaux référentiels existants notamment en intégrant les recommandations prévues par les normes ISO IEC 27001 et 22301.
- **Renforcer la sécurité dans la chaîne d'approvisionnement IT**, en tenant compte de la criticité des tiers en distinguant les impacts critiques et ceux qui le sont moins pour une bonne priorisation des traitements :
  - S'assurer que les tiers répondent aux exigences business en matière de continuité et de sécurité, adapter le cas échéant les clauses contractuelles de sécurité et les exigences de continuité.
  - S'assurer que les tiers ont une maturité suffisante en matière de cyber sécurité et qu'ils sont notamment protégés contre les évènements redoutés par les métiers de l'organisation (problématique des attaques par rebond) ; intégrer des clauses d'audit dans les contrats avec les tiers.
- **Développer une veille sur les vulnérabilités techniques, organisationnelles, physiques et humaines** qui soit adaptée aux activités de l'organisation (notamment sur le plan règlementaire).
- **Évaluer l'exposition aux menaces :** Examiner régulièrement le niveau d'exposition de l'organisation aux menaces identifiées, qu'elles soient externes ou internes.

III - Bonnes pratiques pour l'approche des impacts opérationnels du risque cyber

Dans le propos qui suit, nous abordons l'organisation et la méthodologie pratique, les deux impérativement nécessaires pour identifier et maîtriser les impacts opérationnels concrets des cyber-risques. Il s'agit ici de s'assurer que ces bonnes pratiques sont mises en place. Les éléments ci-joints peuvent donc servir de référence pour évaluer les pratiques existantes.

Les bonnes pratiques s'articulent autour de deux concepts : design et effectivité.

Design (conception)

- **Instaurer un dialogue entre les métiers et l'IT** : Partir des métiers opérationnels pour identifier les sources de valeur/richesse de l'entreprise et les processus et ressources critiques correspondants. **Associer les personnes concernées des métiers à l'identification des impacts opérationnels concrets** afin de proposer des recommandations pragmatiques et proportionnées aux risques perçus par les métiers. **Associer également les spécialistes des systèmes d'information** pour identifier et préciser les scénarii d'attaques qui auraient le plus d'impact sur ces processus critiques.
- **Mettre en place un plan d'actions visant à renforcer la sécurité et/ou la résilience.**
    - **Exemples d'approche (non exhaustif) :**
        - **Démarrer par les comptes financiers :** prendre le compte de résultat de l'organisation ; identifier les processus métiers les plus critiques ; en déduire les actifs les plus à risques ; croiser avec les analyses cybers les plus récentes – tout ceci afin d'éviter de se concentrer sur des scénarios qui ne concerneraient qu'une part économiquement minime de l'organisation ;
        - **Démarrer par les activités majeures de l'organisation :** partir des 5-6 grandes activités de l'organisation ; suivre les chemins critiques opérationnels dans leur mécanisme de production ; déterminer les chainons susceptibles d'être mis à mal par une attaque cyber – afin d'identifier des points critiques qui n'auraient pas été bien vus (exemple de la cyber-attaque sur imprimantes de production dans un cas d'une usine agroalimentaire en France en 2019 qui en empêchant l'étiquetage permettant la traçabilité des produits a stoppé la commercialisation).

- **Proposer une approche d'audit fondée sur les risques** dont la couverture et la granularité seront assurées par **amélioration continue en procédant par itération :** les risques opérationnels sont complétés et raffinés au fil des itérations plus granulaires, plus couvrantes sur le périmètre retenu.

- **Communiquer en amont, pendant, après :** faire apparaitre la gestion des impacts opérationnels des risques cyber comme une évidence organisationnelle.

- **Proposer des indicateurs de maturité** (Key Performance Indicator KPI, Key Conformance Indicator KCI) qui soient compréhensibles et opérationnels (“on ne devient que ce que l’on mesure”).

- **Proposer des fiches réflexes pratiques et lisibles** pour diffuser la méthodologie d’analyse des risques retenue et adaptée à l’organisation, en précisant par exemple, les grandes étapes d'une analyse des risques opérationnels. Cette analyse ne doit pas rester l’apanage des sachants IT mais doit être adaptée à un public non spécialiste en IT. **Cette compréhension commune est en effet nécessaire** dans la détermination des impacts opérationnels qui est un exercice collectif entre les différents acteurs de l’organisation (voir annexe 1).

Effectivité (mise en place) :

- **Constituer un réseau de correspondants métiers**, pouvant par exemple être animé par la fonction Risk Management, conjointement avec l’équipe RSSI (cyber-sentinelles opérationnelles…). Par exemple :
  - Un réseau des correspondants protection des données et sécurité des systèmes d’information (1 correspondant par direction), animé conjointement par le DPO et le RSSI ;
  - Un réseau des correspondants conformité, déontologie, et risques (1 correspondant par direction), animé par les fonctions compliance et contrôle interne de la direction des risques ;

- **Effectuer des appels réguliers à participation des personnes concernées (métiers et IT) pour développer le suivi et la mesure du traitement des risques cyber ayant un impact opérationnel.** En profiter pour étoffer l’analyse et inclure des risques nouveaux (par exemple, à la suite de la revue régulière des incidents informatiques).

- Mettre en cohérence active le Plan de Continuité des Activités et le Plan de Gestion de Crise d’origine Cyber à travers **des sessions d’entrainement à la gestion des risques opérationnels (tests MCO – Maintien en Conditions Opérationnelles).**

- **Etablir un plan pluriannuel d’audit intégrant systématiquement le cyber risque :**
  - Au travers d’un audit d’un processus métier qui intègre la problématique des cyber risques associés ;
  - Ainsi qu’au fil du déploiement de l’audit cyber à partir du métier IT ;
  - Ce qui conduit à une approche mixte et intégrée entre la fonction audit interne, la fonction contrôle interne et le RSSI.

- **Traduire les impacts concrets dans un langage suffisamment intelligible et compréhensible** pour faciliter l’appropriation de ces risques par les organes de gouvernance (ne pas tomber dans un verbiage technique des informaticiens ou des auditeurs ; proposer un glossaire technique compréhensible).
  - *Idéalement, si cela est possible, être capable de traduire dans un langage métier (ex : x nombre de jours d’arrêts de production) ou commercial/financier (ex : % de vente en moins sur le mois)*

- **Collaborer régulièrement et formellement avec les autres acteurs internes et externes** impliqués dans la gestion du risque cyber.

- **Effectuer une veille technologique adaptée aux activités opérationnelles** de l'organisation (menaces ; vulnérabilités techniques) auprès d'organismes spécialisés, nationaux ou internationaux (exemple : CERT-FR).
    - *Cette veille peut d'ailleurs constituer un des éléments de documentation et d'animation des réseaux de correspondants évoqués plus haut.*

IV – Les points d'attention pour l'auditeur et le contrôleur interne

Quelles sont les principales sources d'échec des missions d'audit de l'impact opérationnel des risques cyber ?

- **Ne pas comprendre la notion d'impact opérationnel des risques cyber.**
- **Faire la confusion entre la propriété de sécurité de l'information** et des systèmes et la **propriété de continuité** de l'information et des systèmes.
- **Etablir un cloisonnement excessif** entre les fonctions de Risk Management, de RSSI, de gestionnaire d'exploitation chargé des services de sécurité
- **Avoir un mauvais rattachement du RSSI au sein de l'organisation**, qui le rend trop dépendant de la DSI, de la DAF ou de la Production. Un positionnement au sein de la direction des risques, indépendante des métiers, peut-être de bonne pratique.
- **Avoir une connaissance limitée ou obsolète de la menace et des vulnérabilités opérationnelles** en matière de risques cyber.
- **Ne pas être capable de traduire correctement les impacts opérationnels en langage intelligible** par les organes de direction.
- **Vouloir tout régler au premier passage :** c'est-à-dire ne pas profiter des itérations successives d'analyse de risques pour bien hiérarchiser les sujets, pour se contenter d'aller à l'essentiel en première itération, pour bien affecter les moyens d'audit au fil des itérations et de la granularité de couverture des impacts opérationnels identifiés.

V – Conclusions

Les enjeux opérationnels des risques cyber sont majeurs. Ils nécessitent une compréhension et un engagement formel et régulier des organes de direction. Cet engagement réel est une des tendances lourdes des références normatives internationales (ISO IEC 27001) et des exigences règlementaires européennes (Directive NIS2). Il faut donc veiller à **manager de façon professionnelle les risques cyber** (Plan, Build, Run, Audit and Control) **et en garantir une gouvernance éclairée et active** (cadre référentiel, résultats, ressources, risques, transparence et engagement des acteurs).

Les auditeurs internes et les contrôleurs internes ont toute leur place pour aider à mieux maîtriser ces risques et également pour mieux communiquer avec les organes de direction, et mieux les impliquer. Ils sont les niveaux 3 (auditeurs) et 2 (contrôleurs) qui complètent les actions de production et de contrôle opérationnel de niveau 1 effectuées par la Direction des Systèmes d'Information et ses fournisseurs.

D'un point de vue formation des auditeurs et des contrôleurs internes sur le domaine des enjeux opérationnels des risques cyber, il est pertinent de songer à deux axes de progrès :

- **Un axe endogène à la profession** : la formation spécialisée sur ces sujets par l'IIA, l'IFACI, etc.
- **Un axe exogène** : l'invitation à participer activement à certains travaux d'experts techniques (RSSI, hackers éthiques, etc.) pour mieux comprendre les arcanes technologiques et aider à les synthétiser en management.

ANNEXE 1 : Les grandes étapes d'une analyse des risques opérationnels (exemples de méthodologies).

Phases méthodologiques ISO IEC 27005 (Structuré, assez linéaire, international)	Phases méthodologiques EBIOS RM (Plus flexible, original, franco-français)
Identification des exigences de base des parties intéressées. Ceci inclut les normes, réglementations et politiques d'entreprise qui régissent les activités opérationnelles	Préparation préliminaire (existence d'un socle de sécurité) Atelier 1 : Point de vue du défenseur Définir le périmètre de l'analyse, les métiers, les processus et les systèmes d'information opérationnels concernés.
Définition du contexte : périmètre de l'analyse, processus métiers et leurs systèmes d'information opérationnel	
Identification des risques opérationnels : rechercher, reconnaître et décrire les risques liés à la sécurité de l'information qui impactent directement les opérations, en prenant en compte les sources de risque, les objectifs visés et les vulnérabilités.	Atelier 2 : Qui est l'agresseur ? Évaluer les ressources et la motivation des attaquants potentiels pour impacter les opérations. Atelier 3 : Par où l'attaquant agira-t-il ? Identifier les vulnérabilités et les points faibles dans les systèmes d'information et les processus opérationnels.
Analyse des risques : évaluer la gravité et la vraisemblance des risques cyber opérationnels identifiés, en utilisant des échelles et des matrices appropriées.	Atelier 4 : Comment l'attaquant agira-t-il ? Évaluer la vraisemblance des attaques et les probabilités de réussite sur les processus opérationnels.
Évaluation des conséquences potentielles des événements redoutés sur les opérations, en prenant en compte les critères de conséquences (sévérité d'impact, fréquence, etc.). Définition des stratégies de traitement des risques identifiés, en prenant en compte les objectifs d'entreprise et les ressources disponibles.	Atelier 5 : Quelle stratégie de sécurité ? Définir les mesures de sécurité pour réduire les risques opérationnels identifiés.
Suivi et évaluation des effets des mesures de traitement des risques, et ajuster la stratégie en conséquence. Revue des incidents et intégration éventuelles en analyse des risques (amélioration continue ISO IEC 27001)	Bonne pratique (socle des sécurités)

2 - Sensibiliser le top management, et avec quels types de tableau de bord

Par Quentin CHOPARD, Thierry THOMAS et Vincent MARET

I - Enjeux de la question

La maitrise des risques métier liés à la cybersécurité est une question de direction générale et de conseil d'administration. Il est donc vital pour une organisation de mettre en place les éléments permettant aux dirigeants (Comité exécutif, Conseil d'Administration, Comité d'Audit) d'avoir une vision juste :

- Du niveau de menace cyber pour l'entreprise,
- Du niveau de maîtrise des risques cyber,
- De l'adéquation des dispositifs de résilience (PCA, PRA, ...),
- De l'impact du risque cyber sur les autres risques/fonctions de l'entreprise,
- Du niveau de maîtrise globale de l'ensemble des risques,
- Du niveau de conformité aux lois et de la responsabilités civile et pénale des dirigeant, (RGPD, NIS2, DORA, AI Act, Etc...),
- De l'avancement des plans d'actions et des remédiations,
- Des risques résiduels.

In fine, ces décideurs, dont le temps et les esprits sont occupés par de multiples tâches et responsabilités, doivent pouvoir, en matière de cybersécurité, se saisir des bons sujets et prendre les bonnes décisions en termes de gestion des risques, de stratégie financière, d'investissements et/ou d'allocations des ressources.

C'est une dimension essentielle dans la gestion des risques cyber, et donc un domaine que les fonctions de la maîtrise des risques (audit interne, contrôle interne, gestion des risques, conformité, data privacy) doivent aborder dans leurs missions respectives (plan d'audit, audits, cartographie des risques, tests terrains, ...).

II - Grands principes

Les dirigeants doivent recevoir une information pertinente et bénéficier d'interactions avec des professionnels de la cybersécurité leur permettant d'obtenir ce bon niveau de vision, avec des informations :

- À jour, exactes et sincères,
- En nombre adapté (ni trop, ni trop peu),
- Compréhensibles (pas trop techniques, en lien avec les métiers, etc.),

- Permettant de prendre rapidement les bonnes décisions (en termes de ressources, en cas de cyber crise, etc.),
- Leur permettant de définir le moment opportun pour se saisir d'un sujet (escalade).

III - Bonnes pratiques

A) L'audit interne devrait s'assurer que les informations fournies aux dirigeants, notamment via des dashboards de KPI/KRI (Key Performance Indicator/Key Risk Indicator) :

- Sont pertinentes et exactes par rapport aux risques, au contexte et à la réalité du terrain,
- Sont en volume adapté,
- Sont compréhensibles par les dirigeants et leur permettent de prendre des décisions,
- Sont basées sur des processus (repository, flux, outils type décisionnel) permettant une production fiable d'informations,
- Qu'au-delà de l'organisation elle-même, des dispositions sont prises au niveau des fournisseurs et clients clés (en se basant sur les classements ABC respectifs) et sous-traitants SI,
- Leur permettent de bien saisir et prendre en compte les risques opérationnels et non pas seulement les exigences de conformité.

Par exemple, le nombre d'attaques bloquées par un firewall n'est pas un indicateur très intéressant pour un dirigeant. Doit-il s'alerter de voir que 10 000 attaques sont bloquées par mois ? Est-ce grave ? Que doit-il faire ? En revanche, savoir que seules 25% des applications classifiées comme critiques en termes de disponibilité disposent d'un plan de continuité formalisé et testé est le type d'information qui peut et doit intéresser vivement un dirigeant et l'amener à prendre des décisions.

B) L'audit interne devrait s'assurer que les éléments contribuant à la sensibilisation des dirigeants en termes de cybersécurité :

- Sont adaptés en termes de fréquence, durée et modalités,
- Favorisent leur acculturation dans le domaine de la cybersécurité,
- Incluent des pratiques innovantes (rapport de l'état de la menace, war games, intervention d'experts, de régulateurs, outils de quantification, etc.) ou des exercices favorisant la prise de conscience (ex : Red Team)
    - Exemple A : des exercices de Red Team pilotés par l'audit (3e ligne de défense) et réalisés par une tierce partie de manière ponctuelle (ex : tous les deux ans, sur des sujets nouveaux) ont pu réussir à sensibiliser fortement des directions générales d'entreprises industrielles en particulier quand ils ont pu être traduits en impacts opérationnels.
    - Exemple B : des exercices de quantification du risque cyber pouvant utiliser la méthodologie FAIR et certains nouveaux outils

du marché et qui permettent, quand les hypothèses de modélisation sont acceptées par la direction générale, 1) de comprendre à minima les ordres de grandeur du risque et 2) de pouvoir créer une base pour identifier une trajectoire. Ces approches peuvent également aider au dialogue avec un autre élément clés de la direction générale – la direction financière, dans les conversations sur la couverture assurantielle.

La représentation des différents indicateurs de risques (KRI – Key Risk Indicators) peut se faire via des outils décisionnels (Power BI, Tableau, QlickSens, ...) permettant d'avoir un lien direct avec les bases de données, ou avec des tableaux excel qui sont actualisés régulièrement (selon leur fréquence au préalable définie).

C) L'audit interne devrait s'appuyer sur des comparaisons avec des pratiques de place (benchmark) pour s'assurer que la sensibilisation du top management est au bon niveau, mais aussi pour aider à la prise de décision par les dirigeants.

D) L'audit interne doit lui-même communiquer au bon niveau avec les dirigeants, notamment via des KPI/KRI :

- Sur le niveau de couverture des zones de risque cyber par le plan d'audit interne,
- Sur l'avancée du plan d'audit,
- Sur l'avancée de l'application des recommandations issues des plans d'audit précédents,
- Sur l'état d'avancement des plans d'actions associés aux risques cyber,
- Sur le niveau de résilience global de l'organisation,

IV – Points d'attention

A) De nouvelles approches de quantification des risques commencent à se répandre au sein des entreprises les plus matures en termes de cybersécurité (voir Exemple B plus haut). Elles produisent des valeurs chiffrées en termes de probabilités et d'impacts liés au scenario de risque et de réduction de risque liés à la mise en place de mesures de sécurités / plans d'actions. Si tel est le cas dans l'organisation, les fonctions liées à la maîtrise des risques (audit, gestion des risques, contrôle interne, conformité, data privacy) devraient s'assurer que les dirigeants à qui ces chiffres sont présentés comprennent bien la notion de quantification des risques et de probabilité, tel que par exemple l'impact financier d'une occurrence unique d'une menace (single expectancy loss), et devraient leur donner des exemples illustrant ces chiffres.

B) Le rôle des fonctions liées à la maîtrise des risques n'est pas de calculer les indicateurs fournis aux dirigeants : ceux-ci sont produits par la première et la deuxième ligne (direction des systèmes d'information (DSI), RSSI, ...). Toutefois,

l'audit interne peut vouloir vérifier que les indicateurs fournis aux dirigeants sont exacts, ce qui peut passer par l'analyse du processus de production des indicateurs, mais aussi parfois par leur (re)calcul par l'audit interne.

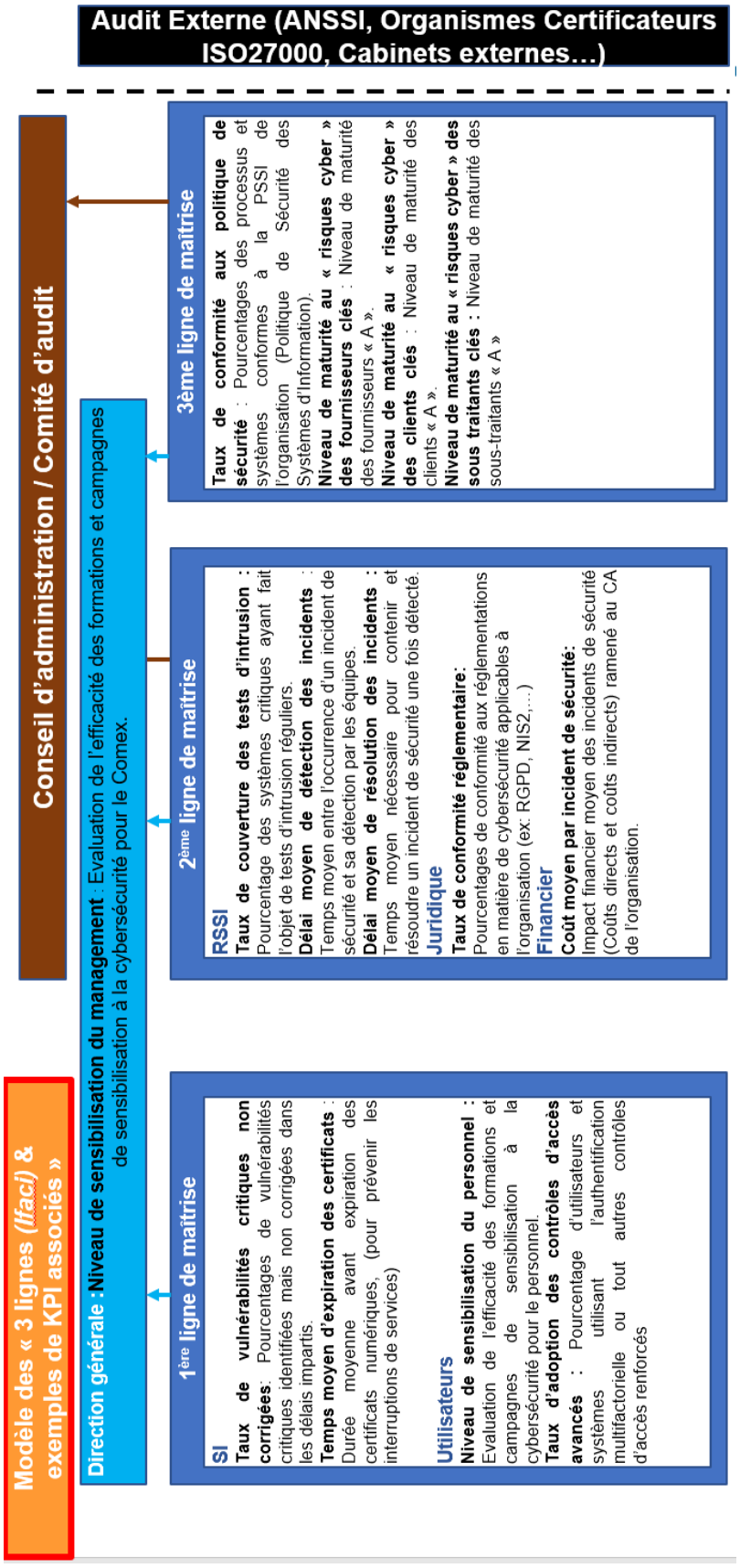
C) L'audit interne doit s'assurer que toutes les parties prenantes, y compris les dirigeants, sont conscients du domaine de validité, et donc des limites et contraintes, des services de « rating » cyber.

V - Conclusions

Le sujet de la sensibilisation des dirigeants aux risques cyber, et plus largement, de la mise à disposition d'informations pertinentes pour leur permettre de remplir efficacement leur rôle décisionnel, est absolument primordial.

Les fonctions liées à la maîtrise des risques (audit interne, gestion des risques, contrôle interne, conformité, data privacy) ont un rôle clé à jouer dans cette démarche en intégrant ces aspects dans leurs missions. Grâce à sa connaissance approfondie des processus internes et des interactions entre les différentes parties prenantes, l'audit interne est idéalement positionné pour évaluer l'efficacité des dispositifs de sensibilisation et des tableaux de bord destinés aux dirigeants, et plus généralement leur contribution à la maîtrise des risques cyber.

