CRIPP

Cadre de Référence International des Pratiques Professionnelles de l'audit interne

Lignes directrices complémentaires

GTAG®

Global Technology Audit Guide

Évaluer le risque de cybersécurité

Les rôles des trois lignes de maîtrise

The Institute of Internal Auditors | Global

Table des matières

Synthèse ... 3
Introduction et enjeux métier ... 4
Principaux risques et menaces liés à la cybersécurité ... 5
Les trois lignes de maîtrise : Rôles et responsabilités ... 6
Responsables et activités clés de la première ligne de maîtrise ... 6
Contrôles usuels des cybermenaces ... 8
Les responsables et les activités clés de la deuxième ligne de maîtrise ... 9
Écueils au niveau de la première ligne et de la deuxième ligne de maîtrise ... 11
Le rôle de l'audit interne en tant que troisième ligne de maîtrise ... 11
Périmètre de l'audit interne et coordination ... 15
Une démarche d'évaluation des risques et des contrôles de cybersécurité ... 17
Référentiel d'évaluation des risques de cybersécurité ... 17
Composante 1 : Gouvernance de la cybersécurité ... 18
Composante 2 : Inventaire des actifs informationnels ... 18
Composante 3 : Configurations de sécurité usuelles ... 19
Composante 4 : Gestion des accès ... 20
Composante 5 : Réponse et remédiation rapides ... 20
Composante 6 : Surveillance permanente ... 20
Rôle du responsable de l'audit interne dans la communication au Conseil et aux autres organes dirigeants de l'assurance relative à la cybersécurité ... 23
Annexe A - Principales normes IIA concernées ... 25
Annexe B - Lignes directrices de l'IIA en la matière ... 26
Annexe C - Définition des concepts clés ... 27
Annexe D - Considérations de l'audit interne en matière de risques de cybersécurité ... 28
Auteurs / Contributeurs ... 32

Synthèse

Ordinateurs, réseaux, programmes, applications, médias sociaux, données... Autant d'outils dont les organisations, quelles qu'elles soient, dépendent de plus en plus et qui accroissent leur vulnérabilité aux cybermenaces. Les failles de sécurité peuvent avoir des conséquences préjudiciables sur les organisations et leurs clients, tant en termes financiers que de réputation. La connexion et l'accès aux informations par des utilisateurs externes à l'organisation accentuent les risques bien au-delà de ce qui est traditionnellement pris en charge par les contrôles généraux informatiques et les contrôles applicatifs. La dépendance des organisations aux systèmes d'information et le développement des nouvelles technologies rendent insuffisantes les approches d'évaluation traditionnelles des contrôles généraux informatiques et applicatifs pour pouvoir fournir une assurance en matière de cybersécurité.

Le concept de cybersécurité regroupe les technologies, les processus et les pratiques qui visent à protéger d'un actif non autorisé les actifs informationnels d'une organisation : ordinateurs, réseaux, programmes et données. Les cyberattaques devenant plus fréquentes et plus graves, il est nécessaire d'améliorer la gestion des risques en matière de cybersécurité.

L'audit interne joue un rôle crucial lorsqu'il évalue les risques de cybersécurité d'une organisation. Pour ce faire, il prend en compte les éléments suivants :

- Qui a accès aux informations les plus précieuses de l'organisation ?
- Quels actifs constituent les cibles les plus probables d'une cyberattaque ?
- Quels systèmes causeraient le plus de perturbations s'ils étaient compromis ou rendus inopérants ?
- Quelles sont les données qui si elles tombaient entre les mains de tiers non autorisés, pourraient causer à l'organisation des dommages financiers, en termes de compétitivité, d'ordre juridiques ou de réputation?
- Le management est-il préparé à réagir en temps opportun en cas d'incident de cybersécurité ?

Ce guide pratique expose les rôles de l'audit interne en matière de cybersécurité, notamment :

- Le rôle du responsable de l'audit interne au regard des activités d'assurance, de la gouvernance, de la gestion des risques et des cybermenaces.
- L'évaluation des risques inhérents et des menaces dans ces domaines.
- Les rôles et les responsabilités de la première, de la deuxième et de la troisième de maîtrise au regard de la gestion des risques, des contrôles et de la gouvernance.
- En cas de lacunes dans les activités d'assurance.
- Les responsabilités en matière de communication et de *reporting* de l'audit interne.

Par ailleurs, ce guide étudie les menaces courantes et les risques émergents auxquels sont confrontées les trois lignes de maîtrise. Il propose également une démarche simple d'évaluation des risques et des contrôles de cybersécurité.

Introduction et enjeux métier

Les auditeurs internes ont besoin d'adopter une nouvelle approche pour fournir une assurance quant aux risques de cybersécurité. Bien qu'utiles, les contrôles généraux informatiques se révèlent insuffisants pour fournir une assurance dans le domaine de la cybersécurité car ils ne sont ni complets ni réalisés en temps opportun. Les objectifs fondamentaux de l'audit tels que l'exhaustivité, l'exactitude et l'autorisation sont toujours pertinents. Toutefois, de nombreux facteurs émergents incitent à adopter une nouvelle approche de l'audit interne qui fournisse des conclusions pertinentes sur les assertions relatives à la cybersécurité.