Exemples de KPI en fonction des 3 lignes :



3 - Le rôle de l'audit et du contrôle interne face aux autres experts internes en cybersécurité

Par Amine SARDI, Lotfi LADOUARI et Olivier SZNITKIES

Introduction

Le risque cyber est le plus souvent, et légitimement, dans le top 10 des risques majeurs des entreprises. Les directions d'audit et de contrôle interne se posent souvent la question de leur positionnement, de l'étendue de leurs responsabilités et de leur capacité d'action quant à ce risque transversal, pervasif et difficilement quantifiable. Aucune organisation n'est équivalente à une autre en matière d'exposition aux risques cyber, en matière de maturité de gestion de ce risque, et d'organisation et de capacités technologiques à faire face à ce risque. Néanmoins, poursuivant la réflexion entamée dans le guide IFACI 2.0 des Cyber-Risques, nous proposons quelques orientations visant à articuler au mieux les travaux de l'audit et du contrôle interne avec ceux des experts internes en cyber sécurité.

Principes & Pratiques

Les auditeurs/contrôleurs internes se posent souvent la question de leur légitimité technique quant à la couverture et à la fourniture d'assurance sur la maîtrise des risques de cybersécurité. Constatant que les auditeurs/contrôleurs internes ont l'habitude d'appréhender efficacement des sujets métiers et industriels également très techniques, nous pensons que la technicité des questions de cybersécurité ne devrait pas être un frein pour contribuer efficacement au sein des organisations à un renforcement de la posture de cybersécurité de celles-ci.

Notre développement vise à partager quelques orientations issues des meilleures pratiques observées parmi les adhérents de l'IFACI et le positionnement de l'audit et du contrôle interne vis-à-vis des différents dispositifs de maîtrise des risques liés à la cybersécurité.

1) Comment établir une collaboration active entre les acteurs d'assurance en matière de cyber-risques

1.a) Domaines de collaboration

Les auditeurs/contrôleurs internes et les RSSI/DSI ont des responsabilités qui se recoupent et des objectifs communs en matière de maîtrise des risques de cybersécurité :

- Le rôle des DSI/RSSI est opérationnel et technique. Il implique d'analyser les risques pour définir les politiques et mesures de sécurité et de veiller à leur bonne mise en œuvre (contrôle et audit). Les DSI/RSSI agissent en première et deuxième ligne de défense sur les cyber-risques.

  La mission de l'audit interne (selon le Cadre de Référence International des Pratiques Professionnelles) est « d'accroître et préserver la valeur de l'organisation en donnant

avec objectivité une assurance, des conseils et des points de vue fondés sur une approche par les risques. 1». L'audit se positionne en troisième ligne de défense.

- Les rôles sont complémentaires avec une vision plus technique pour les RSSI/DSI et une vision métier pour les auditeurs/contrôleurs internes.

- La question cruciale est donc de savoir comment collaborer de manière optimale pour assurer la sécurité et l'efficacité des stratégies et des opérations de cybersécurité. La présence d'un RSSI et l'existence d'une fonction d'audit IT peuvent jouer un rôle déterminant dans cette dynamique. Dans tous les cas, il est essentiel que la responsabilité de la cybersécurité soit clairement définie, qu'elle incombe au RSSI ou, à défaut, au Directeur des Systèmes d'Information (DSI). En outre, la maîtrise de ce risque doit impérativement figurer au cœur des préoccupations de l'audit et du contrôle interne. Cela inclut l'évaluation régulière des systèmes de sécurité, de la mise en place de protocoles de réponse aux incidents, et de l'assurance que toutes les parties prenantes comprennent leurs rôles et responsabilités en matière de cybersécurité. Seule une approche intégrée et proactive permet de gérer efficacement ces risques et de protéger notamment les actifs informationnels de l'organisation.

- Il est possible pour les auditeurs et contrôleurs de fournir une assurance, jusqu'à un certain point, sans expertise technique approfondie et/ou en ayant recours à de l'assistance externe spécialisée, quant à la maîtrise des risques cyber et la mise en œuvre de certaines thématiques clés. Certaines de ces thématiques clés (cf. tableau en section 2) sont listées ci-contre :
    - La gouvernance, la stratégie et l'organisation de la cyber sécurité (Comment est structurée la gouvernance de la cybersécurité au sein de l'entreprise ? Quels sont les rôles et responsabilités des différents comités et parties prenantes ? Existence et positionnement d'une fonction RSSI ? Répartition des rôles et responsabilité entre les 3 lignes de défense ? Etc…) ;
    - La gestion du risque cyber (Le risque cyber est-il recensé dans la cartographie des risques ?) ;
    - Les contrôles et les procédures (Existence d'une politique de sécurité informatique formalisée et maintenue ? Existence de référentiels de conformité ou d'obligations réglementaires en matière de sécurité des SI ?) ;
    - L'existence de programme de formation/sensibilisation des utilisateurs et des collaborateurs de la DSI *(A noter : la dimension du facteur humain dans le cyber-risque est particulièrement critique – voir Q8/Sensibiliser les collaborateurs, et développer une « cyber-hygiène » et mieux contrôler le facteur humain)*;
    - L'inventaire des systèmes et outils (Le périmètre SI est-il documenté ? Les applications critiques sont-elles identifiées ? Existe-t-il un inventaire à jour des sites internet ?) ;
    - L'existence de plan de continuité de l'activité ou de résilience prenant en compte les scénarios de risques cyber ;
    - La maintenance des systèmes (Les versions logicielles des systèmes identifiés sont-elles à jour ?) ;
    - L'existence de sauvegardes suffisamment fréquentes et testées ?
    - La gestion des accès.

[1] https://www.ifaci.com/cadre-de-reference-international-des-pratiques-professionnelles-de-laudit-interne-cripp/

- Les auditeurs/contrôleurs internes peuvent conduire leur approche en partant de l'analyse des risques métiers (interruption ou perturbation d'activité, fuite de données personnelles ou sensibles, fraude, etc.), comme le recommande d'ailleurs l'ANSSI à travers la méthodologie EBIOS RISK MANAGER (https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/).

1.b) Recours à des prestations externes d'expertise technique

- Certains aspects de l'exercice d'audit et de contrôle peuvent nécessiter bien sûr des expertises techniques (Exemples : tests de vulnérabilité, tests d'intrusion, audit de code, etc…). Le recours à une assistance externe peut être une solution et il est possible pour cela de s'appuyer sur des partenaires qualifiés PASSI (Prestataires d'Audit de Sécurité des Systèmes d'Information) par l'ANSSI (https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf).

- Tout en préservant l'indépendance de l'audit interne, nous recommandons, à cet égard, que la sélection d'un prestataire « technique » externe puisse se réaliser, en bonne coordination entre les auditeurs/contrôleurs internes et la DSI afin, d'une part, de s'assurer que les expertises apportées par les prestataires seront alignées avec les contextes individuels des organisations et leur environnement technologique, et d'autre part, afin d'éviter de désorganiser ou de risquer d'impacter la continuité des services SI critiques. Les auditeurs/contrôleurs internes restent les pilotes des objectifs des missions requérant une assistance externe.

- Lorsque l'audit interne décide de faire appel à des prestataires externes pour des tests de pénétration ou des simulations d'attaques dans le cadre d'une évaluation de la cybersécurité (par exemple au travers d'activités de type « red team »), il est crucial de mettre en place un dialogue préalable avec la Direction des Systèmes d'Information (DSI) et la Direction Générale (DG). Ce dialogue permet de prévenir et de gérer efficacement les risques d'interruption des systèmes d'information (SI) de l'organisation. En effet, L'audit interne, en concertation avec la DSI et la DG, assure non seulement que les tests de pénétration ou les simulations d'attaques sont menés de manière contrôlée, mais aussi qu'ils contribuent à renforcer la sécurité sans interrompre les opérations critiques de l'organisation. Un dialogue en amont permet d'anticiper les risques, de mieux gérer les contraintes techniques, et de s'assurer que toutes les parties prenantes sont alignées sur les objectifs, les résultats attendus et les conditions d'exercice des tests. Il conviendra, bien entendu, d'évaluer l'indépendance et l'objectivité des prestataires d'audit de cybersécurité notamment au vu des services qu'ils seraient susceptibles de fournir ou d'avoir fournis à la DSI ou au RSSI.
    - *A noter : la discussion a relevé que dans certains cas exceptionnels, la nécessité de créer des prises de conscience forte de l'état du cyber-risque dans l'organisation a pu conduire certaines directions de l'audit interne a mené des exercices de type « red team » avec un minimum de coordination avec la DSI, ainsi cependant qu'avec la coopération pleine et entière de certains cadres dirigeants clés de la DG. Entre autres, les risques d'interruption des SI doivent alors être particulièrement surveillés.*

1.c) Quels types de mission ?

Plusieurs types de missions liées à la gestion des cyber-risques peuvent être menées par l'audit interne et elles peuvent renforcer ou compléter la démarche de la DSI ou du RSSI :

- L'évaluation des contrôles généraux classiques et non techniques (ITGC) contribuent à renforcer la démarche et le message du RSSI pour la bonne application de la politique de sécurité. Ils permettent de sensibiliser les utilisateurs et éventuellement d'identifier des zones de risques.
- Les démarches de cartographie ou de quantification des risques permettent de lier les cyber-risques aux enjeux métiers et de sensibiliser/mobiliser le management de l'organisation. La quantification du risque cyber en particulier, qui consiste à évaluer financièrement les impacts des scenarios de risques cyber de l'organisation, est un excellent moyen de rapprocher les visions techniques et métiers pour ensuite prioriser les actions de cybersécurité.
- Les missions spécifiques d'évaluation de la maturité défensive (tests d'intrusions, audits de codes, audits verticaux sur un asset critiques) sont à réaliser en bonne intelligence avec le RSSI afin d'assurer une couverture optimale du périmètre des systèmes d'information de l'entité.
- Enfin, l'audit peut notamment porter son attention sur la résilience de l'organisation. C'est un point important qui n'est parfois pas directement ou prioritairement couvert par le RSSI. Il s'agit d'évaluer la maturité de l'organisation pour se relever après un incident de cybersécurité
    - Entre autres : Stratégie et procédures de sauvegarde et de redondance ; Existence d'une cellule de crise en cas d'attaque cyber majeure ; Existence d'une matrice RACI (Responsable, Autorité, Consulté, Informé) clairement définie montrant les responsabilités de chaque partie prenante pendant la gestion de crise ; Existence de plans de continuité ou de reprise d'activité ; Préparation à la gestion de crise, etc….
- Ainsi, le développement d'une relation complémentaire et constructive semble nécessaire au regard des objectifs communs et de l'ampleur de la tâche à accomplir en matière de maîtrise des cyber-risques.

2) Une proposition de modèle de collaboration entre les 3 lignes de maîtrise

Pour établir un modèle de collaboration entre les 3 lignes de maîtrise en matière de cybersécurité, voici une proposition qui précise le rôle de chaque ligne :

Ligne 1 : Équipes opérationnelles de DSI, Utilisateurs SI et Directions métier

Les équipes opérationnelles gèrent au quotidien la mise en œuvre des solutions et des actions en cybersécurité. Les utilisateurs SI et directions métier sont également responsables de la sécurité des informations traitées dans leur domaine respectif.

Ligne 2 : RSSI et Contrôle Interne

Le rôle de la deuxième ligne est de s'assurer que les contrôles mis en place sont suffisants et efficaces. Le RSSI apporte une expertise technique, tandis que le contrôle interne évalue la conformité des actions par rapport aux réglementations et aux politiques internes. Le RSSI

conduit/fait conduire des tests de pénétration périodiques et rend compte de l'efficacité de la gouvernance de la sécurité des SI.

Ligne 3 : Audit interne

La troisième ligne agit de manière indépendante pour vérifier que les deux premières lignes fonctionnent efficacement et que la cybersécurité est correctement gérée au sein de l'organisation y compris et notamment en matière de gouvernance, d'organisation, de formation/sensibilisation des utilisateurs.

Modèle de collaboration détaillé :

	Responsabilités des 3 lignes de défense		
Thématiques clés	**Ligne 1** **Equipes opérationnelle DSI, Utilisateurs SI et Directions métier**	**Ligne 2** **RSSI, Contrôle Interne**	**Ligne 3** **Audit interne**
Gouvernance, organisation, responsabilité en matière de cyber	Mise en place opérationnelle des directives du RSSI et des politiques de cybersécurité.	Le RSSI propose aux organes de gouvernance les politiques de sécurité adapté et veille à leur application. Le Contrôle Interne vérifie leur application et la pertinence de leur conception au vu des exigences de conformité (réglementaire et par rapport aux politiques et procédures définies).	Audit la gouvernance, la responsabilité et l'efficacité des processus.
Cartographie et gestion des risques cyber	Identification des risques au niveau opérationnel.	Le RSSI centralise et met à jour la cartographie des risques cyber. Le Contrôle Interne s'assure de la robustesse du processus.	Evaluation de la méthodologie mise en œuvre par le RSSI et les métiers pour établir une cartographie des risques cyber. Au besoin, (ré)évaluation indépendante des risques identifiés et du processus de gestion de ces risques.
Reporting au management en matière de gestion des risques cyber	Transmission des incidents et des risques identifiés au RSSI.	Le RSSI prépare et transmet les rapports au management. Le Contrôle Interne valide ces rapports.	Vérification de la pertinence et de l'exhaustivité des rapports. Maintien du dialogue avec les organes de gouvernance pour aider à

			la compréhension du reporting et la sensibilisation aux risques cyber.
Politiques, procédures et standards de cybersécurité	Mise en œuvre des standards et procédures définis.	Le RSSI définit les procédures. Le Contrôle interne vérifie leur mise en place et conformité.	Audit de l'application des politiques et procédures sur le terrain.
Formation, sensibilisation	Participation aux formations et application des bonnes pratiques	Le RSSI développe les programmes de sensibilisation. Le Contrôle Interne veille à leur efficacité.	Évalue la pertinence des formations et leur impact sur la culture de cybersécurité.
Surveillance (en continue, périodique)	Surveillance opérationnelle des systèmes.	RSSI met en place la surveillance continue. Le Contrôle Interne s'assure de l'efficacité des contrôles.	Audit des mécanismes de surveillance mis en place.
Outil de gestion de la cyber	Utilisation des outils selon les directives.	Le RSSI choisit et supervise l'utilisation des outils. Le Contrôle Interne vérifie leur utilisation adéquate.	Evaluation des outils en termes d'efficacité et de couverture des risques.
Conduite de tests, de diagnostic ou d'audit cyber	Exécution des tests et remédiation des failles.	Le RSSI coordonne les tests et diagnostics. Le Contrôle Interne en supervise les résultats.	Réalisation d'audits indépendants pour tester la robustesse des contrôles.
Gestion des accès/IAM	Implémentation des solutions d'accès et gestion des droits.	Le RSSI supervise la gestion des accès. Le Contrôle Interne vérifie les processus.	Audit de la gestion des accès pour assurer l'intégrité des systèmes.
Organisation de la résilience	Mise en place de plans de continuité et récupération.	RSSI développe les plans de résilience. Le Contrôle Interne évalue leur pertinence.	Audit de l'efficacité des plans de résilience et de leur application.

Au-delà du modèle proposé, il est essentiel de conserver un dialogue permanent entre les 3 lignes concernant l'état des menaces et des vulnérabilités qui sont en constante évolution afin de mieux maîtriser les risques cyber au sein de l'organisation.

- *A noter : ce type de dialogue avait été proposé dès 2017 dans le Guide 1.0 des Cyber-Risques, dans le cadre un peu plus formel d'un « Comité d'Adaptation aux Cyber-Risques » (voir https://docs.ifaci.com/wp-content/uploads/2018/06/Cyber-risques.pdf p.12-14). Ce dialogue peut prendre cependant de nombreuses formes, en fonction de la culture de chaque organisation. La conversation a ainsi relevé que, par exemple, certaines directions d'audit pouvaient dialoguer de manière constante sur l'évolution du risque cyber avec les directions de la sécurité informatique de différentes filiales d'entreprises multinationales au travers du format simple et efficace que constituait un fil d'échange sur un réseaux social sécurisé d'entreprise.*

Conclusion

Le risque cyber, désormais reconnu comme un des risques majeurs pour les organisations publiques et privées, conduit l'audit interne à devoir se positionner avec rigueur en tant que troisième ligne de défense. Dans ce rôle, l'audit interne se doit non seulement d'évaluer l'efficacité des contrôles mis en place par les autres lignes de défense, mais parfois de pallier les insuffisances de la deuxième ligne lorsque l'organisation manque de maturité ou de ressources en matière de cybersécurité.

L'enjeu principal est de garantir la **maturité de la gouvernance de la cybersécurité**. Cela signifie que les structures et processus de gestion des risques cyber doivent être suffisamment développés pour offrir une maîtrise raisonnable des menaces. L'audit interne peut intervenir en apportant un regard critique et en recommandant des améliorations, tout en veillant à ce que les mécanismes en place permettent une résilience face aux risques émergents.

Par ailleurs, l'audit interne doit encourager une **transparence totale** et adopter une approche de **pédagogie active** vis-à-vis des organes de gouvernance. Il est essentiel que les responsables comprennent clairement la répartition des rôles et des responsabilités entre les lignes de défense. L'audit interne doit également être un catalyseur pour signaler les besoins en moyens supplémentaires, qu'il s'agisse de ressources humaines, technologiques ou financières, afin de renforcer les capacités de la cybersécurité dans l'organisation.

L'audit interne doit anticiper et intégrer les **exigences normatives émergentes** de l'Institut des Auditeurs Internes (IIA), en particulier celles relatives à la gestion des risques cyber. Ces nouvelles normes, encore en cours de discussion fin 2024, auront un impact direct sur la manière dont l'audit interne doit aborder les risques cyber, en adoptant une approche proactive et stratégique pour assurer la robustesse des contrôles.

Enfin, l'audit interne doit pouvoir recourir à des expertises techniques internes ou externes permettant de fournir une assurance concernant les aspects les plus techniques des dispositifs de maîtrise des risques de cybersécurité. Ces évaluations « techniques » ne devraient pas prendre un caractère routinier car elles restent de la responsabilité des premières et deuxièmes lignes de maîtrise.

4 - Les fondamentaux techniques/ contrôles de base à connaitre à minima pour les équipes audit et contrôle internes

Par Carmelita DESOUZA, François MICHAUD, Prince Nyany ILUNGA et Xavier-Alexandre TREU

I - Enjeux de la question

La question relative aux "fondamentaux et techniques/contrôles de base à connaitre à minima pour les équipes d'audit interne et de contrôle internes" reste l'une des premières préoccupations face à :

- La multiplication et à la complexité des règlementations et attentes des parties prenantes (régulateurs, commissaires aux comptes, fournisseurs, clients…) ;
- La complexité croissante des systèmes d'information ;
- L'augmentation des menaces cyber.

Afin de répondre à cette question, de nombreux guides et référentiels proposent des contrôles et bonnes pratiques qui peuvent tous paraitre importants. Mais par quoi commencer ? Comment sélectionner les contrôles les plus pertinents à implémenter en priorité ? Comment s'assurer d'une bonne réalisation de ces contrôles compte tenu du niveau de technicité des auditeurs et contrôleurs internes, afin de ne pas passer à côté de leur mission, tout en répondant aux attentes du management et des différentes parties prenantes ?

II - Grands principes

Parmi les grands principes à retenir :

- Ne pas se lancer à corps perdu dans l'application d'un référentiel. Il en existe une multitude, et ces derniers ne prennent pas en compte les spécificités de l'organisation (secteur d'activité, maturité, business model…) ;
- Se poser les bonnes questions qui vont permettre de spécifier les sujets prioritaires pour l'organisation, et ainsi, assurer l'auditeur d'apporter une valeur ajoutée à son organisation ;
- Mettre en œuvre les contrôles de base qui peuvent être réalisés par un auditeur généraliste. En effet, selon le niveau de maturité, la plupart des contrôles de base ne requièrent pas une expertise et sont en grande partie réalisables par un généraliste. Cela apportera non seulement une meilleure expertise générale au sein de l'équipe d'audit, mais aussi répondra aux attentes des collaborateurs de l'équipe en termes de recherche de nouvelles compétences et d'apprentissage ;
- Ne pas hésiter à avoir recours à des « experts » pour traiter les sujets techniques. L'auditeur généraliste n'est pas censé avoir toutes ces compétences mais il doit être capable de comprendre les enjeux, les risques et d'en superviser les conclusions.

III - Bonnes pratiques

Pour mieux mettre en place les contrôles à minima adaptés à l'organisation, les bonnes pratiques sont les suivantes :

- Interroger la Direction sur sa **stratégie de gestion du risque cyber** et comprendre son niveau **d'appétence au risque cyber** (ambitions technologiques, budgets humains et financiers alloués), et comprendre également les problématiques liées à **l'écosystème de l'organisation** (environnement économique, géopolitique, réglementaire, partenaires, fournisseurs, clients). Les référentiels tels que COBIT, NIST et le Guide d'hygiène informatique abordent cette bonne pratique.

  Cette démarche permet de spécifier les sujets prioritaires pour l'organisation.

  Exemple des questions : Quelles sont les principales priorités stratégiques en matière de cybersécurité ? Quels sont les objectifs à court et à long terme de l'organisation en matière de gestion des risques cyber ? etc…

- Comprendre le niveau de **maturité cyber de l'organisation et l'environnement de contrôle**, par une **coordination** avec les autres parties prenantes : existence d'une PSSI (*Politique de Sécurité des Systèmes d'Information*), d'une cartographie, d'une police d'assurance cyber, d'un RSSI, d'un CIRT (*Computer Incident Response Team*), des contrôles ont-ils été mis en place par la DSI et par le Contrôle Interne, etc… (*Voir aussi Q5/Mesurer la maturité de l'organisation et son niveau d'exposition au risque cyber*).

  Ainsi, au regard du niveau de maturité cyber de l'organisation, il revient à l'Auditeur / Contrôleur Interne de choisir, dans la multitude de référentiels existants, les contrôles les plus adaptés à son organisation.

- Connaître les **actifs de valeur de l'organisation (logiques et physiques)** pour mieux les protéger. Cette démarche permet de **prioriser les efforts sur le patrimoine critique** et relativiser les vulnérabilités sur les zones sans valeur si elles sont isolées. La spécification des sujets prioritaires pour l'organisation permet de ressortir les actifs les plus critiques (cf. NIST, ISO 27001 & 2)

  A titre illustratif, cela comprendra généralement les configurations systèmes, les serveurs, les routeurs, les switch critiques, les mots des passes systèmes et, selon les organisations : les fichiers clients, les procédés techniques industriels, les actifs financiers, le fichier des stocks, les contrats, etc…

- Appliquer **les contrôles incontournables** à la portée des auditeurs/contrôleurs internes généralistes, d'une part, et spécialistes, d'autre part, avec pour objectif le respect des critères DICT (*Disponibilité, Intégrité, Confidentialité et Traçabilité*).

  Ces contrôles devront couvrir l'ensemble du périmètre cyber et tenir compte des priorités définies préalablement. Ceux qui sont trop techniques pour être réalisables par des auditeurs généralistes pourront être effectués par des spécialistes en interne ou par le recours à l'externalisation.