La multiplication des technologies a permis à un nombre croissant d'utilisateurs d'avoir accès aux données des organisations. A travers la chaîne logistique, les parties prenantes telles que les clients et les prestataires ont de plus en plus accès aux données de l'organisation. Une plus grande variété de données est désormais disponible immédiatement, puisque les organisations tendent à stocker de gros volumes d'informations sensibles et confidentielles dans des infrastructures virtuelles telles que le *cloud computing* (informatique dans les nuages).

Autre facteur ayant un impact sur l'approche de l'audit interne : le nombre grandissant d'appareils pouvant être connectés et impliqués en permanence dans l'échange de données (c'est « l'Internet des objets »). À mesure que les organisations se globalisent et que le réseau de collaborateurs, de clients et de prestataires s'étoffe, les exigences d'accès permanent aux données de l'organisation se font plus pressantes. Les jeunes générations sont des *« digital natives »*[1] (enfants du numérique) et s'attendent à disposer d'un accès en temps réel aux données, quel que soit l'endroit où ils se trouvent.

Les menaces non anticipées sur la sécurité peuvent provenir de relations internationales hostiles, de pirates informatiques organisés, d'initiés et de services ou de logiciels de mauvaise qualité. La complexité des dispositifs de cybersécurité est susceptible d'évoluer puisque les missions et les exigences réglementaires relatives à la communication d'incidents ou de failles de cybersécurité continuent à se développer. L'importance de détecter et de communiquer un risque dans un délai imparti l'emporte sur la valeur préventive des contrôles généraux informatiques traditionnels effectués de manière régulière.

Face à ces risques émergents, il est attendu des responsables de l'audit interne qu'ils s'assurent de la mise en œuvre par le management des contrôles préventifs et détectifs. Ils doivent également élaborer une démarche d'audit claire pour évaluer les risques de cybersécurité et les capacités de réaction du management, en se concentrant notamment sur la diminution du temps de réponse. Le responsable de l'audit interne doit s'appuyer sur l'expertise de la première et de la deuxième lignes de maîtrise pour rester au fait des risques de cybersécurité.

[1] Le terme *« digital natives »* apparait en 2001, dans l'article *« Digital Natives, Digital Immigrants »* de Marc Prensky, auteur et conseiller d'éducation. Il fait référence à la génération qui a grandi baignée dans le langage numérique des ordinateurs, des jeux vidéo, des médias sociaux, etc.

Principaux risques et menaces liés à la cybersécurité

La cybersécurité doit concerner les systèmes qui conribuent à l'atteinte des objectifs d'une organisation en termes d'efficacité et d'efficience de ses opérations, de fiabilité des *reportings* internes et externes, et de conformité à la législation et aux règlements applicables. En général, une organisation conçoit et met en place des contrôles de cybersécurité à tous les niveaux de l'organisation pour protéger l'intégrité, la confidentialité et la disponibilité des données.

Les cyberattaques sont perpétrées pour différentes raisons : la fraude financière, le vol ou le détournement de données, les opérations fomentées par des activistes, les tentatives de rendre les systèmes d'information inopérants, de désorganiser les infrastructures critiques et les services vitaux d'un gouvernement ou d'une organisation (liste non exhaustive). Cinq sources classiques de cybermenaces sont présentées dans l'Encadré 1.

Encadré 1 :
Cinq sources classiques de cybermenaces

- États-nations
- Cybercriminels
- Hacktivistes
- Initiés et prestataires de services
- Développeurs de produits et de services de mauvaise qualité

Pour bien comprendre les cybermenaces auxquelles est confrontée une organisation, il convient de déterminer quelles données peuvent avoir de la valeur pour des tiers ou engendrer d'importantes perturbations si elles disparaissent ou sont corrompues. Il est tout aussi important d'identifier le type d'informations susceptibles de causer des pertes financières ou de compétitivité, et d'atteinte à la réputation de l'organisation si elles tombaient entre les mains de tiers ou si elles étaient rendues publiques. Par exemple, les informations relatives aux clients et aux collaborateurs, la propriété intellectuelle, la chaîne logistique, la qualité et la sécurité des produits, les clauses et les tarifs contractuels, la planification stratégique, et les données financières.

Le secteur d'activité dans lequel évolue l'organisation est primordiale pour identifier les cybermenaces. Par exemple, les commerçants s'efforceront de protéger les données de leurs clients ainsi que le bon fonctionnement de leurs services clients. Les organisations centrées sur la recherche et le développement seront plus sensibles à la protection de la propriété intellectuelle. Les industriels s'attacheront à la fiabilité et à l'efficacité des systèmes de production et de la chaîne logistique ainsi qu'à la qualité et à la sécurité des produits. Les cabinets de prestations de services seront davantage concernés par les informations commerciales sensibles des contrats et des modèles de coûts financiers.

Les trois lignes de maîtrise : Rôles et responsabilités

Les bonnes pratiques visant à améliorer l'efficacité et l'efficience des fonctions de contrôle et de gestion des risques sont présentées dans la prise de position de l'IIA « Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces », publiée en janvier 2013. L'une des étapes essentielles de l'évaluation du rôle de l'audit interne dans la cybersécurité consiste à s'assurer que les trois lignes de maîtrise sont bien distinguées et fonctionnent efficacement. De plus, un dispositif de remontée d'informations doit être mis en place pour définir les rôles et les responsabilités de chacun dans l'identification et la remontée des risques dépassant l'appétence pour le risque de l'organisation.

En tant que première ligne de maîtrise, le management détient et gère les données, les processus, les risques et les contrôles. Pour la cybersécurité, cette fonction est souvent attribuée aux administrateurs système et autres, chargés de préserver les actifs de l'organisation. Les activités usuelles de la première ligne de maîtrise sont présentées dans l'Encadré 2 page 7.

La deuxième ligne de maîtrise est constituée des fonctions de supervision du risque, de contrôle et de conformité, chargées de s'assurer que les processus et les contrôles de la première ligne de maîtrise existent et fonctionnent efficacement. Ces fonctions peuvent comprendre des groupes dont la responsabilité est de s'assurer de la gestion efficace des risques et de surveiller les risques et les menaces en matière de cybersécurité. Les fonctions classiques de la deuxième ligne de maîtrise sont répertoriées dans l'Encadré 3 page 9.

En tant que troisième ligne de maîtrise, l'audit interne fournit, à la direction générale et au Conseil, une assurance objective sur les processus de gouvernance, de gestion des risques et de contrôle. Il s'agit d'évaluer l'efficacité générale des activités réalisées par la première ligne et la deuxième ligne de maîtrise, en matière de gestion des risques et d'atténuation des menaces de cybersécurité. Les activités classiques de la troisième ligne de maîtrise sont présentées dans l'Encadré 4, page 12.

Responsables et activités clés de la première ligne de maîtrise

La première ligne de maîtrise est composée des managers opérationnels qui sont propriétaires de la gestion des risques, des contrôles et qui les gèrent. Elle met en place les actions correctives visant à pallier les défaillances au niveau des processus et des contrôles. Les organisations peuvent établir plusieurs fonctions en lien avec la cybersécurité.

Un responsable des infrastructures informatiques *(chief technology officer, CTO)* apportera les connaissances et les orientations concernant les technologies disponibles pour piloter la mission de l'organisation ; il est souvent chargé de protéger la propriété intellectuelle de l'organisation. Une autre de ses responsabilités peut consister à s'assurer que l'organisation est préparée à aborder les prochaines phases de développement technologique, synonymes d'avantage concurrentiel, d'évolution stratégique et d'innovation.

L'organisation peut également faire appel à un responsable de la sécurité *(chief security officer, CSO)*, à un responsable de la sécurité des systèmes d'information *(chief information security officer, CISO)* ou à toute autre personne chargée de la sécurité informatique. Ces fonctions essentielles pour l'identification et la compréhension des cybermenaces, conçoivent et déploient la stratégie de cybersécurité et veillent à l'application des politiques et des procédures de sécurité. Ils prennent souvent l'initiative de développer des programmes de surveillance pour s'assurer que les actifs et les parties prenantes de l'organisation sont correctement protégés.

Un directeur des systèmes d'information *(chief information officer, CIO)* peut être recruté avec pour responsabilité le développement d'un avantage compétitif et le pilotage du changement stratégique dans l'ensemble de l'organisation. Il peut également prendre en charge le développement du programme de cybersécurité des données, la mise en œuvre du programme de formation à la cybersécurité à l'échelle de l'entité et l'élaboration des politiques de cybersécurité.

Aux côtés du directeur général et des membres de la direction générale, ces fonctions (CTO, CSO, CISO et CIO) luttent contre les cybercrimes et les cyberattaques. Si, au sein de l'organisation, certaines entités doivent assumer la responsabilité de leur propre technologie, elles sont tenues de concevoir et de mettre en place les contrôles adéquats pour sécuriser ces technologies et ces données, en coordination avec d'autres activités d'évaluation du risque.

Quand l'organisation n'a pas une taille suffisante pour supporter les fonctions décrites précédemment, une démarche habituelle consiste à réunir un comité de managers SI et opérationnels qui sont concernés par la réponse à apporter aux risques de cybersécurité. Les responsabilités précitées peuvent être partagées entre une ou plusieurs personnes de la première ligne de maitrise disposant de l'autorité adéquate pour répondre aux risques correspondants.