➢ *L'annexe 1 présente des exemples de **contrôles incontournables**, à minima, pour les services d'audit et de contrôle interne, classés en 3 axes de contrôle : Organisationnels ; Physiques / Ressources humaines ; Technologiques.*

IV – Points d'attention

L'auditeur/ le contrôleur interne doit garder à l'esprit plusieurs dangers qui pourraient menacer sa mission :

- Mettre en place une check-list standard de manière impérative est illusoire : les organisations ont toutes leurs particularités qui les rendent différentes. Cela pourrait conduire à omettre certains risques cyber importants spécifiques à l'organisation ;
- L'absence de coordination avec les autres fonctions fournissant de l'assurance (audit interne, contrôle interne, RSSI) peut induire des contrôles redondants ou des omissions dangereuses ;
- Une mauvaise appréciation du risque cyber propre à l'organisation, résultant de ces deux premiers dangers, peut aboutir à la mise en place de contrôles inutiles ou inopérants et à délivrer une « fausse assurance » à la Direction, une évaluation erronée du risque cyber ;
- Par ailleurs, les technologies évoluent (ex. : apparition de l'IA générative, généralisation de l'IoT), les modalités d'attaque également, mais aussi la réglementation (IIA Cybersecurity Topical Requirement, DORA, NIS2, etc.). Les contrôles doivent donc évoluer également pour ne pas devenir rapidement obsolètes. Organiser une veille cyber s'avère donc indispensable. (*voir Q6/ Prendre en compte et intégrer les régulations à venir et Q7/ Se tenir au courant de l'évolution du risque cyber – y compris au niveau géopolitique*) ;
- La matière devient toujours plus technique. De plus en plus de contrôles incontournables peuvent donc nécessiter des auditeurs spécialisés ou « augmentés » (data analytics), lesquels sont très recherchés ;
- Malgré cela, les auditeurs généralistes doivent pouvoir « challenger » les spécialistes qui voudraient être exhaustifs en mettant en place des contrôles qui ne sont pas forcément pertinents pour leur organisation. Il est du devoir de l'auditeur de développer une réflexion générale de type de « design du contrôle », dans le cadre d'une compréhension générale du risque alimentée par le questionnement de la Direction rappelé plus haut (sur la stratégie générale sur le risque cyber et l'appétence au risque cyber). Ce design de contrôle nécessite de mettre en place une architecture du contrôle qui aligne niveau de risque, stratégie générale et compréhension métier. Ce premier niveau fondamental de contrôle du risque ne nécessite pas d'avoir une compréhension technique approfondie. Il peut être complété par la suite par des spécialistes internes ou externes dont l'auditeur généraliste doit s'entourer.
    - *Par exemple, dans certaines organisations, ce sont des auditeurs généralistes qui supervisent la question critique de la gestion des droits, en posant d'abord des questions métiers fondamentales (ex. : qui fait quoi ? qui contrôle la gestion des droits ? Y a-t-il une bonne ségrégation des droits ? etc..)*

V - Conclusions

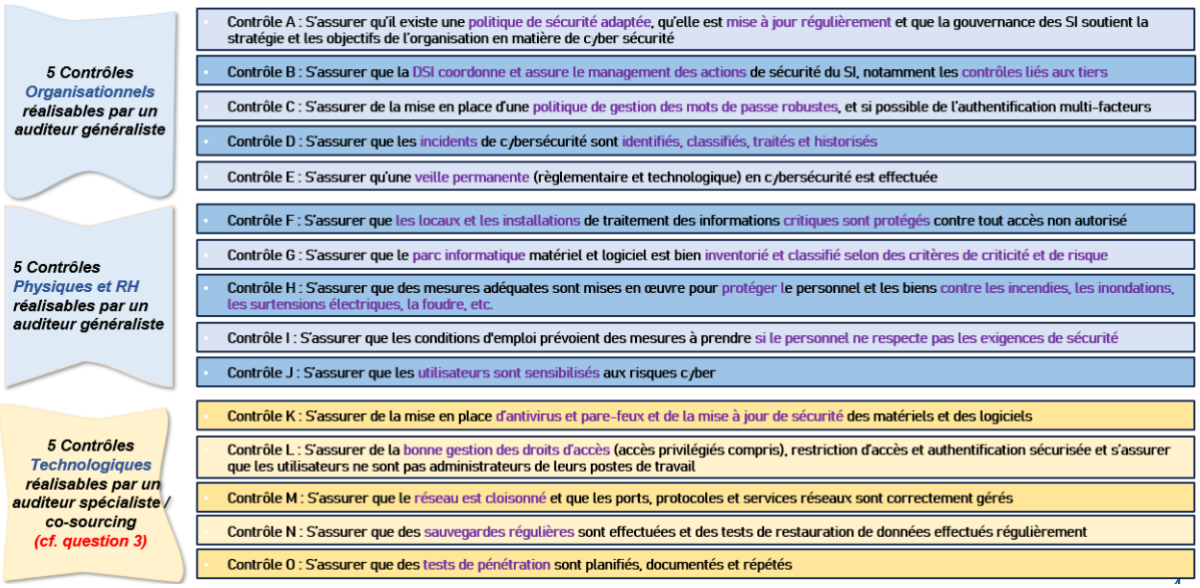
Pour être efficace, la mise en œuvre de contrôles de base ne peut pas être l'application brutale d'une liste tirée d'un référentiel. Elle doit résulter d'une démarche préalable d'interrogations et d'analyse des risques cyber et du contexte propres à l'organisation, par une coordination avec les autres parties prenantes.

Ensuite seulement, grâce à cette compréhension des enjeux, la constitution d'une liste de contrôles issus des référentiels de place pourra être réalisée, en confiant aux auditeurs généralistes les contrôles organisationnels ainsi que les contrôles de type « physiques » ou « ressources humaines » (cf. Annexe 1), et à des auditeurs spécialisés les contrôles technologiques plus précis.

Annexes

Annexe 1

Quelques contrôles incontournables (sans ordre particulier) selon 3 axes de contrôle : Organisationnel, Physique/RH et Technologique



Annexe2

Ces contrôles se retrouvent dans les référentiels : quelques exemples…

Guide IFACI 3.0	CIS V8	NIST CSF 2.0	ANSSI Guide d'hygiène informatique	ANSSI La Cybersécurité pour les TPE/PME en 12 questions	ANSSI-AMRAE Maîtrise du risque numérique – l'atout confiance
Contrôle C : S'assurer de la mise en place d'une politique de gestion des mots de passe robustes, et si possible de l'authentification multi-facteurs	Chapitre 6. Access control management	PR.AA-02 Identities are proofed and bound to credentials based on the context of interactions PR.AA-03 Users, services, and hardware are authenticated PR.AA-04 Identity assertions are protected, conveyed, and verified	Point 10 Définir et vérifier des règles de choix et de dimensionnement des mots de passe Point 13 Privilégier lorsque c'est possible une authentification forte	Question 5. Avez-vous implémenté une politique d'usage de mots de passe ?	
Contrôle G : S'assurer que le parc informatique matériel et logiciel est bien inventorié et classifié selon des critères de criticité et de risque	Chapitre 1. Inventory and Control or Enterprise Assets Chapitre 2. Inventory and Control of Software Assets	ID.AM-01 Inventories of hardware managed by the organization are maintained ID.AM-02 Inventories of software, services, and systems managed by the organization are maintained ID.AM-05 Assets are prioritized based on classification, criticality, resources, and impact on the mission	Point 4 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau	Question 1. Connaissez-vous bien votre parc informatique ?	Étape 2 Comprendre son activité numérique
Contrôle K : S'assurer de la mise en place d'antivirus et pare-feux et de la mise à jour de sécurité des matériels et des logiciels	Chapitre 9. Email and Web Browser Protections Chapitre 10. Malware Defenses	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk PR.PS-05: Installation and execution of unauthorized software are prevented	Point 17 Activer et configurer le pare-feu local des postes de travail	Question 3. Appliquez-vous régulièrement les mises à jour ? Question 4. Utilisez-vous un anti-virus ? Question 6. Avez-vous activé un pare-feu ? En connaissez-vous les règles de filtrage ? Question 7. Comment sécurisez-vous votre messagerie ?	Étape 9 Bâtir sa protection

Annexe 3

Les principaux référentiels *(sans ordre particulier)*

- La suite ISO/CEI 27000 : qui comprend les normes de sécurité de l'information
- Le NIST Cybersecurity Framework (CSF) 2.0
- Le COBIT : qui fournit des indicateurs, des processus et de bonnes pratiques pour la gouvernance des SI ;
- La suite de Global Technology Audit Guide (GTAG) de l'IIA : un ensemble des guides d'audit des systèmes d'informations ;

- Le CIS : 18 CIS Critical Security Controls (v8)
- L'ITIL (Information Technology Infrastructure Library) : qui propose un ensemble de bonnes pratiques pour la gestion des services informatiques ;
- Le « Guide d'hygiène informatique » de l'ANSSI qui présente 42 bonnes pratiques ;
- Le guide « Maîtrise du risque numérique – l'atout confiance » de l'ANSSI-AMRAE avec 15 étapes ;
- La « Cybersécurité pour les TPE/PME » de l'ANSSI en 12 questions ;
- Le Guide des risques cyber 2.0 de l'IFACI en 9 questions clés ;
- Le Cybersecurity Topical Requirement de l'IIA, en cours d'élaboration.

5 - Mesurer la maturité de l'organisation et son niveau d'exposition au risque cyber

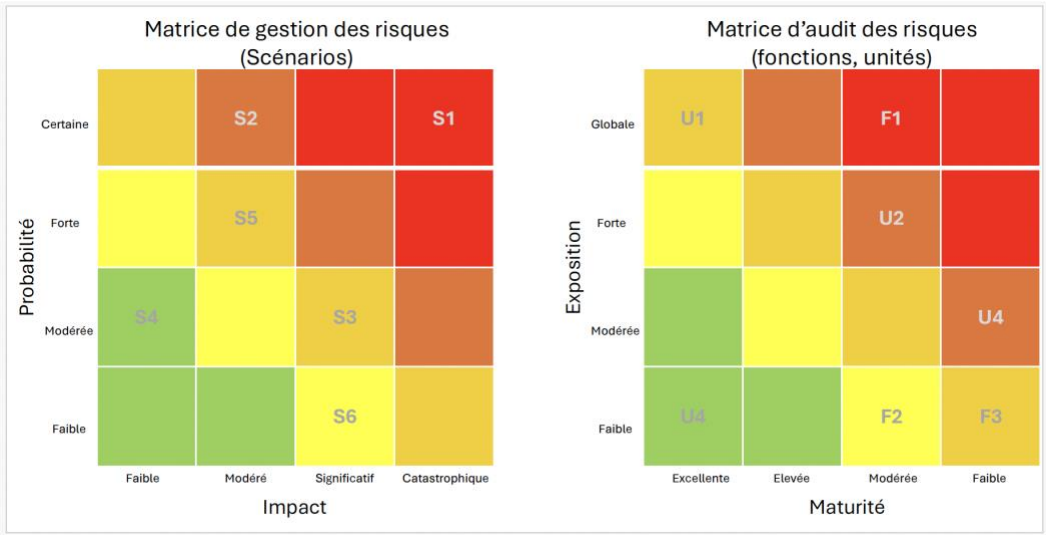
Par Coffi José VIGAN, Marie-Line POITOUT, Mohamed Yassine ZOUGARI et Pierre-Luc REFALO

I - Introduction & Enjeux : Comment contribuer à la maîtrise des risques Cyber ?

- Le Guide 2.0 des risques Cyber publié en 2020 a fixé le cadre des enjeux de l'évaluation de maturité autour de (a) la prise de conscience, (b) la compréhension des principales responsabilités et (c) la diffusion des bonnes pratiques (voir Annexe).

Ces éléments doivent être renforcés et complétés des manières suivantes :

- Clarifier le rôle de l'audit interne (3ième ligne) et de l'évaluation de *maturité* au regard des 1ière et 2ième lignes de contrôle (*sécurité* opérationnelle et *conformité* réglementaire / normative) ;
- Favoriser les prises de décision au regard d'une matrice de risque intégrant les scénarios de risque cyber couvrant la transformation numérique et la protection des données ;
- Contribuer au renforcement des bonnes pratiques sur la base de référentiels cohérents et adaptés au contexte de l'organisation ;
- Elargir le champ de la gestion du risque cyber et de la cybersécurité au-delà du Système d'information en couvrant la sécurité des produits et services ainsi que la «Supply Chain » numérique incluant les fournisseurs et les partenaires – un point désormais critique.



II - Grands principes

Fondamentaux et évolutions depuis 2020

Le Guide 2.0 des risques Cyber publié en 2020 a proposé des **grands principes** qui restent d'actualité. Il convient donc d'abord d'évaluer la maturité sous l'angle de la gouvernance générale (politique, organisation, contrôles) sur la base de référentiels adaptés et contribuant effectivement à la maîtrise des risques cyber :

- Existence d'un corpus réglementaire interne appuyant la certification d'un système de management de la sécurité de l'information (Ex. : ISO27001), les opérations informatiques (Ex. : guides d'hygiène informatique des agences de sécurité, Cloud Security Alliance - STAR, ISAE3402 pour les fournisseurs informatiques) et la protection des données (Ex. : ISO27701) ;

- Nomination d'un Directeur / Responsable de la Cybersécurité / Sécurité des SI (hors de la DSI pour son indépendance) conscient que le profil, le champ d'action et de responsabilité sont très variables ;

- Promotion des pratiques de *« sécurité par conception / par défaut »* au sein de tout projet informatique / numérique sur la base d'une analyse de risques et des impacts opérationnels et financiers, avec un focus sur la protection des données (*privacy by design*) ;

- Mise en place de procédures de contrôle et d'audit selon le modèle en trois lignes de défense.

Au-delà, l'évaluation de la maturité doit à la fois se renforcer et s'élargir selon deux axes majeurs, en termes de :

- Gouvernance : en développant des synergies fortes avec la sécurité/sûreté (intelligence économique et informations sensibles, sécurité des biens et des personnes) et la protection des données personnelles ;

- Pratiques : en intégrant de façon cohérente, la sécurité des SI de gestion (internes), les produits et services (métiers) ainsi que les fournisseurs et prestataires (plateformes externes, chaine logistique).

Ces deux points méritent une attention particulière car ils sont porteurs de risques spécifiques.

Facteurs de risques et évolutions depuis 2020

Le Guide 2.0 des risques Cyber publié en 2020 a proposé des **facteurs de risque** qui là encore, restent d'actualité. Il convient donc d'abord d'évaluer le niveau d'exposition sous l'angle de (a) l'absence de considération du risque cyber par les dirigeants et aussi (b) de mise en œuvre insuffisante des pratiques de base (cf. fondamentaux).

Au-delà, l'exposition au risque cyber augmente selon trois axes majeurs, en termes de :

- Menaces intégrant de plus en plus une dimension stratégique (géopolitique, souveraineté) et sectorielle (compétition, innovation) ;
- Vulnérabilités liées aux objets connectés, aux plateformes et services numériques (Cloud), aux traitements de données (AI) ;
- Réglementation accrue dans de nombreux domaines en Europe (Directive NIS-2 et Règlement DORA, Digital Service Act, Digital Market Act, Cyber Resilience Act, AI Act, etc...)

III - Bonnes Pratiques de l'auditeur

Le Guide des risques Cyber publié en 2020 a proposé trois approches d'évaluation de la maturité de la cybersécurité d'une organisation (*disponible sur le workspace IFACI à https://ifaci.workplace.com/groups/tribu.ifaci.cybersecurite/permalink/1016588208778073/*) :

- Prise en compte des risques cyber dans les enjeux métier en produisant une cartographie des risques (cf. introduction) avec un reporting fort à la direction générale et au conseil d'administration ;
- Utilisation d'un ou plusieurs référentiels adaptés en matière de maîtrise des risques et cohérents avec l'organisation, sa taille, sa présence géographique et son secteur (Ex. : normes PCI pour les paiements, HDS pour les données de santé, TISAX pour l'automobile, etc.) ;
- Mise en œuvre d'un outillage adapté pour automatiser les évaluations et les piloter dans la durée (Cf. Guide des risques cyber 2.0).

Au-delà, des compléments sont nécessaires pour tenir compte de l'évolution des fondamentaux et des facteurs de risque. Ils sont listés ci-contre, associant critères d'application et facteurs de risque.

A. Structurer les référentiels de l'analyse de maturité selon un modèle commun

Le développement des normes, standards et règlements oblige à clarifier et structurer l'usage des référentiels d'audit.

Critères

1. Exploitation de la structure définie dans la Directive NIS, le Règlement RGPD ainsi que le Standard du NIST CSF V2.0 qui s'appuient sur 6 domaines : Gouverner - Identifier - Protéger - Détecter - Réagir et Restaurer ;
2. Utilisation de cette structure pour les risques cyber comme pour la protection des données et la sûreté de l'information / sécurité des biens et des personnes ;
3. Définition de KPI / KRI / KCI pour chacun des 6 domaines en précisant le processus d'élaboration, de collecte, d'analyse et d'aide à la décision (*Voir Annexe*).

Facteurs de risques

1. Approche cloisonnée voire incohérente aux plans technique et juridique, stratégique, tactique et opérationnelle et surtout inadaptée à chaque métier, unité ou fonction ;
2. Absence de vision globale, holistique et partagée sur l'exposition aux risques dans toutes ses dimensions (technique et juridique, organisationnelle - facteur humain et processus) ;
3. Décisions rendues difficiles sur les axes de progrès prioritaires, les domaines de responsabilité type RACI (Responsable, Autorité, Consulté, Informé) et l'allocation des ressources / budgets.

B. Renforcer le contrôle de conformité aux normes et certifications

Les référentiels d'audit doivent veiller à l'intégration des normes, standards et règlements en effectuant des contrôles au bon niveau en termes d'exposition aux risques (opérations, conformité, finance, etc.).

Critères

1. Les obligations réglementaires non dérogeables (responsabilité civile ou pénale) doivent être considérées en premier lieu (dirigeants) ;
2. Les clauses contractuelles (pénalités, audit, révisions, rupture) doivent être revues et validées dans toutes les dimensions du risque (juridique) ;
3. L'analyse du ratio coût / bénéfice de toute mise en conformité doit s'effectuer avec des éléments factuels et démontrables, éventuellement avec un benchmark (finance) ;
4. Le cas échéant, l'appréciation d'un avantage concurrentiel de la mise en conformité doit être effectué en impliquant des décideurs (marketing).

Facteurs de risques

1. Multiplication et intrication des normes, standards et réglementations, avec de potentielles contradictions ;
2. Distinction entre ce qui est obligatoire et optionnel, avec manque possible d'objectivité de l'analyse ;
3. Prise en compte de l'impact des fusions et acquisitions, avec évolution de l'exposition aux risques.

On notera en discussion plusieurs points de réflexion additionnels sur les contrôles :

- Au sein d'une même organisation, des géographies ou des unités métiers peuvent avoir des approches différentes et une vision plus ou moins critique : cela peut servir de points de comparaison afin d'identifier des critères de contrôles pertinents ou non ;
- D'une manière plus conceptuelle, la maturité d'une organisation de contrôle peut s'évaluer à sa capacité à bien déterminer et savoir précisément justifier quels sont les contrôles vraiment prioritaires. A contrario, ne pas le savoir (et donc par exemple, tout mettre sur un pied d'égalité) peut-être le signe d'une méconnaissance intime de l'organisation – bref, d'un manque de maturité. Cela peut constituer une ligne d'investigation de la 3ième ligne de contrôle par rapport à la 1ière ou la 2ième ligne.

C. Intégrer le développement des agences de notation « cyber » à l'évaluation de maturité

L'émergence d'un nouveau segment de marché dans l'analyse de la gouvernance, des risques et de la conformité nécessite une approche spécifique dans le cadre de la « supply chain » numérique.

Critères

1. Utilisation d'agences de notation du système de management interne avec des questionnaires basés sur des normes et standards multiples (ex. : www.cybervadis.com, www.processunity.com, etc…) ;
2. Utilisation d'agences de notation sur les risques liées à l'exposition sur Internet avec des scans permanents / réguliers (ex. : www.boardofcyber.io, www.bitsight.com, www.securityscorecard.com, etc…) ;
3. Utilisation par les clients de l'organisation et les autorités de contrôle, mais aussi par et pour l'organisation elle-même, considérant le contrôle de ses partenaires et fournisseurs ;
4. Consolidation et cohérence de bout en bout en lien avec la police d'assurance et la quantification du risque cyber (indicateur composite, basé sur les points 1. & 2. ci-dessus, et solutions, tels que www.citalid.com par exemple..).

Facteurs de risques

1. Maturité encore insuffisante du marché et des solutions (indépendance, transparence, concurrence) ;
2. Qualité discutable des notations et des résultats (algorithme non standard, évolution des données et des scores non maîtrisés par l'organisation) ;
3. Qualification délicate du rapport coût / bénéfice au regard des exigences des clients et des autorités ;
4. Dimension géopolitique émergente entre acteurs américains et européens avec des risques d'influence des marchés ou de distorsion de concurrence.

ANNEXE : KRI, KCI et KPI

Référentiel / Domaine	KRI (Risque)	KCI (Contrôle)	KPI (Performance)
Gouverner	Évaluation financière et assurance des risques Rapports d'audit interne et externe Exceptions aux politiques	Rapport au comité d'audit et des risques Organisation et moyens (budget) Matrice de risques et plan de mitigations Référentiel des politiques et procédures	Couverture de la certification ISO 27001, 27701et autres Index de risque cyber/ Cyber notations/ Benchmark Évaluation des fournisseurs (annexes sécurité et protection des données)
Identifier	Inventaire des vulnérabilités avec criticité Inventaire des menaces (CERT, CTI)	Inventaire des actifs internes et des fournisseurs avec criticité Inventaire des systèmes surveillés / monitorés	Inventaire des risques évalués dans les projets, les processus opérationnels et les fournisseurs
Protéger		Résultats des sessions de sensibilisation obligatoires et des programmes ciblés par profils Statut des mesures de classification et protection des données	Résultats de tests de phishing Statut de la gestion des comptes à privilège Statut des tests des plans de continuité
Détecter			Nombre d'évènements collectés et analysés Nombre d'incidents détectés et gérés selon leur typologie et leur gravité
Réagir		Rapports d'investigation Notifications / Rapports aux autorités (CNIL, ANSSI)	Nombre d'incidents escaladés et traités selon leur priorité et catégorie Nombre de crises gérées
Restaurer		Rapport d'incident « post mortem » avec plan d'amélioration Notifications / Rapports aux autorités (CNIL, ANSSI)	Nombre de jours pour clore l'incident / la crise

6 - Prendre en compte et intégrer les régulations à venir

Par Arnaud BOILOT, Gilles BRUNET et Marjolaine ALQUIER

I - Enjeux de la question

En tant qu'acteurs de 2ième et 3ième lignes, les contrôleurs internes et les auditeurs internes doivent assurer aux organes de gouvernance et de direction que les nouvelles réglementations en matière de cybersécurité sont bien prises en compte dans l'entreprise.
Ces recommandations et conseils indépendants doivent toutefois être adaptés aux risques auxquels fait face l'entreprise. Aussi, bien cerner l'exposition de l'entreprise, voire celle de ses dirigeants (avec possibilité de responsabilité civile voire pénale personnelle et non seulement morale), est essentiel pour développer les dispositifs adéquats de contrôle interne et les programmes pertinents d'audit interne.