Encadré 2 : Activités usuelles à la première ligne de maîtrise

- Gérer les procédures, les formations et les tests relatifs à la sécurité
- Maintenir les configurations de sécurité des appareils, les mises à jour des logiciels et les correctifs de sécurité.
- Déployer des systèmes de détection d'intrusion et réaliser des tests d'intrusion.
- Configurer le réseau de façon sécurisée pour gérer et protéger le trafic.
- Répertorier les actifs informationnels, les appareils technologiques et les logiciels correspondants.
- Mettre en œuvre des programmes de protection des données et de prévention des pertes ainsi qu'une surveillance adaptée.
- Restreindre les accès par privilège minimal.
- Chiffrer les données chaque fois que possible.
- Mettre en place une gestion des vulnérabilités avec des surveillances internes et externes.
- Recruter et fidéliser des collaborateurs diplômés en SI, en risques SI et en sécurité de l'information.

Contrôles usuels des cybermenaces

Puisque les cybermenaces ont pour but de mettre à mal les systèmes ou de capter des données, les menaces portent souvent sur les lieux de stockage des données sensibles : centres de données, réseaux internes, environnements hébergés en externe et même des plateformes de continuité d'activité. Peu importe où se déroule l'attaque, le résultat final peut entrainer des violations des lois et règlements, des pénalités, des préjudices de réputation et des pertes de revenus.

Les données sensibles ou confidentielles peuvent être classifiées et stockées en interne, en externe, ou les deux à la fois. Pour le stockage en interne, de nombreuses organisations s'en remettent à la technologie : configurations sécurisées, pare-feu et contrôles d'accès comme leur première ligne de maîtrise. Cependant, lors d'une attaque ciblée, quand le pare-feu est surchargé, les assaillants peuvent parvenir à s'introduire et à réaliser des transactions non autorisées.

Pour limiter le risque qu'une attaque de ce genre n'atteigne le pare-feu, la première ligne de maîtrise met en place des actions préventives autour du réseau. C'est un processus délicat qui implique de restreindre les accès et de bloquer le trafic non autorisé. Des mesures de contrôle de détection, telles que la surveillance, doivent aussi être mises en place pour rechercher des vulnérabilités connues, basées sur la connaissance approfondie des produits logiciels, des organisations et des sites web malveillants.

Beaucoup d'organisations dressent une liste blanche du trafic accepté et une liste noire du trafic bloqué. Cependant, une surveillance active et des mises à jour fréquentes sont indispensables en raison de la nature dynamique du trafic sur le réseau. Si l'assaillant parvient à accéder au système, il risque fort, lors de l'attaque suivante, d'obtenir les privilèges administrateurs qui lui permettront d'effacer ses traces.

Quand les données sont stockées en dehors de l'organisation, il est vital pour cette dernière de s'assurer que les prestataires gèrent correctement les risques associés. Une première étape déterminante pour la première ligne de maîtrise consiste à rédiger des contrats robustes qui prévoient : des rapports sur le contrôle des services de l'organisation *(service organization control, SOC),* des clauses d'audit, des accords sur les niveaux de services *(service level agreements, SLA),* et/ou des engagements d'évaluation de la cybersécurité. De plus, les attentes en matière de *reporting* devraient être explicitées pour décrire les niveaux de protection relatifs à la sécurité de l'information.

Après l'évaluation préalable et une fois le contrat négocié et initié, le management doit avoir la possibilité de superviser et de piloter le prestataire en surveillant et en communicant les indicateurs clés pour s'assurer de la conformité avec les niveaux de services (SLA). Si le prestataire ne satisfait pas aux exigences contractuelles, le management peut invoquer la clause d'audit, demander à recevoir une réponse à ses questions en temps opportun, appliquer des pénalités et envisager de faire appel à un autre prestataire si nécessaire.

Le management doit également être attentif aux projets d'attaque basés sur les techniques d'ingénierie sociale, y compris l'hameçonnage *(phishing)* et les appels téléphoniques malveillants. En se faisant passer pour une organisation ou une personne légitime à la recherche d'informations, les assaillants convainquent les individus autorisés à partager des données sensibles, à fournir les accès de leur système, à cliquer sur des liens qui conduisent à des sites web frauduleux ou à réaliser des actions qui installent des logiciels malveillants *(malware)* sur l'ordinateur de la personne. Ces logiciels malveillants sont de plus en plus sophistiqués et ciblent avec toujours plus de précision un objet ou un réseau spécifique. Une fois le *malware* installé, il se réplique à travers tout le réseau de l'organisation, perturbe les performances et la disponibilité des systèmes, dérobe des données et contribue à l'activité frauduleuse des assaillants.

Les logiciels malveillants profitent du manque de vigilance des utilisateurs. Par conséquent rappeler fréquemment à chacun d'être attentif à tout e-mail douteux ou anormal, aux demandes, activités du système ou appels téléphoniques inhabituels est important. Les formations peuvent également aider les collaborateurs à repérer les fausses communications et à rapporter rapidement ce type d'événement pour effectuer des recherches, faire remonter l'information et résoudre l'incident. Les leçons tirées de l'expérience des pairs du secteur constituent de bonnes bases pour les formations, la prise de conscience et l'adoption de mesures préventives supplémentaires.

Les responsables et les activités clés de la deuxième ligne de maîtrise

La deuxième ligne de maîtrise, composée entre autres de la gestion des risques SI et des fonctions de conformité SI, joue un rôle clé dans la conception du programme et des dispositifs de sécurité d'une organisation.

La deuxième ligne de maîtrise

- évalue les risques et les expositions en matière de cybersécurité puis détermine s'ils sont alignés avec l'appétence pour le risque de l'organisation ;
- surveille les risques actuels et émergents ainsi que les évolutions des lois et des règlements ;
- collabore avec les fonctions de la première ligne pour garantir une conception appropriée du contrôle.

Les risques de cybersécurité sont considérablement plus dynamiques que les risques traditionnels et nécessitent une réponse en temps opportun. Comme l'exposition aux

Encadré 3 : Activités usuelles à la deuxième ligne de maîtrise

- Conception des politiques, formations et tests relatifs à la cybersécurité.
- Évaluation des cyberisques.
- Collecte des informations sur les cybermenaces.
- Classification des données et conception d'accès par privilège minimal.
- Surveillance des incidents, des indicateurs clés de risques et mise en place des correctifs nécessaires.
- Recrutement et fidélisation de collaborateurs certifiés en gestion des risques SI.
- Évaluation des relations avec les tiers, les fournisseurs et les prestataires de services.
- Planification / test de la continuité de l'activité, et participation à des exercices et des tests de reprise après sinistre.

risques de l'organisation évolue en même temps que les risques, la deuxième ligne est essentielle pour la gouvernance et la surveillance nécessaires à la préparation et à la sécurisation adéquates de l'organisation face à panorama évolutif de menaces. Un incident de sécurité peut inciter une organisation à revoir son appétence pour le risque et les pouvoirs publics à adapter la législation et la réglementation.

Selon le Guide pratique : « l'audit interne et les activités de la deuxième ligne de maîtrise » de l'IIA, surveiller et concevoir des règles, des normes et fixer des limites constituent les principes clés de la deuxième ligne. Par exemple, des attentes et des règles claires, basées sur les niveaux de risque de vulnérabilité, y compris les taux acceptables de non-conformité, doivent être établies pour faciliter l'application des correctifs aux infrastructures sensibles avant de faire remonter les problèmes à la direction générale.

La deuxième ligne de maîtrise doit travailler en étroite collaboration avec la première et la troisième lignes pour véritablement sensibiliser le Conseil et les organes dirigeants et assurer un *reporting* des contrôles et des risques de cybersécurité adéquat et actualisé. La cybersécurité doit être une priorité pour la deuxième ligne lorsqu'elle réalise son évaluation des risques et en rend compte.

Aussi, selon le secteur et le type d'organisation, une cellule dédiée à l'évaluation des risques de cybersécurité peut être nécessaire.

Le rôle de la deuxième ligne de maîtrise doit être clair. Par exemple, le rôle joué par la conformité SI lors d'un incident urgent de sécurité doit être compris avant la survenue d'un tel incident. Les indicateurs de risques clés, une fois des seuils d'alerte mis en place, s'avèrent aussi des outils très utiles en matière de surveillance, de gouvernance, et de *reporting*.

Des prestataires et des fournisseurs clés interviennent dans les processus critiques des organisations. En ce qui concerne le risque de cybersécurité, la deuxième ligne de maîtrise peut avoir besoin d'évaluer les relations avec les prestataires externes, notamment parce que ces derniers disposent d'accès à des données classifiées et sensibles *via* une connexion directe au réseau ou d'autres méthodes de transfert de données. Les contrôles contractuels et techniques nécessitent d'être revus, il est donc essentiel que les prestataires fournissent périodiquement une assurance avec un *reporting* adéquat des contrôles de cybersécurité décidés en amont.

La deuxième ligne de maîtrise est chargée de s'assurer que le management propose aux prestataires un cadre de bonne gouvernance relatif aux risques de cybersécurité. Ce cadre inclut typiquement l'obtention et la revue de rapports de contrôle, la surveillance des activités de contrôle et la remontée appropriée des risques aux organes dirigeants au sein de l'organisation, tels que le comité de risques fournisseurs, quand ces derniers ne répondent pas aux attentes ou ne respectent pas les dispositions des niveaux de service (SLA).

Écueils au niveau de la première ligne et de la deuxième ligne de maîtrise

La plupart du temps, les écueils proviennent d'un manque d'intégration des contrôles et de surveillance du dispositif de cybersécurité. Chaque jour, de nouvelles menaces et vulnérabilités apparaissent. L'absence de formation, de sensibilisation et de contrôle robustes et réguliers en matière de cybersécurité, favorise les attaques et les menaces envers une organisation et compromet les systèmes vitaux et les données.