Pour réussir dans ce rôle d'aide à la décision, les équipes de Contrôle Interne et d'Audit Interne doivent impérativement se faire aider par les personnes compétentes, bien au-delà des équipes du contrôle et d'audit interne.

La législation pouvant évoluer dans le temps, il est essentiel d'assurer l'accompagnement des dirigeants au moment opportun. Cela permettra d'éviter une mise en conformité dans l'urgence si les conseils sont prodigués trop tardivement, ou de mobiliser inutilement des ressources et de fournir des conseils inappropriés si faits trop tôt (exemple : directive européenne encore non transposée en droit local). On notera enfin que le suivi du risque règlementaire et de ses implications éventuellement directes sur la responsabilité civile ou pénal du dirigeant peut constituer aussi une voie de sensibilisation forte au cyber-risque pour le top management. Il pourrait donc représenter un enjeu important dans les relations entre la 2ième et 3ième lignes d'un côté, et la Direction de l'autre.

II - Grands principes

Afin de répondre à ces enjeux, cinq grands principes peuvent être appliqués :

- **Veille réglementaire :** disposer d'un panorama le plus large possible, dynamique dans le temps, en anticipant les réglementations à venir et leur applicabilité à l'entreprise. A cette fin, les ressources internes mais aussi externes à l'entreprise peuvent être utilisées. Ne pas oublier non plus de prendre en compte toutes les géographies pertinentes et leurs instances de régulation (ex. : SEC aux Etats-Unis).

- **Cartographie des risques de cybersécurité :** une analyse détaillée des risques cyber de l'entreprise permettra de mieux prioriser les actions à mettre en place pour s'assurer de la conformité aux nouvelles réglementations.

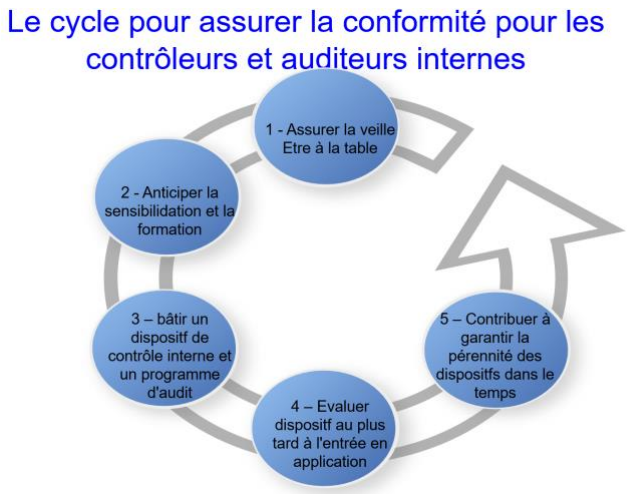
- **Coordination avec les autres fonctions d'assurance :** disposer du regard de spécialistes permettra d'avoir la pertinence nécessaire. A ce titre, les directions juridiques jouent un rôle clé, mais on peut citer également les directions Sécurité, IT et Compliance.

- **Sensibilisation et formation continue :** les nouvelles réglementations cyber s'appliquant à l'ensemble de l'entreprise (voir jusqu'à sa relation avec ses fournisseurs), les connaissances techniques des départements Sécurité ne sont aujourd'hui plus suffisantes. Répandre la culture cyber au sein de l'entreprise est nécessaire au moyen de formations et sensibilisations, y compris pour les dirigeants.

- **Dispositifs multi-réglementations :** se cantonner à une seule réglementation fait peser sur l'entreprise le risque d'une non-conformité par rapport à une autre réglementation. Pour assurer un effet de levier, il est préférable de se baser sur des bonnes pratiques cyber et sur différents référentiels reconnus. Variant peu dans le temps, ces bonnes pratiques et référentiels contiennent les points de contrôle clés reconnus internationalement. En s'en inspirant pour l'entreprise, les référentiels de contrôle interne et les programmes d'audit interne permettront une meilleure couverture du risque réglementaire.

III - Bonnes pratiques

L'Audit Interne et le Contrôle Interne sont deux fonctions distinctes mais complémentaires pour assurer la maîtrise des risques et la conformité réglementaire dans une entreprise ou une organisation.



Bonne pratique #1 - Assurer un minimum de veille / se tenir informés des évolutions : « Être à la table ! »

Pour assurer l'anticipation, il est nécessaire, pour les acteurs du risque, d'établir et d'entretenir un réseau de correspondants clés au sein de l'entreprise, mais aussi à l'extérieur de celle-ci, par exemple avec les Commissaires aux Comptes.
Il est en outre primordial de construire une relation pérenne et régulière avec la Direction Juridique. Grâce à leurs relations privilégiées, et forts de cette prise de connaissance anticipée des évolutions réglementaires, les contrôleurs et auditeurs internes seront mieux à même de communiquer au moment adéquat et assez tôt auprès des organes de gouvernance comme les Comités d'Audit et des Risques voire des Directions Exécutives. L'Audit Interne, aidée de la Direction Juridique, du Risk Management et de toute autre partie prenante doit jouer son rôle

d'éclaireur. Le *sponsoring* des comités de gouvernance est primordial pour mettre en œuvre les dispositions règlementaires dans l'entreprise et assurer la maitrise des risques.

Bonne pratique #2 - Anticiper la sensibilisation et la formation des contrôleurs/auditeurs internes

La maitrise des risques liés aux nouvelles réglementations ne peut être assurée qu'avec des personnels sensibilisés et formés aux nouvelles dispositions.
Les contrôleurs et auditeurs internes doivent préparer et organiser leur montée en compétence souvent dans des domaines nouveaux (ex. : protection des données, DORA, IA, NIS2…) et si possible bien avant l'entrée en application des règlementations. Cela passe notamment par des formations internes ou externes quand elles sont disponibles assez tôt.

Au minimum, il est conseillé de consulter les sites des autorités et institutions concernées, des associations professionnelles qui peuvent proposer des guides de mise en œuvre ou aider les entreprises dans la compréhension des textes. Intégrer des groupes de travail internes notamment avec les parties prenantes clés mais également externes au sein de réseaux professionnels dédiés est également un bon moyen de récolter de l'information et de développer par anticipation l'expertise sur les nouveaux sujets pour préparer la suite dans de bonnes conditions. Le décryptage de textes dans ses grandes lignes, et avec le soutien des juristes, est une étape indispensable pour les contrôleurs et auditeurs internes.

Bonne pratique #3 - Anticiper et bâtir un dispositif de contrôle interne et un programme de travail d'audit

Les nouvelles régulations induisent de nouveaux risques pour l'entreprise et peuvent nécessiter une révision de la cartographie des risques et des processus impactés. Les contrôleurs et auditeurs internes avec le Risk Management doivent identifier, évaluer et cartographier efficacement les risques liés aux nouvelles réglementations. Ces étapes sont indispensables pour mettre en place des dispositifs de contrôle adaptés et élaborer des plans d'audit pertinents sur les domaines impactés. La mise en place d'un dispositif de contrôle interne efficient doit être bâtie sur la base d'une cartographie des risques cybersécurité à jour et en fonction du niveau d'exposition de l'entreprise aux risques liés aux nouvelles dispositions réglementaires.

Comment néanmoins s'assurer que l'organisation ne sera pas dépassée par les ajouts de nouveaux risques et leurs contrôles ? En réalité, il sera plus aisé pour l'entreprise d'identifier et de prendre en compte les impacts des nouvelles réglementations si elle dispose déjà d'un **dispositif robuste de contrôle interne de la cybersécurité, basé sur les meilleures pratiques** de la profession et régulièrement évalué par les auditeurs internes et externes. L'écart de prise en compte en sera d'autant plus **minime et nécessitera que peu d'évolutions** pour être conforme. Ce **socle de contrôles de cybersécurité** issu des standards professionnels reconnus, indépendamment des réglementations, est la meilleure garantie pour l'entreprise de sa maitrise des risques cybersécurité et de sa conformité aux dispositions réglementaires en vigueur et à venir, **dans les temps et au meilleur coût**.

L'Audit Interne dans son rôle d'évaluation des dispositifs de contrôle interne doit construire assez tôt son plan d'audit et ses programmes de travail adaptés aux risques et aux activités impactées par les nouvelles réglementations.

L'Audit Interne pourra prévoir 2 niveaux de mission :

- Mission de gouvernance pour s'assurer de l'efficacité de l'organisation, de la pertinence de l'analyse des risques notamment ;
- Mission d'efficacité des contrôles sécurité mis en place pour couvrir les risques spécifiques.

Bonne pratique #4 - Être en capacité d'évaluer la maturité des dispositifs au plus tard à l'entrée en application

L'Audit Interne évalue et conseille sur l'intégration des nouvelles régulations, tandis que le Contrôle Interne met en place les dispositifs opérationnels pour s'y conformer au quotidien. Une collaboration étroite entre ces deux fonctions est essentielle pour être en capacité d'évaluer l'efficacité des dispositifs de maîtrise des risques et d'apporter une assurance aux organes de gouvernance sur le niveau de conformité de l'entreprise à la réglementation.
Pour une bonne maîtrise des risques, il est recommandé de réaliser un audit de gouvernance au plus tard 6 mois avant l'entrée en application de la réglementation et de réaliser des audits plus opérationnels dans l'année d'entrée en application.
Pour les plus petites structures impactées par la réglementation et avec des risques élevés, il est recommandé de procéder à un état des lieux avant l'entrée en application pour évaluer la pertinence de l'analyse d'impact et des risques et au plus tard dans les 6 mois, par les équipes d'Audit Interne ou des prestataires experts en cybersécurité.

Bonne pratique #5 - Contribuer à garantir la pérennité des dispositifs de contrôle dans le temps

Une fois les éventuels nouveaux contrôles identifiés pour répondre aux dispositions réglementaires, il est nécessaire de mettre à jour le référentiel de contrôle de cybersécurité de l'organisation et de tester régulièrement son efficacité. L'Audit Interne devra intégrer dans son plan d'audit annuel ou triennal des missions de gouvernance et sur l'aspect opérationnel. Pour confirmer la pertinence du dispositif de contrôle de cybersécurité, la bonne maîtrise des risques implique d'apporter régulièrement une assurance aux comités de gouvernance sur le niveau de conformité aux différentes réglementations.

Le maintien dans le temps de la veille réglementaire par les contrôleurs et les auditeurs internes est indispensable. Il nécessite un dialogue étroit et régulier avec la Direction Juridique, le Risk Management, le Compliance Officer et les Commissaires aux Comptes.

IV – Points d'attention

L'intégration des régulations à venir est un enjeu majeur pour les entreprises. Comprendre et anticiper ces risques est essentiel pour assurer une conformité à ces nouvelles régulations et éviter des sanctions potentielles. Il est d'autant plus important d'en tenir compte que des manquements peuvent entrainer des risques désormais de nature pénale pour les dirigeants eux-mêmes.

Les quatre principaux risques associés sont :

- **Complexité et sur-régulation**
  La complexité ainsi que le nombre croissant des régulations relatives à la cybersécurité constituent pour les entreprises un réel défi. C'est particulièrement vrai des multinationales qui doivent anticiper et tenir compte des réglementations nationales, internationales et extraterritoriales, certaines pouvant même être en contradiction entre elles.
  ⇨ *La clé est d'anticiper et d'identifier les acteurs (internes et externes à l'entreprise) sur lesquels s'appuyer pour développer une stratégie de conformité robuste qui prend en compte toutes ces variables*.

- **Mauvaise(s) interprétation(s)**
  Les mauvaises interprétations des régulations peuvent avoir des conséquences graves. Une compréhension erronée par la direction des nouvelles contraintes et opportunités peut accroître le risque civil voire pénal pour les dirigeants.
  De plus, sensibiliser et former l'ensemble de l'entreprise, y compris les dirigeants, les métiers et les opérationnels, est complexe. La méconnaissance des éléments clés des réglementations peut mener à des contrôles et des audits non pertinents, compromettant ainsi la conformité globale de l'entreprise.
  ⇨ *Afin d'éviter toute mauvaise interprétation il est important de se renseigner et de se former auprès d'associations ou d'organismes spécialisés.*

- **Fonctionnement en silo**
  L'isolement de l'audit ou du contrôle internes vis-à-vis des autres fonctions d'assurance, telles que l'IT, la direction juridique, la compliance, les assurances et les ressources humaines, peut entraîner une vision fragmentée de la conformité. Le manque d'implication du management ou bien encore une adhésion tardive aux nouvelles régulations peuvent également aggraver ce risque.
  ⇨ *Une approche intégrée et collaborative avec les différents acteurs de l'entreprise est essentielle pour surmonter ces défis.*

- **Temporalité inadéquate**
  Il est crucial de maintenir dans le temps les compétences des contrôleurs et auditeurs internes pour qu'ils restent à jour avec les évolutions réglementaires. De plus, l'absence d'anticipation, qu'il s'agisse de partir trop tôt ou trop tard, peut entraîner des lacunes dans la conformité.
  ⇨ *Une planification proactive et une formation continue sont indispensables pour garantir une conformité durable et efficace.*

V - Conclusions

Audit Interne

L'Audit Interne doit rester à l'affût des évolutions réglementaires à venir dans les domaines concernant l'organisation. Ses missions d'évaluation et de conseil doivent intégrer ces nouvelles exigences réglementaires :

- Analyser les impacts des nouvelles régulations sur les processus, les risques et les contrôles existants ;
- Évaluer le niveau de conformité de l'organisation par rapport aux nouvelles exigences ;

- Formuler des recommandations pour se mettre en conformité (actions, plans d'actions, etc...) ;
- Conseiller le management sur les meilleurs moyens d'intégrer ces nouvelles régulations ;
- Planifier des missions d'audit spécifiques sur les domaines impactés par les nouvelles régulations.

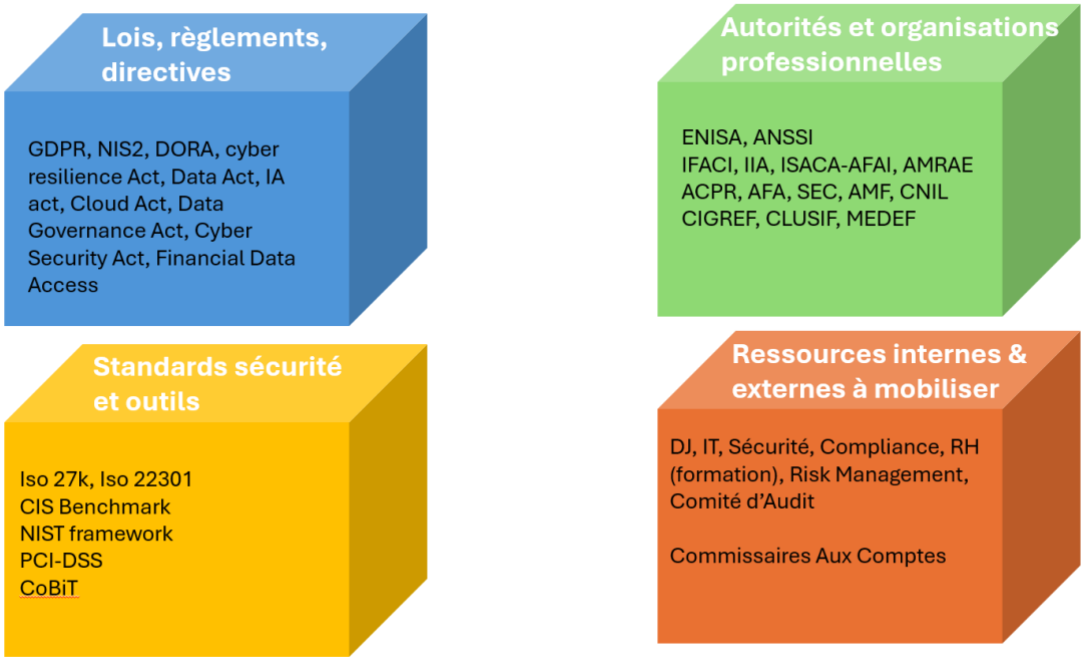
Contrôle Interne

Le dispositif de Contrôle Interne doit être adapté pour prendre en compte les nouvelles obligations réglementaires :

- Identifier et évaluer les nouveaux risques induits par les nouvelles régulations ;
- Définir et mettre en œuvre les nouveaux contrôles et procédures nécessaires ;
- Former les collaborateurs concernés sur les nouvelles exigences à respecter ;
- Intégrer les nouveaux contrôles dans les plans de contrôle permanent ;
- Assurer le suivi et le reporting de la mise en conformité.

En résumé, l'Audit Interne évalue et conseille sur l'intégration des nouvelles régulations, tandis que le Contrôle Interne met en place les dispositifs opérationnels pour s'y conformer au quotidien. Une collaboration étroite entre ces deux fonctions est essentielle.

Annexes



7 - Se tenir au courant de l'évolution du risque cyber – y compris au niveau géopolitique

Par Azou CHEKATT, Isabelle PINILLA et Xavier GUIFFARD

1. Enjeux

L'Agence de l'U.E. pour la cybersécurité met en avant l'élargissement des risques cyber aux trois dimensions du cyberespace : physique, logique et cognitive. La majorité des attaques ciblent les programmes informatiques ou les données, mais les attaques récentes ont également visé les infrastructures réseau et les installations industrielles. La couche cognitive, qui concerne l'information circulant sur le web 2.0, est la plus difficile à appréhender en raison de la difficulté à détecter les manipulations de l'information et les atteintes à la réputation et à la confiance numérique. En 2024-2025, la gestion du risque cyber nécessite donc une défense adaptée dans ces trois dimensions, avec une anticipation grâce à une vision dynamique de la cybersécurité.

De manière générale, le risque cyber connait une constante évolution via de nouvelles technologies (ex : émergence de l'intelligence artificielle) qui viennent s'ajouter à l'augmentation des attaques par ransomware, ou encore les risques supply chain, IoT, IA et cloud…issus de couches technologiques précédentes. La gestion de ce risque nécessite donc anticipation et vision dynamique afin d'assurer la mise en place d'une défense adaptée, ainsi qu'entre autres la sensibilisation des employés et dirigeants. Cette évolution rapide doit être mise en rapport avec la réalité d'un risque désormais avéré, avec des impacts devenus massifs et coûteux.

Le risque cyber est également lié à l'évolution de la situation géopolitique avec des risques d'espionnage et de cyberattaques potentiellement orchestrés par certains gouvernements, conduisant notamment les états à chercher à protéger leurs infrastructures critiques en excluant l'usage de technologies d'industriels étrangers. Par exemple, en France, les antennes 5G de l'industriel chinois Huawei devront être abandonnées dès 2031.

2. Grands principes

La conduite d'une veille et l'évaluation quotidienne des risques cyber deviennent clé pour l'entreprise afin de pouvoir réagir aux nouvelles vulnérabilités, failles zéro day, événements géopolitiques et changements de son écosystème modifiant son exposition. L'entreprise doit donc disposer d'une organisation, de processus et de ressources lui assurant une connaissance permanente de son périmètre et de ses expositions selon des informations fiables et à jour.

Tout ceci doit lui permettre d'évaluer continuellement les risques et de pouvoir réagir au plus tôt. Dans le détail, il s'agit de :

A. FORMALISER la fonction et la mission de suivi du risque cyber ;
B. CONNAITRE son périmètre et son exposition incluant l'écosystème de l'entreprise (partenaires, géographie, ...) ;
C. S'ALIMENTER d'une information fiable et à jour, auprès de différentes sources (étatiques, prestataires, partenaires, ...) ;
D. ANALYSER le risque en partant du « métier » ;
E. PARTAGER l'analyse de risque au sein de l'organisation ;
F. AGIR face à l'évolution du risque.

3. Les bonnes pratiques

A. FORMALISER : Inclure la veille permanente, l'évaluation des risques dans les Politiques

Il s'agit de s'assurer que l'entreprise a bien décliné l'activité de veille permanente des risques, de leurs évaluations et de leurs suivis dans son organisation et dans ses procédures. Ainsi, l'auditeur devra s'assurer que :

- Les rôles et responsabilités sont formalisés (RACI, fiches de postes et missions) ;
- Toutes les politiques d'évaluation des risques et de gestion des fournisseurs sont en place et permettent une évaluation des parties prenantes comme dans la méthode EBIOS RM de l'ANSSI ;
- Les risques par pays sont identifiés et régulièrement revus (écosystème et la Supply Chain inclus).

B. CONNAITRE : Maîtriser son périmètre et son exposition incluant l'écosystème de l'entreprise (partenaires, géographie, ...)

En premier lieu, l'entreprise doit disposer d'une vision à jour de son écosystème et des processus clés de l'inventaire de ses actifs critiques (matériels et immatériels) et leurs implantations géographiques incluant les obligations réglementaires par pays, des technologies (version en place) qu'elle utilise et celles qu'utilisent ses partenaires (ex : cloud, éditeurs identifiés à risques). La revue des BIA (Business Impact Analysis) doit être réalisée afin de s'assurer que les processus clés et actifs critiques sont identifiés.

Puis l'auditeur vérifiera qu'un catalogue pertinent de contrôles adressant les scénarios de risques identifiés est bien en place. L'auditeur vérifiera également que les contrôles et audit & pentest sont conduits et documentés avec actions correctives suivies. Il pourra utiliser différents référentiels de contrôles cyber (CIS Framework, ISACA, ENISA, ANSSI, MITRE, ISO 27002/01, PCI DSS, etc....). La revue des clauses contractuelles avec les partenaires en matière de cyber doit être également en place.

Aussi, l'auditeur vérifiera qu'une activité de Cyber Threat Intelligence (CTI) est en place afin de détecter les menaces et risques Cyber en amont. Cette veille peut être réalisée en interne avec des outils comme OpenCTi, avec des sources disponibles sur internet (Ex. : MANDIANT, réseau CERT, Dark web, etc…), ou encore via des prestataires externes (Ex. : CITALID, Orange Cyberdéfense, etc…).

Enfin, l'auditeur évaluera le processus de détection et de réponse aux incidents Cyber qui devra être en place et intégrer tout l'écosystème de partenaires pouvant impacter la cybersécurité. Cela passera par la revue du système de collecte des logs de sécurité (SIEM/SOC) et des use cases ; l'analyse des incidents et leur réponse sur une période donnée ; et l'assurance que des revues régulières des incidents de Cyber sont conduites avec les partenaires. L'auditeur pourra se référer au référentiel de L'ANSSI « Crise d'Origine Cyber – Les clés d'une gestion opérationnelle et stratégique » (voir https://cyber.gouv.fr/sites/default/files/2021/12/anssi-guide-gestion_crise_cyber.pdf).

C. *S'ALIMENTER : Garantir la fiabilité des sources*

La surveillance de l'évolution du risque cyber suppose une veille et des échanges auprès de sources fiables (Ex. : ANSSI, ENISA, ComCyber-MI, DGSI, CERT FR, …), notamment les régulateurs qui disposent le plus souvent de structures sectorielles adaptées au domaine de l'entreprise, ainsi que le développement par les personnes en charge de réseaux professionnels et personnels avec leurs pairs et d'autres spécialistes, du monde universitaire par exemple.

Fiabiliser les sources d'information et de constats peut nécessiter également un accompagnement par une sous-traitance spécialisée : c'est le rôle de la Cyber Threat intelligence.

Enfin, la formation des collaborateurs auprès des grands instituts de sécurité (Ex. : IHEMI, IHEDN, IFACI…) contribue au développement d'experts internes en même temps qu'elle favorise contacts et exposition auprès de sources d'information fiables pour l'organisation.

D. *ANALYSER : Effectuer une analyse de risques*

Il serait impossible voire contreproductif d'essayer de se tenir au courant de l'évolution du risque cyber dans une approche holistique sans prendre en compte les spécificités de l'organisation. Le risque cyber est bien trop diffus et hétérogène pour être aborder sans angle particulier.

C'est pourquoi il est nécessaire de procéder à une analyse de risque afin de déterminer quels sont les scenarios de risques majeurs qui concerne votre périmètre. Cette analyse doit partir des ressources critiques pour l'activité de l'organisation pour lesquelles la disponibilité, l'intégrité ou la confidentialité pourraient être affectées par des actions cybernétiques de sabotage (perturbation/interruption d'activité), de chantage / atteinte à l'image (vol et divulgation de données), manipulation (hacktivisme / influence),

d'espionnage (vol de données sensibles), ou encore de fraude (détournement de fond / usages illicites) – *[voir entre autre Q1/ Les impacts opérationnels concrets du risque cyber pour des réflexions et approches autour de ces sujets]*.

Chaque scenario est identifié au croisement d'une ressource critique (ex. : base de données des clients, code source d'une solution logicielle militaire) ; d'un ou plusieurs types d'atteinte (ex. : disponibilité, confidentialité ou intégrité) ; d'une ou plusieurs conséquences (ex. : perturbation / interruption d'activité, vol de données sensibles, etc…) ainsi que d'une catégorisation de l'origine de la menace (ex. : criminalité, acteur étatique, etc…).

Entre autres méthodes, la méthode EBIOS Risk Manager (EBIOS RM) publiée par l'ANSSI avec le soutien du Club EBIOS permet cette analyse de risques et propose une boite à outils adaptable à vos objectifs en la matière.

Il sera ensuite possible de cibler pertinemment le suivi de l'évolution du risque cyber en fonction des scenarios de risques identifiés pour l'organisation.

E. PARTAGER : Sensibiliser les parties prenantes

Le risque cyber concerne toutes les composantes de l'organisation et l'ensemble des métiers. Il suppose donc une approche transverse et un pilotage constant. Si la fonction de RSSI est cardinale pour réduire le risque, la bonne information du Top management et la volonté de ce dernier est essentielle à une défense adaptée. La stratégie de sécurité est globale doit donc être pilotée au-delà du seul RSSI. Le suivi de l'évolution du risque cyber doit ainsi être partagée à l'intérieur et autour de l'organisation, à travers notamment :

- Une politique de formation adaptée pour diffuser l'esprit de protection cyber dans toutes les couches de l'organisation ;
- Une politique de veille et de dialogue extérieur au-delà des seuls régulateurs ou des institutionnels, pouvant inclure un partage des retours d'expérience avec les organisations professionnelles, ou encore un renforcement du lien avec le monde de la recherche universitaire.

Enfin la sensibilisation ne parait efficace que lorsqu'un niveau suffisant de questions et de doutes finit par interroger le top management : Sommes-nous exposés ? Sommes-nous bien protégés ? *[Pour aller plus loin, voir Q2/Sensibiliser le top management, et avec quel tableau de bord]*

F. AGIR : Garantir la bonne réaction

Bien sûr, se tenir au courant de l'évolution du risque cyber doit **permettre à l'organisation de réagir en fonction de son évolution**. L'objectif est d'**anticiper au maximum** la survenue d'un évènement qui pourrait nuire à l'entité et de prendre à temps les mesures les plus appropriées pour **l'empêcher, en réduire les effets et les éviter ou à défaut préparer la crise**.

Pour ce faire, il est nécessaire de compléter l'analyse des scenarios de risque par une **matrice de criticité** au croisement de l'impact maximal estimé selon des seuils (financiers notamment) aux bornes de l'organisation (limité, significatif, critique, catastrophique) et de la probabilité d'occurrence (peu probable, rare, possible, fréquent).

La criticité permet de catégoriser les risques (limité, modéré, fort ou majeur) et de déterminer la conduite à tenir via une **matrice de priorisation** au regard des moyens d'action (cf. annexe « cartographie des risques ») :

- Traitement prioritaire pour les **risques forts ou majeurs** sur lesquels les **moyens d'actions sont (très) significatifs** (Par exemple : risque de rançongiciel sur le système de gestion des clients qui peut être fortement réduit par la mise en place d'une sauvegarde offline régulière) ;
- Surveillance renforcée pour les **risques forts ou majeurs** sur lesquels les **moyens d'actions sont limités** (exemple : risques de vendor locking ou d'impact maximum en raison d'une défaillance d'un fournisseur clé – tel que, par exemple, la panne informatique mondiale de juillet 2024 déclenchée suite à une mise à jour défectueuse de Crowdstrike) ;
- Zone d'amélioration pour les **risques limités ou modérés** sur lesquels les **moyens d'actions sont (très) significatifs** ;
- Veille pour les autres risques limités ou modérés.

Cette approche peut être affinée par une **quantification du risque cyber** qui consiste à modéliser le plus précisément possible les conséquences financières de la réalisation d'un scenario de risque. Modéliser signifie identifier et évaluer tous les types de coûts associés (remise en état, perte de productivité, perte de C.A., atteinte réputationnelle, coûts règlementaires…). Il est possible de travailler pour cela avec un partenaire spécialisé. Certains éditeurs, y compris en France, peuvent proposer la modélisation et la maintenance des scénarios selon des méthodologies dédiées (FAIR notamment), voir même gérer l'évolution de la menace (avec ajout de Cyber Threat Intelligence). Grâce à ces éditeurs, on peut ainsi obtenir une quantification dynamique du cout maximal de réalisation de chaque scenario et de l'exposition annuelle moyenne (cout moyen annuel estimé de la réalisation d'un scenario)[2].

En parallèle de ces démarches d'évaluation, il est nécessaire de mettre en place un dispositif concret de réaction à travers :

- Un **processus formel d'alerte et d'escalade** permettant à l'organisation de **prendre les bonnes décisions en fonction de l'évolution d'un risque identifié**. Par exemple, si un scenario de risque dont l'impact serait significatif voit sa probabilité d'occurrence augmenter de rare à possible du fait d'un évènement géopolitique (Ex. : déclenchement d'un conflit), sa criticité passera de modérée à forte et ce scenario requerra dès lors un

[2] Voir par exemple ci-contre une liste d'entreprise française dont CITALID, créée par deux anciens de l'ANSSI https://www.silicon.fr/Thematique/cybersecurite-1371/Breves/Gestion-du-risque-cyber-pourquoi-il-faut-outiller-387156.htm#:~:text=Concurrent%20d'Egerie%20et%20d,contexte%20IT%20de%20l'entreprise.

traitement prioritaire. Il est nécessaire que le processus d'alerte du management soit établi et suivi afin de garantir la mise en œuvre des mesures nécessaires.

- Des **plans de continuité / reprise d'activité formalisés (PCA, PRA) et prêt à l'emploi** en cas de réalisation d'un scenario de risque. Ces plans peuvent comprendre des phases préparatoires qui sont à activer lors de l'émergence du risque (exemple : lancement de la restauration des sauvegardes sur le data center de secours).
- Des **tests réguliers des dispositifs de gestion de crise** afin de garantir leur efficacité et leur fonctionnement fluide en cas de besoin.

4. Conclusion - Points d'attention

Se tenir informé de l'évolution du risque cyber n'est pas une option. Cette démarche est fondamentale pour une approche maîtrisée du risque cyber dans l'organisation et son écosystème étendu. Elle nécessite de maintenir des scenarios de risques évalués et/ou quantifiés et permet d'anticiper et de réagir afin de protéger au mieux l'organisation.

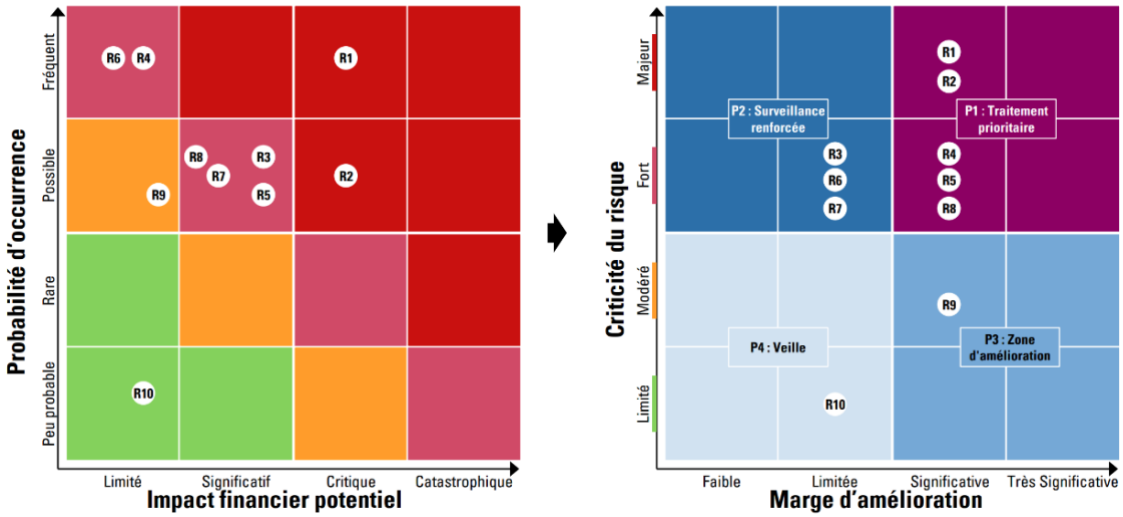
Il est crucial de ne pas l'ignorer, en particulier dans un monde ou les changements géopolitiques influent de plus en plus sur le risque Cyber. L'approche doit donc être par définition dynamique : il est dangereux de se fonder sur une vision statique (il faut donc veiller entre autres à la bonne réactualisation des sources d'information).

L'exercice requiert des compétences cyber et métiers et ne doit pas être cantonné aux personnes en charge de la cybersécurité. Il faut donc s'assurer qu'il existe, par exemple, une bonne compréhension entre les acteurs au profil cyber / CTI (Cyber Threat Intelligence) et éventuellement les profils « géopolitiques » dans l'organisation.

On notera par ailleurs que la maîtrise du risque cyber est clé pour éviter que les évaluations externes non sollicitées réalisées par des agences de rating soient les seuls référentiels pour les partenaires (assurances notamment) et/ou clients. De manière plus générale, il est nécessaire de développer un réseau large d'informations afin de ne pas dépendre que d'une seule source et de recouper l'information. Il est important de disposer de sources françaises qualifiées, idéalement au plus haut niveau institutionnel. Il peut aussi être utile d'avoir des sources étrangères, y compris hors Union Européenne, tout en prenant note de la nécessité de toujours maintenir des sources souveraines.

Enfin, se tenir informé de l'évolution du risque cyber doit impérativement permettre le déclenchement de mesures de réaction concrètes si le risque devient significatif pour l'organisation. Rien ne serait plus dommageable que de ne pas réagir à la réalisation d'un risque identifié et suivi. Il est donc nécessaire, comme cela a été déjà rappelé plus haut, de réfléchir en amont à un système d'escalade avec actions concrètes en fonction du niveau d'alertes.

ANNEXE CARTOGRAPHIE DES RISQUES (EXEMPLE) :



Les seuils d'impacts peuvent par exemple être catégorisé en fonction du chiffre d'affaires ou du résultat. Par exemple, l'impact peut être :

- *Limité si la perte de chiffre d'affaires estimée est inférieure à 1 millions d'euros ;*
- *Significatif si la perte de chiffre d'affaires estimée est supérieure ou égale à 1 millions d'euros et inférieure à 5 millions d'euros ;*
- *Critique si la perte de chiffre d'affaires estimée est supérieure ou égale à 5 millions d'euros et inférieure à 10 millions d'euros ;*
- *Catastrophique si la perte de chiffre d'affaires estimée est supérieure ou égale à 10 millions d'euros.*

8 - Sensibiliser les collaborateurs, développer une « cyber-hygiène » et mieux contrôler le facteur humain

Par Audric YEPNDJOUO, Charline GARNIER et Olivier MEYER

I - Enjeux de la question

D'après une étude d'IBM Security Services[3], 90% des incidents cyber sont liés au facteur humain (autant dans le monde civil que dans le monde militaire).

Post-covid 19, l'augmentation du télétravail introduit plusieurs risques de cybersécurité spécifiques, liés notamment à l'environnement de travail à distance (isolement des salariés), l'utilisation de dispositifs personnels (configurations de sécurité faibles) et la dépendance accrue aux technologies de communication numérique (utilisation des réseaux Wi-Fi publics ou domestiques non sécurisés). Les contrôles techniques sont essentiels pour sécuriser une entreprise face aux menaces cyber, mais ils ne sont pas suffisants. Une approche de sécurité complète et efficace doit inclure plusieurs dimensions.

Selon Kaspersky Daily[4]*, près de la moitié des incidents de cybersécurité (46%) sont imputables à un manque de précaution ou de formation des collaborateurs, mettant en évidence l'importance du facteur humain dans la prévention des attaques. La formation et l'information des collaborateurs deviennent la pierre angulaire de la défense contre les cyberattaques. La mise en place d'une formation exhaustive des collaborateurs instaure une culture "cyber" au sein des entreprises. Enfin, on peut noter que dans certaines grandes entreprises, la remontée de l'état de ce risque humain pour la cybersécurité de l'organisation peut se faire jusqu'au niveau d'un suivi mensuel au Comex : cela illustre l'importance de la question.

La responsabilité de la sensibilisation aux risques de cybersécurité des collaborateurs d'une entreprise est souvent partagée entre plusieurs parties prenantes :

- La direction générale a la responsabilité ultime de garantir que la sécurité de l'information est une priorité pour l'ensemble de l'organisation. Ce point est traité dans Q2 / Sensibiliser le top management, et avec quels types de tableau de bord.
- Le RSSI est généralement le principal responsable de la mise en œuvre des programmes de sensibilisation à la cybersécurité. Il élabore les politiques, organise les formations et assure la communication des meilleures pratiques de sécurité. Le RSSI est un expert du sujet ; cependant, une approche trop technique pourrait mener à élaborer des formations ou des documents trop spécialisés et difficilement compréhensibles pour l'ensemble des collaborateurs.
- Les RH jouent un rôle clé en intégrant la sensibilisation à la cybersécurité dans le processus d'onboarding des nouveaux employés et en organisant des sessions de formations régulières pour l'ensemble du personnel. Cependant, la fonction RH n'a pas toujours conscience ou connaissance de l'importance des risques associés.
- Les managers ont également une part de responsabilité : ils doivent s'assurer que leurs équipes comprennent et suivent les politiques de sécurité.

Les rôles et responsabilités ne sont pas toujours clairement déterminés dans cette gouvernance de sensibilisation. Dans ce contexte, l'équipe d'Audit Interne peut se positionner pour améliorer

[3] IBM Security Services 2014 Cyber Security Intelligence Index
[4] https://www.kaspersky.com/blog/the-human-factor-in-it-security/

ce processus et s'assurer que les programmes de sensibilisation en place sont efficaces. Mesurer l'efficacité des sensibilisations aux risques cyber est crucial pour s'assurer que les employés comprennent et appliquent les meilleures pratiques de sécurité.

La formation ne doit pas être sélective et doit toucher tous les échelons de l'entreprise. Elle doit également être continue pour garantir la mise à jour constante des connaissances, cruciale pour atténuer les risques. L'inclusivité est essentielle, avec des solutions de formation adaptées à chaque niveau et à chaque collaborateur. Un risque de "training fatigue" est à prendre en compte et l'utilisation d'outils ludiques est essentielle pour maintenir l'intérêt du collaborateur. De plus, la documentation liée à la cybersécurité en interne (PSSI, SMSSI et autres règles internes) doit être adaptée et accessible aux collaborateurs pour assurer une mise en pratique adéquate des bases acquises pendant les formations et une meilleure résilience opérationnelle.

II - Grands Principes

A. Dans le contexte actuel de cybermenaces croissantes, une simple formation de sensibilisation des utilisateurs ou des nouveaux arrivants n'est plus suffisante. Une **véritable stratégie de sensibilisation des utilisateurs aux risques cyber** est essentielle pour protéger les entreprises contre les attaques potentielles et faire des utilisateurs la première ligne de défense de l'entreprise.

B. Cette stratégie doit être conçue de manière à prendre en compte les **risques spécifiques** de l'entreprise et à **cibler particulièrement les utilisateurs présentant des risques plus élevés**. Toutefois, elle doit également assurer un **socle commun** de connaissances pour tous les employés, garantissant ainsi une base solide de sensibilisation à la cybersécurité.

C. Pour garantir l'efficacité de cette stratégie, il est impératif de mettre en place un **processus de mesure de son impact**. Bien que cela puisse représenter un défi, ce processus est crucial pour identifier les points forts et les faiblesses de la stratégie et pour effectuer les ajustements nécessaires.

D. Par ailleurs, il est essentiel de promouvoir une **culture de transparence et de remontée des anomalies sans crainte de sanctions sévères**. Une telle culture encourage les employés à signaler les incidents de sécurité sans hésitation, ce qui permet à l'entreprise de réagir rapidement et efficacement.

E. Enfin, il est nécessaire que la stratégie de sensibilisation reste **flexible et s'adapte aux évolutions technologiques** (Ex. : low code / code minimal, intelligence artificielle, etc...) ainsi qu'au contexte potentiellement changeant de risque pour l'entreprise.

III - Bonnes pratiques

A. <u>Une stratégie de sensibilisation doit être définie</u>

Une simple formation, aussi élaborée soit-elle, ne peut être considérée comme suffisante pour définir une stratégie de sensibilisation des utilisateurs. Cette stratégie doit être

définie et documentée afin d'assurer la cohérence des actions menées avec les risques et les objectifs de l'entreprise. Cette stratégie de sensibilisation doit :

- Définir les rôles et responsabilités de chaque partie prenante (RSSI, RH, manager) ;
- Avoir des objectifs clairs qui sont à la fois atteignables et mesurables ;
- Être basée sur une identification des risques pour l'entreprise et doit permettre de couvrir les risques identifiés les plus pertinents ;
- Identifier les populations nécessitant des actions ciblées ;
- Faire l'objet d'une mesure périodique de son efficacité ;
- Être soutenue via un engagement fort de la direction pour montrer l'importance de la sensibilisation et des bonnes pratiques ;
- Faire l'objet d'une révision périodique afin de s'assurer qu'elle reste alignée avec les nouveaux risques pour l'entreprise.

Pour les entreprises les plus matures (ou pour les auditeurs / contrôleurs internes souhaitant revoir une stratégie de sensibilisation), la stratégie pourra être basée sur un cadre de contrôle comme le NIST 800-50r1 « Building a Cybersecurity and Privacy Learning Program »[5].

B. Importance d'Actions Spécifiques en Fonction des Risques et des Populations dans un Programme de Sensibilisation à la Cybersécurité

Une sensibilisation générique constitue la première étape d'une stratégie de sensibilisation à la cybersécurité, mais elle ne doit pas être la seule. Il est crucial de compléter cette base par des actions spécifiques adaptées aux différents risques et populations au sein de l'entreprise. Cette approche ciblée permet de mieux couvrir les diverses vulnérabilités et menaces auxquelles l'organisation peut être confrontée. Les audits internes peuvent jouer un rôle fondamental dans cette démarche en évaluant régulièrement l'efficacité des actions de sensibilisation et en recommandant des ajustements pour répondre aux évolutions des risques et des technologies.

Identifier les populations à risque spécifique est essentiel pour déployer des actions de sensibilisation efficaces. Par exemple, les développeurs nécessitent une sensibilisation particulière concernant la gestion du cycle de vie du développement logiciel (SDLC – Software Development Life Cycle) afin de prévenir les vulnérabilités dans le code qu'ils produisent. De même, les équipes chargées de manipuler des données personnelles ou critiques doivent être formées spécifiquement sur les meilleures pratiques de protection et de gestion de ces informations sensibles.

La sensibilisation doit également être adaptée en fonction de la typologie de la population. Les jeunes et les nouveaux arrivants sur le marché du travail, par exemple, peuvent ne pas avoir acquis tous les bons réflexes en matière de cybersécurité. Pour ces groupes, il est essentiel d'inclure des modules de formation qui couvrent les bases de la sécurité numérique et des comportements sûrs en ligne. En intégrant ces nouvelles recrues dans une culture d'entreprise forte, axée sur la sécurité, on renforce leur engagement et leur vigilance face aux cybermenaces. On pourra aussi noter que la sensibilisation des managers peut aussi avoir un effet d'entrainement sur l'ensemble des populations encadrées : elle peut constituer une approche supplémentaire pour augmenter efficacité et efficience des stratégies générales de sensibilisation.

[5] https://csrc.nist.gov/News/2023/nist-releases-draft-sp-800-50-rev-1

L'équipe d'Audit Interne pourra notamment utiliser ce tableau ci-dessous pour identifier certaines populations spécifiques dans sa propre entreprise.

Exemples de populations présentant des risques spécifiques		
Population	**Risques Spécifiques**	**Enjeux**
Cadres et dirigeants	Phishing ciblé (spear phishing), ingénierie sociale, ransomware	Protection des informations stratégiques de l'entreprise, risques de réputation et financiers élevés
Développeurs et équipes techniques	Exposition à des vulnérabilités logicielles, pratiques de codage non sécurisées, accès privilégié à des systèmes sensibles	Protection des données sensibles, garantie de la sécurité des infrastructures critiques, prévention des fuites de données
Employés travaillant à distance	Utilisation de réseaux non sécurisés, partage de fichiers non sécurisé, manque de mise à jour des logiciels	Protection des données personnelles et professionnelles, prévention des accès non autorisés, maintien de la sécurité des informations
Personnel administratif	Hameçonnage (phishing), manipulation des données, utilisation de logiciels non autorisés	Protection des données personnelles et professionnelles, prévention des fraudes internes, gestion des accès
Nouveaux employés	Manque de connaissance des politiques de sécurité, susceptibilité aux attaques de phishing, erreurs humaines	Intégration sécurisée dans l'entreprise, prévention des failles de sécurité dues à l'ignorance, renforcement de la culture de sécurité dès l'entrée en fonction
Tierces parties (fournisseurs, partenaires)	Accès à des systèmes et données sensibles, mauvaise gestion des accès, pratiques de sécurité hétérogènes	Sécurisation de la chaîne d'approvisionnement, protection des informations partagées, gestion des risques de tiers
Administrateurs système et réseau	Accès privilégié aux systèmes et données, mauvaise configuration des systèmes, absence de gestion des accès	Maintien de l'intégrité et de la disponibilité des systèmes, prévention des abus d'accès, renforcement de la sécurité des infrastructures informatiques

C. La mesure de l'efficacité des actions de sensibilisation

La stratégie de sensibilisation étant aujourd'hui l'un des axes majeurs de la défense contre les risques cyber, il est indispensable que l'Audit et le Contrôle Interne s'assurent que des processus d'évaluation de l'efficacité des mesures et de l'atteinte des objectifs sont en place.