Pour atténuer ce risque, de nombreuses organisations ont créé un comité de la cybersécurité. Le plus souvent piloté par le responsable de la sécurité *(Chief Security Officer, CSO)* le responsable de la sécurité de l'information *(Chief Information Security Officer,CISO)* et/ou le responsable de la protection de la vie privée, ce comité se réunit régulièrement avec les parties prenantes de l'infrastructure, du réseau et les équipes de sécurité, ainsi qu'avec les membres concernés par la gestion du risque SI et de la conformité SI. L'un des principaux objectifs du comité est de prendre connaissance des actifs clés de l'organisation, des évaluations des risques, des probabilités des menaces, de l'impact potentiel et des contrôles en place pour protéger de la meilleure façon ces actifs des cyberattaques. Le comité aborde également la question des menaces émergentes et des indicateurs pertinents, y compris les résultats des récents tests d'intrusion, qui mettent à l'épreuve l'efficacité des défenses de sécurité en imitant les actions de véritables assaillants.[2]

D'autres dangers peuvent apparaître :

- En l'absence de lignes de maîtrise clairement identifiées fonctionnant en étroite collaboration pour s'assurer que les risques importants sont connus et gérés de façon efficace et efficiente.
- Par manque d'implication et de soutien de la direction, pour que la stratégie en matière de cybersécurité reçoive toute l'attention nécessaire.
- Faute de réponse en temps opportun et d'analyse causale post-incident.
- En l'absence de dispositifs d'escalade et de responsabilités définis pour répondre aux incidents de plus en plus sérieux.
- Faute de compétences nécessaires.
- A cause d'une connaissance insuffisante du secteur et des méthodes pour répondre de façon proactive aux risques émergents.
- Pour des investissements ou un budget insuffisants en termes de temps, de moyens financiers et de ressources consacrés aux initiatives de cybersécurité, y compris la maintenance de routine et les correctifs.

Le rôle de l'audit interne en tant que troisième ligne de maîtrise

Si la gouvernance relève principalement de la responsabilité du Conseil et de la direction générale de l'organisation, son évaluation est l'un des principaux rôles de l'audit interne. La Norme 2110.A2[3] de l'IIA requiert que l'audit interne évalue la gouvernance des systèmes d'information de l'organi-

[2] ISACA, "ISACA Glossary of Terms," 69. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (consulté le 20 juin 2016). Tous droits réservés. Reproduction autorisée.

[3] Cadre de Référence International des Pratiques Professionnelles (CRIPP, *International Professional Practices Framework*) (Altamonte Springs : The Institute of Internal Auditors, Inc., 2013), 30.

sation et soutienne la stratégie et les objectifs de l'organisation.

En tant que troisième ligne de maîtrise, l'audit interne joue un rôle important dans la coordination avec la deuxième ligne, notamment en matière de cybersécurité. L'audit interne peut être consulté sur les sujets suivants :

- Les relations entre cybersécurité et les risques de l'organisation.
- La priorisation des réponses et des activités de contrôle.
- L'audit des activités de maitrise des risques de cybersécurité à travers tous les aspects pertinents de l'organisation ; par exemple, accès privilégié, conception du réseau, gestion des fournisseurs, surveillance et autres.
- Les missions d'assurance relatives aux activités de remédiation.
- La sensibilisation au risque et la coordination avec la gestion des risques de cybersécurité, notamment dans les organisations dont les fonctions de la première ligne et de la deuxième ligne sont peu matures.
- La confirmation que des dispositions en matière de cybersécurité sont incluses dans les plans de continuité d'activité de l'organisation et dans les tests de reprise après sinistre.

Encadré 4 :
Activités usuelles à la troisième ligne de maîtrise

- Réaliser des évaluations en continu des mesures préventives et de détection liées à la cybersécurité.
- Évaluer les actifs SI des utilisateurs bénéficiant d'un accès privilégié pour les configurations de sécurité classiques, les sites web posant problèmes, les logiciels malveillants et l'exfiltration de données.
- Suivre la mise en œuvre des activités de remédiation.
- Évaluer le cyberisque des organisations de services, des tiers et des prestataires (note : la première ligne et la deuxième ligne de maîtrise partagent cette responsabilité permanente).

Dans le cadre de l'évaluation de l'efficacité du processus de gestion des risques requis par la Norme 2120, l'audit interne évalue de façon indépendante les les risques et les contrôles liés à la cybersécurité pour s'assurer de leur cohérence avec les risques de l'organisation. Il s'agit de revoir l'adéquation de la deuxième ligne de maîtrise concernant les cadres, les normes, le management des risques et la gouvernance.

De plus, l'audit interne évalue l'efficacité des contrôles de la première ligne de maîtrise. Il est important de noter que les contrôles généraux informatiques sont fondamentaux sans toutefois apporter une solution complète capable d'atténuer les risques de cybersécurité. La complexité de la cybersécurité nécessite plusieurs niveaux de contrôle, tels qu'une surveillance du risque, la détection des évènements quand ils surviennent, et la mise en œuvre d'actions correctives.