Si la mise en œuvre de KPI standard sur l'exécution des actions de sensibilisation est nécessaire (par exemple, le taux de la population de l'entreprise ayant suivi une formation

ou le nombre de campagnes de phishing réalisé), ils ne doivent pas être considérés comme suffisant pour s'assurer de l'efficacité de la stratégie de sensibilisation.

La compréhension des messages ou la réussite des campagnes simulées sont de meilleurs indicateurs de l'impact de la stratégie (surtout l'évolution de ces résultats dans le temps) et sont souvent fournis par défaut par les outils de formation (par exemple le taux de réussite à un quizz) ou par les fournisseurs de tests de phishing. Sur ces derniers, il est notamment intéressant de suivre à la fois le taux de mauvais clic (c.a.d., les utilisateurs qui « tombent dans le piège »), mais également le taux de déclaration de ces mails aux équipes de sécurité.

La mesure doit également permettre de vérifier l'efficacité de la stratégie de sensibilisation pour l'entreprise en analysant la couverture des risques spécifiques à l'entreprise (par exemple, les taux de risques élevés qui ont fait l'objet d'une action de sensibilisation), ou bien des populations présentant des risques spécifiques.

Enfin, la mesure de l'efficacité des campagnes de sensibilisation ne doit pas se focaliser uniquement sur les exercices. Des indicateurs sur les incidents réels doivent compléter le panel pour s'assurer de l'efficacité de la stratégie, comme par exemple le nombre d'incidents de sécurité.

Une fois l'existence d'un socle d'indicateur confirmé, il faut ensuite s'assurer d'un reporting régulier de ces derniers, et surtout de l'existence de plan d'action lorsque ceux-ci ne sont pas au niveau ou lorsque l'évolution montre une faible efficacité de la stratégie de sensibilisation.

D. Favoriser la remontée des incidents

La sensibilisation des utilisateurs à la cybersécurité est une composante essentielle de la protection des systèmes d'information des entreprises. Parmi les actions clés à mener, la remontée d'incidents joue un rôle crucial pour limiter l'impact des cyberattaques et améliorer la posture de sécurité globale.

La première étape consiste à formaliser et à communiquer clairement aux employés les procédures à suivre en cas d'incident de cybersécurité. Ces procédures doivent être accessibles et compréhensibles par tous, et définir les étapes à suivre pour signaler un incident, telles que la nature de l'incident, les informations à fournir et les contacts à privilégier.

Faciliter la remontée d'incidents est essentiel. L'entreprise doit mettre à disposition des employés des canaux de communication dédiés, tels qu'une adresse e-mail spécifique, un numéro de téléphone ou un portail en ligne sécurisé. Ces canaux doivent être clairement communiqués et accessibles facilement par tous les collaborateurs. Des boutons de reporting des e-mails de phishing constituent une bonne pratique à implémenter.

Pour inciter les employés à signaler les incidents sans crainte, il est important de mettre en place des mécanismes de récompense et de reconnaissance. Cela peut inclure des primes financières, des valorisations individuelles ou collectives, ou des formations complémentaires sur la cybersécurité.

L'analyse des incidents remontés est une source précieuse d'enseignements pour améliorer la posture de sécurité de l'entreprise. Il est crucial de mettre en place un processus de retour d'expérience permettant d'identifier les failles de sécurité, de corriger les vulnérabilités et d'adapter les procédures de gestion des incidents en conséquence.

E. La stratégie de sensibilisation doit pouvoir s'adapter aux évolutions des risques

Les nouvelles technologies, telles que l'intelligence artificielle (IA) et le low code qui sont traités dans le Guide (*voir Q9/Le risque cyber dans les projets informatiques, y compris cloud, low-code, IA*), apportent également de nouveaux risques qui doivent être intégrés dans la stratégie de sensibilisation. Une stratégie rigide, qui ne s'adapte pas aux évolutions technologiques et environnementales, sera inefficace à long terme. Il est donc indispensable de mettre en place une stratégie flexible et évolutive, capable de s'adapter aux innovations technologiques et aux nouvelles menaces qu'elles peuvent engendrer.

Il faut également tenir compte de l'environnement de l'entreprise et de la société dans son ensemble (« threat intelligence ») pour identifier les nouvelles tendances ou les nouveaux risques sur lesquels sensibiliser les utilisateurs. Par exemple un cas concret en 2024 : l'utilisation accrue des QR Code dans le cadre d'un grand évènement sportif en France entraine des risques d'attaque par QR Code (« quishing ») qui pourrait faire l'objet de sensibilisations spécifiques pour les entreprises *(A noter : sur l'évolution des risques, voir Q7/ Se tenir au courant de l'évolution du risque cyber – y compris au niveau géopolitique)*. De manière plus pragmatique, un changement significatif dans l'environnement de l'entreprise (acquisition, nouveau marché, nouveau produit) devrait faire l'objet d'une analyse de risque pour adapter la stratégie de sensibilisation.

IV - Facteurs de Risques

Une stratégie de sensibilisation à la cybersécurité est un outil essentiel pour protéger les entreprises contre les cybermenaces. Cependant, elle ne peut à elle seule couvrir tous les risques, notamment ceux liés à la malveillance interne. Les employés, bien qu'informés et formés, peuvent parfois représenter une menace s'ils agissent de manière malveillante ou négligente. Par conséquent, une vigilance accrue et des mesures supplémentaires doivent être mises en place pour atténuer ces risques internes.

Le facteur humain est l'un des aspects les plus complexes à maîtriser dans la cybersécurité. Même une stratégie de sensibilisation bien conçue peut être mise à mal si les employés subissent du stress ou une pression professionnelle intense, ce qui peut réduire leur vigilance face aux attaques. Ainsi, il est crucial d'intégrer des mesures de bien-être au travail et de gestion du stress dans le programme de sensibilisation afin de maintenir une attention constante des employés aux menaces potentielles. En outre, comme déjà rappelé plus haut, il faut prendre garde aux effets de fatigue du training qui peuvent banaliser les efforts de sensibilisation et les rendre moins efficace – ou pire, conduire à leurs évitements. Il faut donc s'assurer de l'attractivité et de l'intérêt bien compris de ceux-ci.

Enfin, comme noté en introduction, il s'agit d'une responsabilité partagée avec plusieurs départements de l'entreprise dont les Ressources Humaines. La multiplicité des acteurs peut constituer un facteur de risques, surtout si le sujet est mal perçu, mal expliqué ou bien n'est pas

introduit dans les KPI d'actions à réaliser (ex : % de complétion de programmes de sensibilisation pour telles ou telles populations).

Conclusion

En conclusion, pour qu'un programme de sensibilisation à la cybersécurité soit véritablement efficace, il doit non seulement former les employés aux bonnes pratiques en fonction de leurs attributions mais aussi évoluer en fonction des nouvelles menaces et technologies. Les audits internes jouent un rôle crucial en identifiant les faiblesses de ces programmes et en veillant à ce que les stratégies de sensibilisation restent pertinentes et efficaces. Les points essentiels ont été regroupé dans un programme de question pour aider un auditeur généraliste dans la réalisation de l'audit, disponible en annexe.

Annexes

Annexe 1 – tableau exemple de KPI pour mesurer l'efficacité de la stratégie de sensibilisation

KPI	Objectif du KPI	Exemple concret d'objectif
Taux de participation et d'engagement	Suivre le taux de participation aux questionnaires, ateliers, formations et autres actions de sensibilisation	90% de la population cible a suivi une formation sur l'année passée
Taux de réussite	Suivre le taux de réussite des participants aux questionnaires, ateliers, formations et autres actions de sensibilisation	Tous les participants doivent avoir 75% de bonne réponse pour valider une formation
Taux de clics sur les simulations de phishing	Pourcentage d'utilisateurs qui cliquent sur des liens ou pièces jointes malveillants dans des e-mails de simulation de phishing.	Objectif de moins de 10% de taux de clic sur les simulations Objectif de 90% d'utilisateurs ayant cliqué plus de 3 fois qui participent à des formations spécifiques
Taux de signalement des e-mails suspects	Pourcentage d'utilisateurs signalant des e-mails suspects aux équipes de sécurité.	Objectif de 20% d'utilisateurs qui remonte les e-mails des campagnes de phishing
Nombre d'incidents de sécurité	Suivi du nombre d'incidents de cybersécurité avant et après les campagnes de sensibilisation afin de valider la prise de conscience des employés aux risques	Réduction de 30% des incidents de sécurité lié à des clics sur des e-mails frauduleux
Suivi de la sensibilisation par rapport aux différentes lignes de services	L'objectif est d'identifier les populations qui obtiennent les moins bonnes réponses lors de campagne de phishing et de comprendre la raison.	Suppression des freins identifiés et adaptation de la sensibilisation à chaque population
Mise en place de plan d'actions	En cas de mauvais résultats lors des tests, mettre en place de nouvelles actions de sensibilisation ou adapter la stratégie de sensibilisation afin que les collaborateurs s'améliorent	Amélioration significative des résultats des populations identifiées

Annexe 2 – Guide d'audit pour la revue de la stratégie de la sensibilisation pour un auditeur interne généraliste

Sur la base des éléments présentés dans ce document sur la question 8, auditer un processus de sensibilisation des collaborateurs aux risques de cybersécurité consiste à évaluer l'efficacité, la couverture et l'impact de ce programme. L'audit interne peut suivre les étapes clés suivantes :

- Clarifier ce que l'audit vise à évaluer : l'efficacité, la portée, la qualité des formations, la conformité réglementaire, etc.
- Rassembler toutes les politiques, procédures, plans de formation, supports pédagogiques, rapports de formation, et tout autre document pertinent.
- Vérifier que tous les collaborateurs, y compris les nouveaux employés et les contractuels, reçoivent une formation en cybersécurité.
- S'assurer que les formations couvrent tous les aspects pertinents de la cybersécurité (phishing, gestion des mots de passe, sécurité des données, etc.).
- Examiner le contenu des formations pour s'assurer qu'il est à jour, pertinent et conforme aux meilleures pratiques et aux réglementations en vigueur.
- Vérifier que les formations sont adaptées aux différents niveaux de compétence et aux rôles des employés (stagiaires, externes, partenaires, jeunes).
- Vérifier que les supports de formation et la documentation cybersécurité sont clairs et accessibles.
- Examiner les méthodes utilisées (e-learning, sessions en personne, ateliers, simulations, etc.) pour s'assurer qu'elles sont variées et engageantes.
- S'assurer que les formations sont dispensées régulièrement et mises à jour en fonction de l'évolution des menaces et des technologies.
- Analyser les résultats des tests et des évaluations post-formation (quiz, simulations de phishing).
- Évaluer les changements de comportement des employés via des enquêtes, des observations directes du RSSI et/ou des collaborateurs IT et via l'analyse des incidents de sécurité.
- Obtenir des retours d'expérience des participants sur la pertinence et l'efficacité des formations.
- Consulter les formateurs et les responsables de la sécurité pour leur avis sur l'impact des programmes de sensibilisation.
- Analyser et challenger les KPI définis pour le programme de sensibilisation (taux de participation, taux de réussite aux tests, réduction des incidents, etc.).
- Vérifier que le programme de sensibilisation est conforme aux réglementations et aux normes de sécurité applicables (par exemple, GDPR, ISO 27001).
- S'assurer qu'il existe des mécanismes pour évaluer régulièrement l'efficacité du programme et pour apporter des améliorations en fonction des retours et des évolutions du paysage des menaces.
- Analyser la récurrence et l'impact des incidents pour comparer avec le contenu des formations afin de s'assurer de la cohérence des sujets abordés lors des sensibilisations et de la maitrise des risques.

En suivant ces étapes, un audit du processus de sensibilisation aux risques de cybersécurité permettra de garantir que les collaborateurs sont bien informés et préparés pour faire face aux menaces, et que le programme de sensibilisation est efficace et conforme aux meilleures pratiques et aux exigences réglementaires. La sensibilisation continue et la participation active

de tous les niveaux de l'entreprise sont essentielles pour maintenir une posture de sécurité efficace et améliorer la résilience globale face aux menaces numériques.

Pour aller plus loin, la norme NIST 800-50r1 (en anglais) est en cours de révision et est dédiée exclusivement à la sensibilisation des utilisateurs.

9 - Le risque cyber dans les projets informatiques, y compris cloud, low-code, IA

Par Frederic PREVAULT, Pierre-Yves ROMATIER et Sébastien ROCHE

I - Enjeux de la question

Le risque numérique (dit risque cyber) touchant à la confidentialité, intégrité, disponibilité des systèmes d'informations et des produits réalisés par les entreprises s'impose comme un des enjeux du XXIème siècle. Il doit être analysé et évalué dès le lancement de n'importe quel projet - dont notamment les sujets cloud, IA, Low / No Code. Les risques cyber doivent absolument être pris en considération dans ces projets, en dépit des effets de mode ou des pressions internes des métiers ou de l'IT pour des développements et mises en production rapides.

Contexte(s) & menace(s)

a) Cloud :

Les défis importants auxquels une organisation est confrontée lors d'une migration ou de l'utilisation du cloud, où la gestion des données est globalement confiée à un tiers, sont relatifs à la protection des données (confidentialité, intégrité et disponibilité), le contrôle des accès et des identités (administration interne et externe), la sécurité des applications (vulnérabilités exposées au réseau, protection des communications), et la conformité réglementaire (extra territorialité, RGPD, NIS2...).

De manière générale, la gestion des tiers constitue l'une des grandes menaces pour l'usage du Cloud.

b) Intelligence Artificielle :

La technologie dite d'intelligence artificielle (IA), après plusieurs dizaines d'années d'évolution, est en plein essor dans son déploiement opérationnel, notamment l'IA générative. C'est un enjeu actuel pour l'Audit Interne.

Des menaces spécifiques existent - par exemple :

- ***Attaques par infection :***
  Ces attaques consistent à contaminer un système d'IA lors de sa phase d'entraînement, en altérant les données d'entraînement ou en insérant une porte dérobée.

- ***Attaques par manipulation :***
  Ces attaques consistent à détourner le comportement du système d'IA en production au moyen de requêtes malveillantes. Elles peuvent provoquer des réponses inattendues, des actions dangereuses ou un déni de service.

(A noter : on trouver ci-contre un tableau de 10 menaces spécifiques posées par l'I.A., établi par l'OWASP, ou Open Web Application Security Project, une organisation mondiale de référence à but non lucratif dédiée à l'amélioration de la sécurité des applications web.)

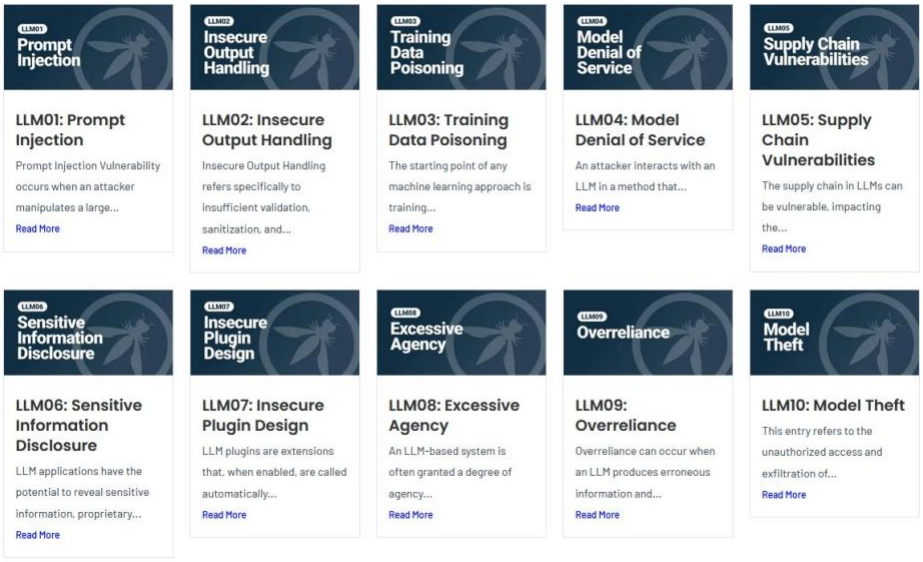


Figure 1 Top 10 des risques pour un projet IA LLM (source OWASP)

A un niveau plus fondamental, il existe un risque via l'I.A. de créer une « boîte noire » difficile à maitriser.

c) Low Code :

Le développement de solutions logicielles pour les organisations a été un axe majeur pour améliorer rapidement et efficacement leur capacité de résilience face aux nouvelles exigences du marché. Les progrès technologiques ont conduit à l'émergence de plateformes de développement d'applications dites « low-code » et « no-code » (LCNC), offrant une approche plus accessible.

À la manière d'un jeu de Lego, les LCNC se compose de briques distinctes permettant de construire une application sur-mesure répondant aux processus métiers et internes d'une organisation ou contribuant à la conduite de projets numériques.

Dans un contexte général caractérisé par l'accroissement des charges et une tendance à l'inflation du socle de dépense, liés notamment aux coûts des programmeurs qualifiés en forte hausses et l'envolée des frais d'hébergement informatiques, les LCNC ont suscité un intérêt important en raison de leur capacité à permettre aux utilisateurs non-techniques de créer des applications personnalisées et d'être une solution dite « Software as a Service » (SaaS), c'est-à-dire, un service externe de type « cloud » dont l'infrastructure informatique n'est pas la propriété de l'organisation mais hébergée et gérée par un tiers et accessible en ligne.

Poussées par la nécessité de lancer de nouveaux produits et services plus rapidement sur le marché par les équipes commerciales et marketing ou par la mise à disposition de solutions logicielles sur-mesure pour les fonctions supports, les organisations se sont orientées vers les LCNC qui connaissent une croissance explosive : Gartner prévoit que d'ici 2027, 70% des nouvelles applications d'entreprise seront construites à l'aide de ces outils, contre seulement 25% en 2020. Cette tendance devrait générer un marché de 16,5 milliards de dollars d'ici 2027, représentant plus de 16% de taux de croissance annuel composé depuis 2022.

L'une des grandes menaces liées aux LCNC, c'est le développement et l'utilisation par des personnes insuffisamment sensibilisées aux questions de cybersécurité ; ainsi, à nouveau, qu'une exposition mal maitrisée aux risques de tiers (proposant les plateformes de LCNC) ou encore une

absence de gouvernance – évidemment manifeste dans le cas d'usages de type « shadow », non déclarés à l'organisation.

(Note : une description plus large des LCNC se trouve en annexe de ce chapitre)

II - Grands principes

Grands principes communs aux trois technologies

Pour toutes ces questions, il convient que l'Audit Interne / Contrôle Interne s'assurent qu'une méthode d'évaluation des risques (autrement appelé « Security by Design ») soit connue et déclinée au sein des organisations.

- *Par ex. : La méthode EBIOS, méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques de manière structurée et formalisée.*

Recommandation #1 : S'assurer de l'application d'une méthodologie d'évaluation et traitement du risque numérique / cyber pour l'ensemble des projets y compris cloud, IA et low/no-code.

Recommandation #1b : Pour les entités publiques, utiliser le service réalisé par l'ANSSI / CNIL MonServiceSécurisé https://monservicesecurise.cyber.gouv.fr/.

Grands principes pour l'I.A. :

- Nécessité d'une gouvernance et des processus en place (Comitologie et indicateurs, activité de contrôle, cycle de vie, maîtrise des actifs …). Cette gouvernance doit autant s'attacher à la phase de développement, qu'à la phase d'exploitation/production en contrôlant également les usages.

- L'Audit Interne et le Contrôle Interne doivent s'assurer que les projets d'I.A. répondent à un objectif business clair tout en étant encadrés par une gouvernance. Celle-ci devrait s'appuyer sur des éléments de maitrises de risque (KRI), de performance (KPI) mais aussi de contrôle interne notamment vis-à-vis d'enjeux de conformité réglementaire (IA Act Juillet 2024 - https://artificialintelligenceact.eu/fr/l-acte/).

- Un comité éthique est aussi nécessaire pour éviter de reproduire les préjugés et les discriminations du monde réel, d'alimenter les divisions, de menacer les droits de l'homme et les libertés fondamentales.

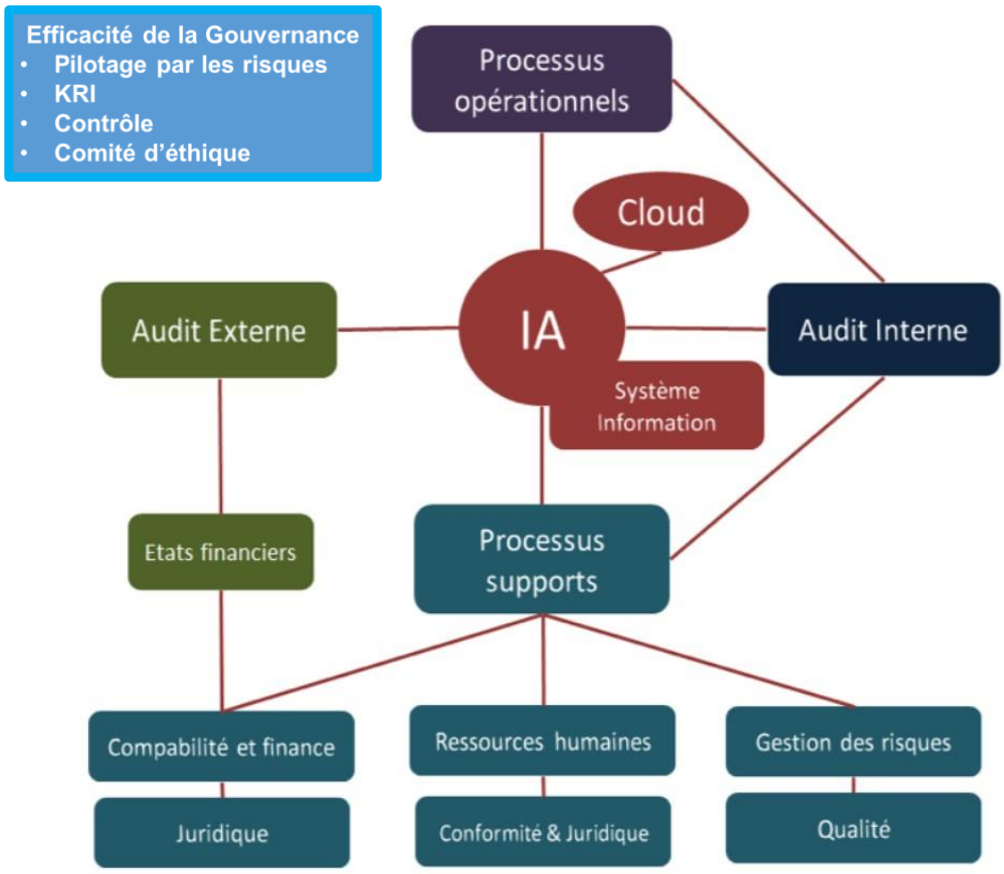


Figure 2 Source : IFACI 2018 - L'univers de l'intelligence artificielle et les défis à relever

Le cycle de vie du projet IA doit être aussi formalisé : le risque numérique / cyber doit ainsi être adressé à chacune des étapes. L'Agence de l'Union européenne pour la cybersécurité (ENISA) propose le cycle de vie suivant :

Figure 1: AI lifecycle generic reference model

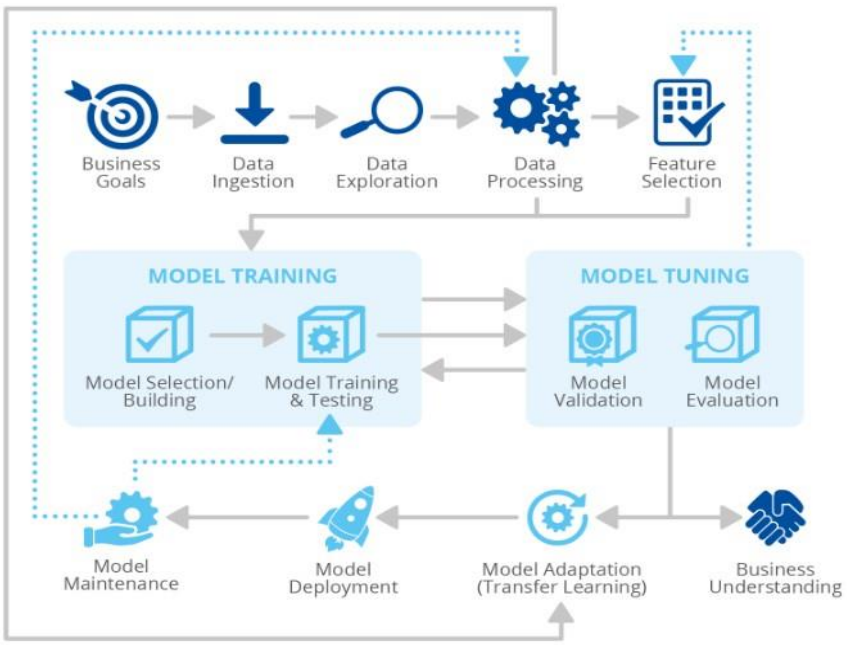


Figure 3 ENISA 2020 - CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence

Grands principes pour le Low Code / No Code :

Les projets Low-Code / No Code (LCNC) permettent à n'importe quel membre de l'organisation de développer un projet. Or, ce faisant, les menaces liées à la sécurité et à la conformité des projets LCNC sont soustraits aux équipes expertes, sans qu'il y ait clairement une partie prenante qui assume la responsabilité des pannes et des expositions financières ou réglementaires en cas des dysfonctionnements suivants :

- Accroître l'exposition de l'organisation à des incidents de sécurité et de non-conformités par manque de capacité à faire face aux cyberattaques sur les données critiques et au cyber-espionnage sur le fonctionnement des processus internes et métiers ;
- Induire des surcoûts et dissiper les ressources de l'organisation sur des projets peu contributifs, ou mal dimensionnés, voire concurrents par manque de maîtrise en raison de l'implication insuffisante des équipes expertes ;
- Perte de contrôle, dépendance vis-à-vis des fournisseurs et expositions à des sanctions juridiques et financières par manque de pilotage des contrats d'externalisation et d'une utilisation anarchique des offres « cloud » dont « SaaS ».