Puisque l'assurance fondée sur les évaluations distinctes et traditionnelles ne parvient pas à suivre le rythme des évolutions des risques de cybersécurité, la mise en place d'une stratégie d'assurance innovante est nécessaire. De plus en plus, on recourt à des techniques d'audit continu pour évaluer les changements intervenus dans les configurations de sécurité, les tendances comme les cas particuliers dans les risques émergents, les temps de réponse et les activités de remédiation.

Pour accroître la valeur de l'audit interne, le responsable de l'audit interne peut chercher à adopter une démarche d'assurance en continu innovante à travers des évaluations permanentes, qui permettent une communication proactive et en temps opportun sur les risques émergents. Le GTAG *(Global Technology Audit Guide)* « Audit en continu : coordonner l'audit et le contrôle en continu pour fournir une assurance continue » clarifie la façon de bâtir une stratégie pour réaliser des évaluations en continu en coordination avec les fonctions de la deuxième ligne de maîtrise.

Selon le guide pratique, *« Reliance by Internal Audit on Other Assurance Providers »,* l'audit interne peut s'appuyer sur la deuxième ligne de maîtrise à condition que l'auditeur interne ait reperformé ou vérifié les travaux et aboutisse à la même conclusion. Par exemple, au lieu de réaliser une nouvelle fois un test d'intrusion effectué par le management des risques SI, un auditeur interne peut se baser sur les détails du test (y compris le périmètre) et décider s'il est envisageable de se fier aux résultats. Chaque fois que possible, l'auditeur interne doit observer et interroger le personnel technique qui a effectué le travail, en s'appuyant sur les résultats et les leçons tirées pour les inclure dans les futures procédures d'audit interne relatives à la cybersécurité.

En accord avec la première ligne et la deuxième ligne de maîtrise, l'audit interne devrait discuter et établir de façon claire les attentes à l'égard des prestataires externes. Et selon l'étendue des services, ces prestataires peuvent organiser une surveillance continue du risque de cybersécurité, compte-tenu de la demande croissante d'infrastructures hébergées favorisée par le développement du *cloud computing*. Grâce aux outils de contrôle en continu, les prestataires ont développé des compétences en cybersécurité qui leur permettent de proposer au management un moyen abordable pour mesurer rapidement le cyberisque et réduire les temps de réponse. Toutefois, ces services ne sont pas les premières sources d'assurance, et les organisations utilisatrices demandent rarement que leurs prestataires assurent une surveillance continue.

Vous trouverez ci-dessous les dix questions que les responsables de l'audit interne doivent poser quand ils évaluent la gouvernance d'une organisation en matière de cybersécurité.

1. La direction générale et les organes de gouvernance (comité d'audit, Conseil d'administration, etc.) sont-ils sensibilisés aux risques clés liés à la cybersécurité ? Les initiatives en matière de cybersécurité reçoivent-elles le soutien approprié ? Sont-elles considérées comme prioritaires ?
2. Le management a-t-il réalisé une évaluation des risques pour identifier les actifs susceptibles de subir des cybermenaces ou de connaître des incidents de sécurité ? L'impact potentiel (financier et extra-financier) a-t-il été évalué ?
3. La première et la deuxième lignes de maîtrise collaborent-elles avec leurs pairs du secteur (conférences, forums et *webcasts*, par exemple) pour rester au fait des risques nouveaux/émergents, des faiblesses usuelles et des failles de cybersécurité ?
4. Les politiques et procédures de cybersécurité sont-elles en place ? Les collaborateurs et les sous-traitants ont-ils régulièrement suivi des sessions de sensibilisation à la cybersécurité ?
5. Les processus SI ont-ils été conçus pour détecter les cybermenaces ? Sont-ils opérationnels ? Le management dispose-t-il de suffisamment de dispositifs de surveillance en place ?
6. Des mécanismes de *feedback* sont-ils en place pour fournir à la direction générale et au Conseil un point de vue sur le statut des programmes de cybersécurité de l'organisation ?

7. Le management dispose-t-il d'une *hotline* opérationnelle ou de procédures d'urgence dans l'éventualité d'une cyberattaque ou d'une cybermenace ? Ces procédures ont-elles été portées à la connaissance des collaborateurs, des sous-traitants et des prestataires ?
8. L'audit interne est-il en mesure d'évaluer les processus et les contrôles visant à limiter les cybermenaces ? Le responsable de l'audit interne doit-il envisager de recourir à des ressources supplémentaires spécialisées ?
9. L'organisation dispose-t-elle d'une liste de prestataires externes ayant accès au système, y compris ceux stockant des données en externe (prestataires SI, fournisseurs de stockage dans le *cloud*, organismes de paiement, par exemple) ? Une mission d'évaluation de l'efficacité des contrôles de l'organisation dans le cadre du programme de gestion des risques de cybersécurité a-t-elle été effectuée ?
10. L'audit interne a-t-il identifié correctement les cybermenaces communes auxquelles est confrontée l'organisation (par exemple, états-nations, cybercriminels, haktivistes, systèmes en réseau, opérateurs de *cloud*, fournisseurs, systèmes de médias sociaux, logiciels malveillants), et les a-t-il inclus dans l'évaluation des risques de l'audit interne et dans le processus de planification ?