Malgré ce formidable levier de croissance et d'innovation que représentent les projets LCNC, le recours à ce type de solution introduit par construction une zone de menace cyber forte et indirecte par l'intermédiaire d'un fournisseur « cloud ».

Dans un contexte où les intentions, les capacités offensives et les opportunités exploitées par les attaquants et les acteurs malveillants sont en pleine expansion, le niveau de la menace cyber ne cesse d'augmenter. Face à la multitude de menaces, les atténuer est essentiel pour garantir une utilisation sûre de ces outils.

Recommandation #2 : S'assurer de l'encadrement des projets cloud, IA & Low Code/ No Code par une gouvernance et des processus adaptés (cycle de vie, contrôle interne, maitrise des actifs).

III - Bonnes pratiques

a) Cloud

Bonnes pratiques Cloud		
Définition	*Objectif(s)*	*Référentiel/ Points de contrôle/ Outils*
Évaluation des besoins et sélection du modèle de cloud *IaaS, PaaS, SaaS*	Analyse des besoins métiers et techniques, des critères de sécurité et de conformité et des objectifs de performance	NIST (National Institute of Standards and Technology) CSA (Cloud Security Alliance) ENISA (European Union Agency for Cybersecurity) ISO/IEC 2700 GDPR (General Data Protection Regulation) PCI-DSS (Payment Card Industry Data Security Standard) OWASP (Open Worldwide Application Security Project)
Évaluation de la sécurité du fournisseur du cloud	Vérification des certifications de sécurité, audit des politiques et procédures de sécurité du fournisseur, examen réglementaire	
Transparence et visibilité	Localisation des centres de données et accès aux rapports/outils de surveillance	
Support et service client	Vérification du niveau de support (24/7, SLA)	
Plan de continuité d'activité et de reprise après sinistre	Revue des plans et des résultats des tests PCA/CRA, continuité et récupération des données *(D'autant plus importants que la résilience de l'activité peut dépendre de la redondance d'actifs gérés par une tierce partie et par les conditions gouvernant le contrat d'externalisation)*	

On notera tout particulièrement le Guide de l'ANSSI « Recommandations pour l'hébergement des SI sensibles dans le cloud », publié le 9 juillet 2024, pouvant servir de référence pour le travail de l'auditeur et du contrôleur interne.

b) Intelligence Artificielle

On soulignera de manière générale :

- La nécessité de considérer pleinement comme un projet IT en tant que tel toute initiative I.A., avec donc en corollaire l'importance de prendre en compte la maitrise du cycle de vie ;
- L'importance de maitriser les actifs spécifiques aux projets I.A. (ex : données, modèles, poids du modèles…) ;
- L'importance de la gouvernance à nouveau dans la phase de développement mais également dans la phase de production / usage par les utilisateurs ;
- La nécessité sous-jacente de développer une liste de Key Risk Indicators (KRI) ;
- L'importance des dimensions éthiques (ex : biais, impacts sociaux éventuels, etc..).

Bonnes pratiques IA		
Definition	***Objectif(s)***	***Référentiel/Points de contrôle/Outils***
Analyse de risque sur les systèmes d'I.A. avant la phase d'entraînement	Existence d'une méthodologie d'analyse de risque. Assurer le critère approprié de la gouvernance de la donnée. Cartographier de manière exhaustive tous les éléments, dont les sous-parties du système d'I.A. Identifier le scénario de partage de responsabilités. Considérer la protection des données.	Méthode EBIOS-RM. Data Management Association (DAMA) "DMBOK2". Outil de gestion d'actif (Configuration management database - CMDB).
Protection de l'intégrité des données d'entraînement du modèle d'IA	S'assurer de l'intégrité des données d'entraînement du modèle tout au long du cycle d'entraînement.	Vérification systématique de la signature ou de l'empreinte (hash) des fichiers utilisés.
S'assurer du suivi des bonnes pratiques / Standard	Définir un référentiel.	[ANSSI] 35 recommandations-de sécurité pour un système d'IA générative

On notera tout particulièrement le Guide de l'ANSSI «Recommandations de sécurité pour un système d'IA générative », publié le 29 avril 2024, pouvant servir de référence pour le travail de l'auditeur et du contrôleur interne.

C) Low-Code / No-Code (LCNC)

On soulignera entre autres :

- La nécessité de considérer une application LCNC comme toute autre application, pouvant donc poser un cyber-risque à l'organisation ;
- La nécessité d'évaluer les partenaires sélectionnés dans le cadre de l'externalisation de l'activité entrainé par le développement et/ou l'exploitation de projets LCNC (on peut par exemple considérer les panels de certification) ;
- Comme dans tout projet IT, la nécessité d'appliquer les mêmes tests (ex : tests de régression, etc..).

Low/No-code		
Définition	***Objectif(s)***	***Référentiel/Points de contrôle/Outils***
Les rapports de certification *System and Organization Controls (SOC)* ***Normes internationales de (cyber)sécurité (ISO/IEC)***	Évaluer et traiter les risques informatiques et la cybersécurité liés aux services externalisés	• SOC 1 - Type 2: *ISAE3402 (international) - SSAE18 (US)* *Revue du contrôle interne informatique du prestataire* • SOC 2 - Type 2: *ISAE3000 (international) - SSAE18 (US)* *Revue de la gestion des données hébergées par le prestataire* • ISO/IEC 27001:2022 : *Management de la sécurité de l'information* • ISO/IEC 27005:2022 : *Gestion des risques cyber*
La revue de post-implémentation du projet *Post-Implementation Review (PIR)*	Examiner la maîtrise des risques liés à la mise en place d'une nouvelle solution	• Revue de la gestion de projet (*analyse de rentabilité, équipe, etc.*). • Revue des accès, de la gestion des rôles, de la politique de mots de passe et des mécanismes MFA/SSO. • Examen des cycles de migration, d'exécution des tests et de validation. • Revue de conformité (*CNIL, RGPD, traçabilité et KPIs*)
Les contrôles de configuration	Revoir la sécurité des applications Web	OWASP Low-Code/No-Code Top 10

On notera tout particulièrement les éléments produits par **OWASP Low-Code/No-Code Top 10**, pouvant servir de référence pour le travail de l'auditeur et du contrôleur interne.

IV – Points d'attention

Le Cloud computing est un domaine complexe avec des multiples concepts techniques :

- Les cadres de références peuvent être utilisés aux risques d'appliquer des standards inadaptés ou insuffisants (exemple ANSSI 2024 – Recommandations pour l'hébergement des SI sensibles dans le cloud, CCM, ISO/IEC 27017…) ;
- Les risques de conformités réglementaire ne doivent pas être sous-estimés, elles imposent des exigences strictes de la gestion des données confiées à un tier, les auditeurs ou contrôleurs doivent être formés en correspondance, une mauvaise compréhension de ces régulations peut entraîner des violations de conformité coûteuses ;
- Les risques liés à la gestion des accès et des identités (interne et externe) peuvent être sous-estimés, pouvant entrainer des violations de sécurité majeur, tels que accès non autorisés ou escalade de privilèges. Ainsi, les politiques IAM (pour « Identity and Access Management » ou Gestion des Identités et des Accès), authentification multifactorielle (MFA) et la gestion des rôles peuvent faire l'objet de recommandations et d'améliorations.

V - Conclusions

La gestion du risque cyber dans les projets informatiques, y compris cloud, IA et low/no-code est devenu un impératif. Le Contrôle Interne et l'Audit Interne doivent ainsi s'assurer que les fondamentaux sont bien en place (gouvernance, processus, pilotage par les risques par la première et deuxième ligne) tout en restant en veille sur les référentiels et outils proposés (en particulier : ANSSI, ENISA, NIST, OWASP) afin de proposer un niveau de maturité à l'organisation.

Annexe I – Intelligence Artificielle

Référentiels réglementaires

- **[UE] : IA Act Juillet 2024 -** https://artificialintelligenceact.eu/fr/l-acte/

Bonnes pratiques

- **[ANSSI / CNIL – FR] :** https://monservicesecurise.cyber.gouv.fr/
- **[ANSSI – FR]** https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative
- **[BSI – GE]** https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html#doc916902bodyText8
- **[ENISA – UE]** https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- **[NIST – USA] Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile** https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
- **[OWASP]** https://owasp.org/www-project-ai-security-and-privacy-guide/
- **[OWASP]** https://genai.owasp.org/llm-top-10/

Référentiel de contrôle

- **The IIA's Updated AI Auditing Framework** https://www.theiia.org/en/content/tools/professional/2023/the-iias-updated-ai-auditing-framework/

- **[OWASP – référentiel de contrôle]** https://genai.owasp.org/wp-content/uploads/2024/05/LLM_AI_Security_and_Governance_Checklist-v1_FR-2.pdf

Annexe II – LCNC (Low-Code / Now-Code)

Gartner a défini les LCNC comme permettant de développer et d'exécuter rapidement et de manière autonome des applications personnalisées tout en limitant et simplifiant l'utilisation des langages de programmation.
Elles ouvrent le champ des possibles :

- *Création d'un outil pour gérer les contacts clients et flux de prospection ;*
- *Semi-automatisation de la saisie, de la transmission et de la vérification des notes de frais ;*
- *Élaboration d'un tableau de bord pour la conduite de projet avec des comparatifs entre le nombre de tâches clôturées, en retard et restantes à conduire ;*
- *Mise en place d'une interface graphique accessible sur un téléphone mobile pour simplifier la déclaration des objectifs et résultats de ventes par les commerciaux.*

Ainsi les principaux cas d'usages visent à la modernisation des capacités existantes de l'organisation ou à l'augmentation de celles-ci par des initiatives d'automatisation.

Le « low-code » offre une approche visuelle et conviviale du développement, minimisant le besoin de codage traditionnel. Bien qu'un certain codage puisse toujours être nécessaire, ce dernier simplifie le procédé pour une création d'application plus aisée, en s'appuyant sur des modèles et composants prédéfinis pour reconnaître les fonctions souhaitées par l'utilisateur afin de fournir les lignes de code. Cette approche modulaire permet un prototypage rapide et des tests itératifs jusqu'à ce que les fonctionnalités espérées soient atteintes.
Le « no-code » outrepasse cela et s'affranchit de toutes contraintes techniques, permettant aux « citizen developers » - débutant absolu, voire néophyte complet, en matière informatique - de créer des programmes complets sans écrire de lignes de code à l'aide de fonctionnalités prédéfinies, de l'intelligence artificielle et d'interfaces « glisser-déposer ».

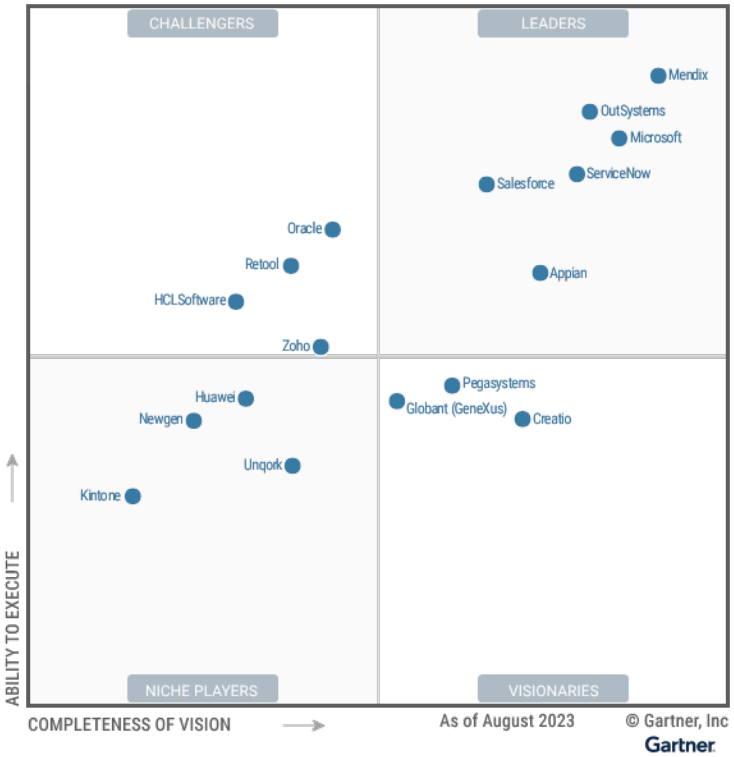


Figure 1 - Analyse de marché des éditeurs LCNC selon Gartner, 2023 – voir « Magic Quadrant for Enterprise Low-Code Application Platforms » (2023, Gartner)

Les LCNC révolutionnent le développement d'applications : l'élimination des obligations du codage traditionnel offre un terrain de jeu inespéré pour les « citizen developers », qui n'ont besoin que de très peu ou pas de connaissances en programmation pour se laisser aller aux joies de l'innovation digitale, autrefois réservées aux ingénieurs de la Silicon Valley.

La demande, la croissance et la prédominance des projets LCNC s'assimilent à une « boîte de Pandore» pour les fonctions de sécurité des systèmes d'information (SSI), d'audit et contrôle interne et de conformité et légal.

A l'image des meubles IKEA, vous économisez de l'argent en effectuant le montage vous-même, sans avoir besoin d'un artisan qualifié, et en cas de blocage, vous trouverez toujours un tutoriel sur Youtube. Cependant, les meubles nécessitent notamment un entretien régulier, un catalogue de pièces détachées en cas d'usure et des services contractualisées pour assurer les conditions d'après-vente et de garantie client.

10 - Vérifier et contrôler l'état des risques-cyber des fournisseurs clés de l'entreprise ou des entités cible d'opérations d'acquisition.

Par Bruno LECHAPTOIS, Faiza MESSAMRI, Lucile RIVERA et Valérie MERCIER

I - Enjeux de la question

L'entreprise du XXIème siècle vit dans un écosystème réseau global digitalisé et interconnecté avec des parties prenantes externes. Une attaque de cybersécurité sur un maillon de la chaine peut entrainer la perte de contrôle de l'entreprise. De ce fait, le niveau de sécurité de son système d'information dépend étroitement du niveau de sécurité des systèmes d'information de ses tiers dont les fournisseurs.

Par ailleurs, l'évolution des systèmes d'information vers des solutions nuagiques « cloud », dématérialisées et connectées conduit encore plus à englober les fournisseurs dans une vision intégrée pour se protéger des attaques de cybersécurité qui peuvent être introduites via des tiers dont les fournisseurs ou les entreprises nouvellement acquises.

A ceci s'ajoute :

- L'augmentation de la menace d'attaque par les tiers (dans le TOP10 du panorama 2023 de la menace selon l'ENISA) ;
- Le renforcement du cadre réglementaire en Europe (NIS2, DORA, entre autres) sur la sécurité des systèmes d'information afin d'améliorer la résilience des entreprises ;
- Le risque de réputation (l'atteinte à la réputation des entités victimes directes ou indirectes de cyber attaque).

II - Grands principes

- Identifier les attendus des réglementations et les acteurs externes
    - Inclut : Autorités de régulation ; normatives ; capacités d'expertise, notamment l'ANSSI, en charge de l'application de la NIS2 ; mais aussi autorités d'audit ; rôle des CACs (Commissaires Aux Comptes)…
- Identifier l'environnement interne étendu aux fournisseurs/ prestataires /cibles d'acquisition
    - Inclut : Organisation dont RSSI et gouvernance ; politiques internes ; risques internes et relatifs aux fournisseurs ; soutiens d'autres fonctions de la deuxième ligne de maîtrise ; sensibilisation / formation des collaborateurs…
- Evaluer la solidité du dispositif de contrôle interne et suivre les corrections
    - Stratégie de réponse aux incidents, PRA (Plan de Reprise d'Activité), mesure des impacts ;
    - Conduite d'audits pour apporter une assurance raisonnable sur la solidité du dispositif de contrôle Interne.

III - Bonnes pratiques

A - Intégrer le risque cyber dans la stratégie de Contrôle Interne

- S'assurer qu'un responsable (RSSI) porte la démarche (analyse des risques, compréhension de l'environnement interne et externe, programme de maîtrise, évaluation et suivi des plans de corrections) ;
- S'assurer que le RSSI est intégré dans l'analyse des cibles d'acquisition et les actions identifiées prises en compte dans l'évaluation ;
- S'assurer que la démarche est définie : les fournisseurs clefs (critiques d'un point de vue business ou d'un point de vue sécurité) identifiés, contrôlés au moins une fois par an, sur la base d'exigences définies par une contractualisation (dispositions juridiques et opérationnelles) et de fiches de sécurité permettant une revue des exigences à checker vis-à-vis d'un fournisseur ;
- S'assurer que les acteurs (en interne et chez les fournisseurs) appliquent la démarche pilotée par le RSSI et lui rendent compte (porteurs des risques, porteurs des contrôles, fonctions concernées - achats, sécurité, juridique, porteurs opérationnels) ;
- S'assurer qu'un plan de formation/ sensibilisation au risque de cybersécurité lié aux tiers est déroulé dans l'organisation et chez les fournisseurs ;
- S'assurer qu'une organisation est en place pour pouvoir réagir à un incident cyber d'un fournisseur ou d'une cible d'acquisition (maitrise d'un plan de reprise d'activité régulièrement testé, maîtrise de la communication vers les parties prenantes notamment les autorités, analyse des incidents chez le fournisseur et dans l'entreprise avec impact mesuré et mise en œuvre d'actions correctives post incidents) ;
- S'assurer que les résultats du programme de maîtrise sont partagés par le management et les autres fonctions concernées de la deuxième ligne de maîtrise et que les obligations légales sont respectées (utilisation d'un tableau de bord avec suivi d'indicateurs clefs et reportings réguliers) ;

B - Intégrer le risque cyber dans la stratégie d'audit

- Dans une approche d'une stratégie et d'un plan d'audit qui intègre le processus gestion des risques et contrôle interne (Norme IIA 9.1), il est intéressant d'intégrer dans le plan d'audit pluriannuel le risque cyber sécurité en provenance des fournisseurs/tiers clefs en coordination avec les prestataires d'assurances en risque cyber internes et externes (RSSI, experts, ANSI…) ;
- Intégrer le risque cyber dans les audits de processus liés à des fournisseurs (ex : sécurité de l'accès logique des données, Continuité des services, respect du RGPD…) ;
- S'assurer de la conformité : au niveau réglementaire (ex : NIS2), au niveau des politiques et procédures internes (ex. : PSSI, respect des clauses SSI et RGPD du contrat lié aux risques

cyber) ; au niveau des normes et référentiels (ex : ISO 27 001 …) ; au niveau de la conformité contractuelle ;

- Evaluer la pertinence de la démarche de contrôle interne fournisseurs mis en place, tel que les procédures d'identification, de contractualisation, d'évaluation et de contrôle des fournisseurs ; la définition des rôles et des responsabilités ; les contrôles mis en place ; les tableaux de bord ; le pilotage du dispositif par RSSI ; ainsi que l'application de la démarche par les acteurs… ;

- Evaluer la capacité de l'organisation à faire face à un risque cyber fournisseurs au travers de tests d'intrusion et de l'évaluation du PCA (*Plan de Continuité de l'Activité*) et de l'existence de plans de secours métiers identifiés et testés ;

- Réaliser des tests de sécurité et de sensibilisation vers les fournisseurs (Ex. : test d'intrusion physique et informatique, campagne de phishing…) pour évaluer la maîtrise du risque cyber fournisseur (dans la mesure de la possibilité règlementaire et contractuelle) ; Tests de sécurité différenciés vers les fournisseurs ou en interne ;

- Communiquer les résultats de l'audit aux parties prenantes de la démarche (RSSI, responsable des risques, fournisseurs le cas échéant), afin d'identifier les actions correctives à mettre en place et de garantir une amélioration continue ;

- S'assurer du suivi et de la mise en œuvre des plans d'action (actions correctives) liés aux fournisseurs.

IV – Points d'attention

Facteurs de risques

- **Analyse partielle et/ou non pertinente des fournisseurs clefs** : pour comprendre les criticités cyber et business, s'assurer de l'implication de l'ensemble des fonctions (business, cyber) ;

- **Pertinence/Fiabilité d'évaluation des outils du marché** : garder un avis critique sur leur pertinence, en particulier sur des outils non souverains et/ou non transparents ;

- **Favoriser le business au dépend des risques cybersécurité** par exemple contractuellement ou du fait de dépendances inter-entreprises
    - *D'où la nécessité, comme déjà rappelé plus haut, de vérifier l'existence et la pertinence de clauses d'audit dans les contrats ; et également de s'assurer si nécessaire que les arbitrages et le questionnement avec le fournisseur a bien été engagé, dans le cadre d'un risque où la 3ième ligne de défense de l'entreprise peut être engagée de manière significative.*

- **Défaut de compétence** des intervenants internes (audit et contrôle interne) en matière de cybersécurité ;

V - Conclusions

Contrôler l'état des risques cyber des fournisseurs clefs de l'entreprise ou d'entités cibles d'opérations d'acquisition nécessite outre une **organisation coordonnée** (RSSI, services achats, juridiques, responsables opérationnels, avec des relais au sein des fournisseurs, contrôle interne, audit Interne), un **cadre juridique et financier** bien défini sur les risques des fournisseurs.

Il est également nécessaire d'anticiper l'évolution des obligations légales tout comme les attaques cyber, en adaptant les plans de protection et de reprise d'activité.

Annexes

Définir la criticité d'un fournisseur pour une entreprise

Vue Métier – un fournisseur critique

- Fournisseur dont la défaillance/l'arrêt de service engendrerait un impact significatif dans l'activité de l'entreprise

Vue Sécurité – un fournisseur critique

- Fournisseur ayant accès au SI de l'entreprise
- Fournisseur hébergeant des données clefs de l'entreprise
- Fournisseur hébergeant un service clef pour l'entreprise
- Fournisseur de solutions critiques du SI de l'entreprise

Choix des outils d'évaluation et de contrôle maturité cybersécurité des tiers

Dépend de la volumétrie des fournisseurs critiques identifiés dans une entreprise
Différentes approches possibles avec différentes finalités en fonction du service fourni

- **Vérification par certifications de tiers** (exemple : ISO27001, SOC2Type2)
- **Audit sur mesure** par des sociétés de services cybersécurité spécialisées
- **Vérification par analyse questionnaire** sur mesure assujetti à preuves
  - S'inspirer de l'ANSSI - guide d'hygiène cybersécurité de l'ANSSI en 42 mesures Guide d'hygiène informatique | ANSSI (cyber.gouv.fr)
  - S'inspirer des travaux du CESIN - – questionnaire d'évaluation fournisseurs en draft CESIN
- **Utilisation de société d'évaluation maturité cybersécurité**
  - Émergence de solutions françaises: Ex. : cybervadis
- **Utilisation d 'agences de cyber-rating**:
  - /!\ à prendre avec précautions, sociétés américaines type Bitsight, Securityscorecard – sans transparence ni garantie de fiabilité des données
  - Émergence de solutions françaises: Ex. : board of cyber, scoverity

Partie III

Aller Plus Loin

Conclusion intermédiaire :

Le Guide est désormais à vous !

Guy-Philippe Goldstein

Le Guide IFACI 3.0 des risques cyber a été conçu dans un esprit d'ouverture et de pragmatisme, avec pour objectif de fournir **un point de départ solide pour les auditeurs et les contrôleurs internes**. Il ne cherche pas à être exhaustif ni à proposer des solutions définitives, car la cybersécurité est un domaine bien trop vaste et évolue à une vitesse qui rend toute tentative d'énumération complète vouée à l'obsolescence. Au contraire, ce document se veut **une première porte d'entrée, un ensemble de repères et de réflexions** à partir desquels chacun pourra approfondir, nuancer ou remettre en question les approches proposées, en fonction de sa propre expérience et des spécificités de son organisation. Les différentes technologies, du cloud à l'intelligence artificielle en passant par l'émergence de la robotique ou du calcul quantique, se transforment régulièrement, tout comme les menaces et les thèmes qu'elles soulèvent. Hier, on parlait surtout de la protection des réseaux ; aujourd'hui, les notions de résilience et de coopération sont devenues des piliers fondamentaux. **Demain, il faudra sans doute composer avec de nouveaux paradigmes, et il serait illusoire de croire que ces évolutions cesseront**. C'est pourquoi l'approche adoptée ici est résolument itérative : plutôt que de tenter d'ériger d'emblée une cathédrale, il s'agit de poser les fondations d'un village, voué à s'agrandir au fil des années.

Cet état d'esprit repose sur la conviction que la cybersécurité n'est pas un sujet exclusivement technique, mais un véritable sport collectif, mobilisant tous les métiers et l'ensemble de l'écosystème d'une organisation. **Les auditeurs et les contrôleurs internes, de par leur position transversale, ont un rôle déterminant à jouer** : ils peuvent favoriser l'adhésion à une culture de la sécurité, éclairer la direction sur les risques émergents, évaluer l'efficacité des dispositifs existants et proposer des axes d'amélioration. Les premières réponses proposées dans ce Guide ont pour vocation de servir de balises ; elles n'ont pas pour ambition de tout résoudre immédiatement. Il faut voir ces points de repère comme un moyen de structurer la réflexion et de stimuler la discussion, autant dans la sphère des auditeurs que dans celle des contrôleurs internes.

Maintenant que ce Guide est publié, **il appartient à ceux pour qui il a été conçu : vous, les professionnels sur le terrain**. Vous pourrez vous en emparer pour le critiquer, l'enrichir, l'illustrer de cas concrets ou encore le confronter à d'autres référentiels existants. **Chaque lecteur est encouragé à s'interroger sur ce qui lui paraît pertinent dans les propositions avancées** et sur les limites éventuelles qui pourraient se présenter. Certaines pistes fonctionneront sans doute très bien dans un contexte donné, tandis que d'autres demanderont des ajustements ou se révèleront inadaptées à certaines particularités. **L'invitation est donc lancée à tous ceux et celles qui souhaitent réagir**, qu'il s'agisse de formuler un désaccord constructif, de partager une expérience significative ou de poser de nouvelles questions. Toute contribution est susceptible de faire progresser la réflexion commune et de nourrir la dynamique d'amélioration continue.

Pour faciliter cette conversation, diverses modalités seront mises à disposition : on peut discuter sur les **réseaux internes de l'IFACI, s'adresser directement aux coordinateurs du Guide**, ou se réunir lors d'événements ultérieures dédiés à la cybersécurité. L'IFACI s'efforcera

au fil des mois qui viennent de prendre en compte les retours qui lui seront adressés, car c'est en croisant les points de vue et en confrontant les idées que l'on consolide une démarche d'audit et de contrôle interne à la fois robuste et en phase avec les enjeux cyber d'aujourd'hui et de demain.

En définitive, ce Guide se veut **un outil vivant, propice à la co-construction** d'un socle de connaissances et de pratiques capables d'évoluer en même temps que le paysage technologique. Par cette mise en commun des expertises et des retours d'expérience, la communauté des auditeurs et des contrôleurs internes pourra bâtir, au fil du temps, un dispositif de défense cyber toujours plus solide et adapté aux défis à venir.

Et désormais c'est à vous de jouer : le Guide vous appartient, pour autant qu'il vous donnera envie de contribuer - dans la foulée des 33 premiers auteurs que nous saluons et remercions vivement ici pour tous leurs efforts, et dont une biographie pourra être trouvée dans les pages qui suivent.

Biographie des participants

Amine Sardi
Amine, 33 ans, est auditeur interne IT chez le groupe SMABTP avec 10 ans d'expérience dans les métiers de l'audit interne. Passionné par les sujets liés à la maîtrise des risques cyber, il a été chef de mission d'audit au Crédit Agricole Assurances. Diplômé de deux masters en Audit et Contrôle de Gestion et en Direction Administrative et Financière (DAF), Amine a également suivi plusieurs formations spécialisées en systèmes d'information (SI).

Anny Siboni Zerbib
Diplômée d'expertise comptable, ancienne auditrice chez PW puis consultante en organisation, Anny Siboni-Zerbib est en charge de la maîtrise des risques et de l'audit interne au sein de la Haute Autorité de Santé. Elle est également en charge du dispositif de continuité d'activité.

Arnaud Boilot
Actuellement Risk Manager et Contrôleur Interne au sein de la Direction de la Sécurité d'Orange, Arnaud a été précédemment auditeur interne et responsable anti-fraude. Titulaire d'un DESS en Télécom, il a travaillé précédemment pour un équipementier puis dans le groupe Orange dans des fonctions commerciales et de développement.

Audric Yepndjouo
Auditeur informatique, Audric est un véritable passionné des nouvelles technologies. Après des études en management des systèmes d'information, je travaille aujourd'hui depuis plus de sept ans dans le domaine de l'audit des systèmes d'information.

Azou Chekatt
Azou est Auditeur IT et Cybersécurité depuis 2017 au sein de la Direction de l'Audit Interne du Groupe Orange après 12 années en tant qu'Ingénieur Avant-Vente puis Bid Manager en charge de la conception de solutions et d'architectures Telecom & Réseau, Sécurité et e-Santé chez Orange Business Services. Il est certifié CISSP (ISC2), PCI ISA Internal Security Assessor (PCI DSS), ISO/IEC 27001 Lead Auditor et 27005 Risk Manager.

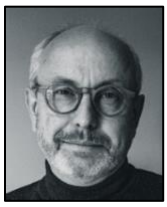
Bruno Lechaptois
Bruno est Directeur Adjoint du Contrôle Interne pour Orange. Après un parcours d'ingénieur, puis de contrôleur de gestion et de directeur financier, dans différentes sociétés en Europe, Bruno a élaboré et mis en place le programme Sarbanes-Oxley pour le groupe Orange, et poursuivi le développement du contrôle interne au-delà du domaine financier.

Carmelita De Souza
En charge du contrôle interne pour le Groupe ADP, Carmélita a précédemment occupé un poste similaire chez Prisma Media. Son parcours inclut des missions d'auditeur interne à la Caisse Nationale d'Assurance Maladie, ainsi que des missions de commissariat aux comptes. Elle est diplômée de l'ESC Pau Business School.

Charline Garnier
Charline a travaillé pendant 8 ans au sein de The Adecco Group. Elle a commencé sa carrière au poste d'assistante comptable puis a été promue Contrôleur des risques. Après une reprise d'études en formation continue, elle obtient en 2020 un master en Management et Stratégie d'Entreprise de l'ESDES à Lyon et rejoint l'équipe d'Auditeur interne France. Elle est aujourd'hui auditrice interne au sein du groupe GL events avec un périmètre international.

Faiza Messamri
Faiza est auditrice interne, chez l'assureur Nîmois spécialiste des solutions de l'immobilier SADA Assurances, après un parcours dans l'audit public comme inspectrice des finances à l'Inspection Générale des Finances algérienne.

François Michaud
Directeur de l'Audit interne du groupe Le Conservateur, groupe mutualiste indépendant d'assurance vie et de gestion patrimoniale, François a commencé sa carrière en commissariat aux comptes chez PwC. Il a également été Directeur Administratif et Financier des filiales françaises du groupe financier britannique Legal & General puis du groupe de courtage Colonna.



Frédéric Prevault
Diplômé de l'Université Louis Pasteur de Strasbourg, Frédéric est actuellement Directeur de l'audit Interne IT de Forvia (Faurecia et Hella) depuis 5 ans. Parmi ses expériences, on peut compter: la gouvernance et la direction qualité informatique au niveau du Groupe (certifié IATF), chef de projets, du pilotage industriel et la direction de sites.

Frédéric Vilanova
Frédéric est un expert en management des risques et en gouvernance de la cybersécurité. RSSI en banque, il a fondé Effective Yellow, qui accompagne les dirigeants dans leur montée en maturité cybersécurité, ISO27001 ou NIS2. Il a été manager et directeur chez EY, PWC, Capgemini, en CAF et à Monaco.

Gilles Brunet
Collaborateur au sein de la Direction de l'Audit du Groupe Orange, Gilles a exercé différentes fonctions d'auditeurs IT - Directeurs de missions sécurité et IT puis Directeur en charge du Programme, Processus et Méthodes de l'Audit Interne. Animateur de l'Antenne Ifaci Auvergne-Rhône-Alpes et Réserviste Civique, Gilles est chargé de prévention au sein du Réseau des Experts Cybermenances en région Auvergne-Rhône-Alpes rattaché à la Police Nationale/Police Judiciaire.

Guillaume Malespine
Guillaume est directeur de l'audit, du contrôle interne, et des risques de l'UGAP, principale centrale d'achat public en France. Il a également en charge la compliance et la déontologie, et est médiateur interne.

Isabelle Pinilla
Diplômée de l'IAE de Paris-Sorbonne, Isabelle a occupé différents postes au sein de l'audit interne du Ministère des Armées avant de rejoindre la direction des affaires financières du Ministère des Armées en tant que cheffe de bureau adjointe au sein du bureau de la qualité comptable.

José René Coffi Vigan
José René Coffi est Auditeur interne pour la BCEAO, la Banque Centrale des États de l'Afrique de l'Ouest. Fort d'une riche expérience au sein de la Direction des Systèmes d'Information, au titre de la gestion opérationnelle des infrastructures technologiques, de la sécurité des données et de la transformation numérique, il met désormais en pratique son expertise d'auditeur certifié des systèmes d'information (CISA) dans le cadre de la gestion des risques et de la conformité.

Lotfi Ladouari
Lotfi est Auditeur Informatique Groupe chez Fnac Darty. Auparavant, Lotfi a été responsable gestion des risques IT chez KPMG. Il a également travaillé en contrôle de gestion chez Air France-KLM Cargo et Amundi Asset Management, développant une expertise dans le domaine de l'asset management.

Lucile Rivera
Lucile est directrice adjointe de l'Inspection générale du Conseil départemental de Seine-Saint-Denis depuis septembre 2019. Elle supervise l'audit interne, élabore et suit les plans d'audit, consolide la gestion des risques et le contrôle interne. Biostatisticienne de formation, elle débute dans l'industrie pharmaceutique puis intègre la fonction publique territoriale en 1997. Après plusieurs postes stratégiques (protection maternelle, autonomie), elle a pu s'occuper des questions d'audit interne, conduite de projets et transformation numérique, en s'intéressant particulièrement aux cyber-risques du secteur public.

Marie-Line Poitout
Marie-Line est Directrice Audit et Contrôle du Groupe Clariane, première communauté européenne du soin, de la santé et de l'hospitalité au service des personnes fragiles. Clariane est une entreprise à mission côtée.
Auparavant, Marie-Line a été pendant 13 ans au sein du Groupe Primonial, Directrice en charge de l'audit, du contrôle permanent, de la conformité et des risques. Après un début de carrière dans un cabinet d'audit, elle a été Responsable Conformation des Services d'Investissement (RCSI) de W Finance, filiale d'Allianz.

Marjolaine Alquier
Marjolaine est Directrice Audit & Contrôle Interne pour Covivio. Elle y dirige les fonctions d'audit interne, de contrôle interne, de la conformité et de gestion du risque pour le Groupe. Diplômée de l'Université Panthéon Assas (Paris II), Marjolaine a auparavant exercé diverses fonctions au sein de directions financières durant sa carrière.

Mohamed Yassine Zagouri
Diplômé de Skema Business School et de l'ESP-EAP, Yassine est Auditeur Expert Informatique et Product Manager au sein de l'Inspection Générale d'Audit de la banque publique Bpifrance. Il est également formateur sur des thématiques telles que la méthodologie d'audit interne, les risques cyber et les systèmes d'information.

Olivier Meyer
Olivier, directeur de l'audit interne IT chez The Adecco Group, supervise les audits en IT, cybersécurité et digital du groupe. Fort de plus de 18 ans d'expérience, dont 13 chez KPMG, il est expert en gouvernance IT et passionné par les nouvelles technologies. Olivier est membre du groupement professionnel des systèmes d'information de l'IFACI.

Olivier Sznitkies
Président fondateur d'Audiligence, société de conseil et formation spécialisée en audit et contrôle interne, prévention de la fraude et cybersécurité, Olivier a été directeur de l'audit interne EMEA du groupe LafargeHolcim après 15 ans d'expérience comme auditeur SI chez KPMG. Ingénieur informatique, titulaire des CISA, CISM et CFE et auditeur de l'IHEDN, Olivier a contribuéà la rédaction de plusieurs publications dont le Guide d'Audit de la Gouvernance des SI.

Pierre-Luc Refalo
Pierre-Luc est vice-président au sein de la Direction de l'Audit Interne du Groupe Capgemini, en charge des domaines IT, Cybersécurité et Protection des données.
Il est conférencier international et auteur de 3 ouvrages de référence dont "La sécurité numérique de l'entreprise », primé au FIC 2013.

Pierre-Yves Romatier
Pierre-Yves est Senior IT Auditor chez Kering depuis 2023, soutenant la stratégie "Empowering Imagination" via des missions d'audit des systèmes d'information et de la cybersécurité à l'international. Formé lors d'un Master SIEE (Audit et Conseil) à Paris-Dauphine en alternance chez EY, il a par la suite acquis cinq années d'expérience en audit IT dans le service Technology Risk d'EY Consulting.

Prince Nyany Ilunga
Diplômé en informatique de gestion, Prince à débuter sa carrière professionnelle dans les entreprises de télécommunications (Microcom puis Cybernet) en tant qu'Ingénieur réseau et télécom. Depuis 2011, il est Auditeur Interne à la Banque Centrale avec un focus sur l'audit du SI.

Quentin Chopard
Diplômé de l'université de Technologie de Troyes et de l'Université Panthéon Sorbonne, Quentin est chargé d'études risques au sein du Groupe Aéroports de Paris après des expériences au sein d'un cabinet d'audit et du Groupe Michelin.

Sébastien Roche
Sébastien est auditeur interne au sein du Groupe Orange depuis 8 ans. Certifié par le SANS et reconnu comme un Orange Expert Senior sécurité , il assure également des missions d'éclairage stratégique sur les enjeux cyber actuels et ceux de demain.

Thierry Thomas
Thierry est chargé de missions d'audits interne et d'inspection générale » au sein de OFB (Office Français de la Biodiversité). Avec une solide expérience de DOSI/CIO dans la conduite de projets internationaux, son parcours se distingue par une diversité d'expériences dans les secteurs public et privé, et par une expertise à la fois en stratégie/management, en organisation, en conduite du changement et en transformation digitale, audit interne en environnement multiculturels.

Valérie Mercier
Valérie est responsable Gouvernance et Support au sein de la Direction Sécurité du Groupe Orange. Elle pilote notamment la gouvernance sécurité des fournisseurs ainsi que le support sécurité sur les opportunités de fusion et acquisition du groupe. Diplômée de l'EPF, Sciences Po et certifiée ISO/IEC 27001 Lead Auditor, Valérie a +20ans d'expérience dans les domaines IT, Achat et management à l'international.

Vincent Maret
Vincent est associé KPMG en charge des activités de conseil en Cybersécurité, Protection des données personnelles et IA de confiance. Il accompagne depuis plus de 25 ans les entreprises dans la maitrise des risques liés à la cybersécurité et aux données personnelles. Avant KPMG, il a travaillé pour EY, PWC et CGI. Il a réalisé et supervisé de centaines de missions relatives à la cybersécurité, tant dans le domaine de la gouvernance que sur des sujets opérationnels et technologiques, pour le compte de Directeurs Cybersécurité, de DSI, de directions d'audits internes et d'inspections générales, de directions des risques, de directions générales et de responsables métiers, ainsi que dans des contextes de M&A. Il est également l'auteur du livre « Blockchains, intelligences artificielles, objets connectés, ordinateurs quantiques - Quels risques technologiques ? »

Xavier Guiffard Xavier est le directeur de l'audit interne, des risques et du contrôle interne du Groupe Canal+.
Il a débuté sa carrière dans le conseil puis a développé son expérience à l'international dans le secteur des télécommunications et de l'audiovisuel avant de rejoindre l'audit interne de Vivendi en 2017 puis de Canal+ en 2025.
Il est diplômé de l'EDHEC, auditeur de la 3ème session nationale Cybersécurité et Souveraineté Numérique de l'IHEDN et réserviste citoyen au sein du corps des officiers de la gendarmerie nationale.

Xavier-Alexandre Treu
Diplômé de l'EM Strasbourg, après avoir exercé différentes fonctions en commissariat aux comptes chez Deloitte Luxembourg, puis en Risk management au sein du Crédit Agricole, Xavier-Alexandre est désormais Directeur de l'Audit Interne de la banque Barclays après avoir été Directeur de l'Audit Interne du Groupe ODDO BHF en France. Il est également CIA et CISA.

Ressources et Bibliographie

Documents ANSSI :

- Guide d'hygiène informatique de l'ANSSI (en 42 mesures) - cyber.gouv.fr
- Méthode EBIOS RISK MANAGER - https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/
- Liste des produits et services qualifiés (ANSSI) : https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
- "Crise d'Origine Cyber – Les clés d'une gestion opérationnelle et stratégique" - https://cyber.gouv.fr/sites/default/files/2021/12/anssi-guide-gestion_crise_cyber.pdf
- "Recommandations pour l'hébergement des SI sensibles dans le cloud" (juillet 2024)
- "Recommandations de sécurité pour un système d'IA générative" (avril 2024)
- Service MonServiceSécurisé - https://monservicesecurise.cyber.gouv.fr/
- Guide pour l'elaboration d'une politique de sécurite de systeme d'information, Section 3: Principes de securité, Direction centrale de la securite des systemes d' information, Mars 2004, disponible à https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-section3-principes-2004-03-03.pdf

Documents UE :

- AI Act (juillet 2024) - https://artificialintelligenceact.eu/fr/l-acte/
- ENISA "CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence" (2020)

Documents IIA/IFACI :

- Guide IFACI 2.0 des Cyber-Risques (2020 - https://www.ifaci.com/wp-content/uploads/2024/01/Guide-des-risques-cyber-Ifaci-2.0-2020.pdf)
- Guide IFACI 1.0 des Cyber-Risques (2017) - https://docs.ifaci.com/wp-content/uploads/2018/06/Cyber-risques.pdf
- "L'univers de l'intelligence artificielle et les défis à relever" (IFACI 2018)
- "The IIA's Updated AI Auditing Framework" - https://www.theiia.org/en/content/tools/professional/2023/the-iias-updated-ai-auditing-framework/

Documents AMRAE

- Maitrise du risque numérique: l'atout confiance, novembre 2019 https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

Normes et standards :

- ISO/IEC 27000 (suite)
- NIST Cybersecurity Framework (CSF) 2.0
- COBIT
- GTAG (Global Technology Audit Guide) de l'IIA
- CIS Critical Security Controls (v8.1)
- ITIL
- ISO/IEC 27001:2022
- ISO/IEC 27005:2022
- PCI-DSS
- ISAE3402/SSAE18
- ISAE3000
- NIST 800-50r1

Autres références :

- OWASP (Open Web Application Security Project) : https://owasp.org/
  En particulier :
  - Liste OWASP Low-Code/No-Code Top 10
  - Liste OWASP du Top 10 des risques IA – sur Machine Learning : https://owasp.org/www-project-machine-learning-security-top-10/ ; sur Generative AI : https://genai.owasp.org/
  - Liste OWASP des contrôles LLM AI Cybersécurité et gouvernance (voir : https://owasp.org/www-project-top-10-for-large-language-model-applications/llm-top-10-governance-doc/LLM_AI_Security_and_Governance_Checklist-v1_FR.pdf)
- Gartner "Magic Quadrant for Enterprise Low-Code Application Platforms" (2023)
- Cloud Security Alliance (CSA)
- Data Management Association (DAMA) "DMBOK2"
- BSI (Allemagne) sur l'Intelligence Artificielle - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html