Encadré 5 :
Les signaux qui alertent sur les failles potentielles dans la gouvernance

- Une structure de gouvernance hétérogène et fragmentée.
- Une stratégie incomplète.
- Des retards dans la démarche de cybersécurité.
- Des coupes et des réductions de budget.

Ces 10 questions mettent bien en évidence la nécessité d'une gouvernance robuste, au plus haut niveau et dans l'ensemble de l'organisation. Quand les réponses sont systématiquement positives dans toute l'organisation, il est probable qu'une gouvernance adaptée soit en place.

À partir des réponses obtenues, le responsable de l'audit interne peut commencer à identifier les signaux d'alerte liés à la cybersécurité. Il évalue si la deuxième ligne de maîtrise opère de façon stratégique et si la première ligne de maîtrise est bien placée pour identifier et répondre aux risques et mettre en œuvre rapidement les actions correctives. L'évolution globale dépendra de la structure de gouvernance . L'Encadré 5 répertorie les signaux d'alerte sur les failles potentielles dans la gouvernance.

Il revient au responsable de l'audit interne d'interpréter les réponses préliminaires à ces questions et de commencer le processus d'identification des domaines menacés selon une approche fondée sur les risques. Le jugement professionnel du responsable de l'audit interne est important dans la compréhension de l'interdépendance des menaces contre la cybersécurité.

Il est important de noter que la structure de gouvernance de la direction générale peut impacter la façon dont ces signaux d'alerte sont perçus. C'est pourquoi, le jugement professionnel du responsable d'audit interne et l'approche d'audit fondée sur les risques peuvent faciliter la communication de ces signaux d'alerte et évaluer si le management dispose de contrôles pour atténuer les menaces.

Les signaux d'alerte les plus courants peuvent mettre en évidence des symptômes d'une gouvernance insuffisante : un manque de vision stratégique dans le programme de cybersécurité et les initiatives qui y sont liées et/ou des retards de plusieurs années dans les activités relatives à la cybersécurité. Des coupes significatives dans le budget de la sécurité doivent également attirer l'attention. Si la fonction de sécurité de l'information est passive et n'a pas la volonté ou la capacité de rendre compte au management des cybercontrôles nécessaires, il peut être utile de sensibiliser davantage la direction et d'augmenter le soutien à la fonction.

Périmètre de l'audit interne et coordination

La délimitation du périmètre pour couvrir le risque de cybersécurité est un exercice conjoint pour lequel l'audit interne doit, dans sa planification, prendre en compte les fonctions de la deuxième ligne de maîtrise. La planification de l'audit est plus efficace lorsqu'elle intégre les fonctions qui mettent en perspective la hiérarchisation de l'impact métier et avec lesquelles il faudra collaborer pendant et après l'audit interne.

Le responsable de l'audit interne détermine ce qui est couvert par le plan d'audit interne et repérer les domaines pour lesquels l'assurance peut ne pas être fournie. Dans le cadre de la Norme 2050 de l'IIA , une couverture adéquate du risque de cybersécurité nécessitera de collaborer avec la première et la deuxième lignes de maîtrise pour s'assurer que l'audit interne identifie l'information la plus importante pour l'organisation. L'audit interne travaille alors avec les propriétaires de données concernés (y compris la gestion de données de l'entreprise), évalue le processus de fourniture de services et détermine qui a été autorisé à accéder aux données en contexte et quelle est l'importance de ces données.

L'audit interne travaille ensuite avec le management opérationnel pour identifier les systèmes et les technologies qui permettent l'accès aux informations sensibles (par exemple, les données des collaborateurs, les données personnelles identifiables, le numéro des cartes de crédit des clients, l'historique des commandes fournisseurs). La collaboration avec le management aidera également à s'assurer que les éléments pertinents liés aux vulnérabilités de cybersécurité sont contrôlés de façon permanente. L'audit interne doit envisager de prendre en compte les personnes autorisées à accéder aux informations sensibles lors de la définition du périmètre d'audit et évaluer la technologie liée à ces accès.

Les questions suivantes facilitent le processus d'identification des informations sensibles :

- Quelle information est considérée comme sensible et pourquoi ?
- Quelle est la valeur des données (pour les fraudeurs, les concurrents, etc.) ?
- Où l'information est-elle accessible, traitée et stockée ?
- Comment l'information est-elle transmise ?
- Quel est le niveau de rigueur à respecter pour accorder ou supprimer un accès ?
- Les niveaux d'accès ont-ils été déterminés en fonction des rôles ? Quels rôles disposent d'un accès administrateur ?
- Comment l'accès est-il attribué, approuvé, contrôlé et supprimé ?
- Quel est le degré de protection des données en accès non autorisé ?

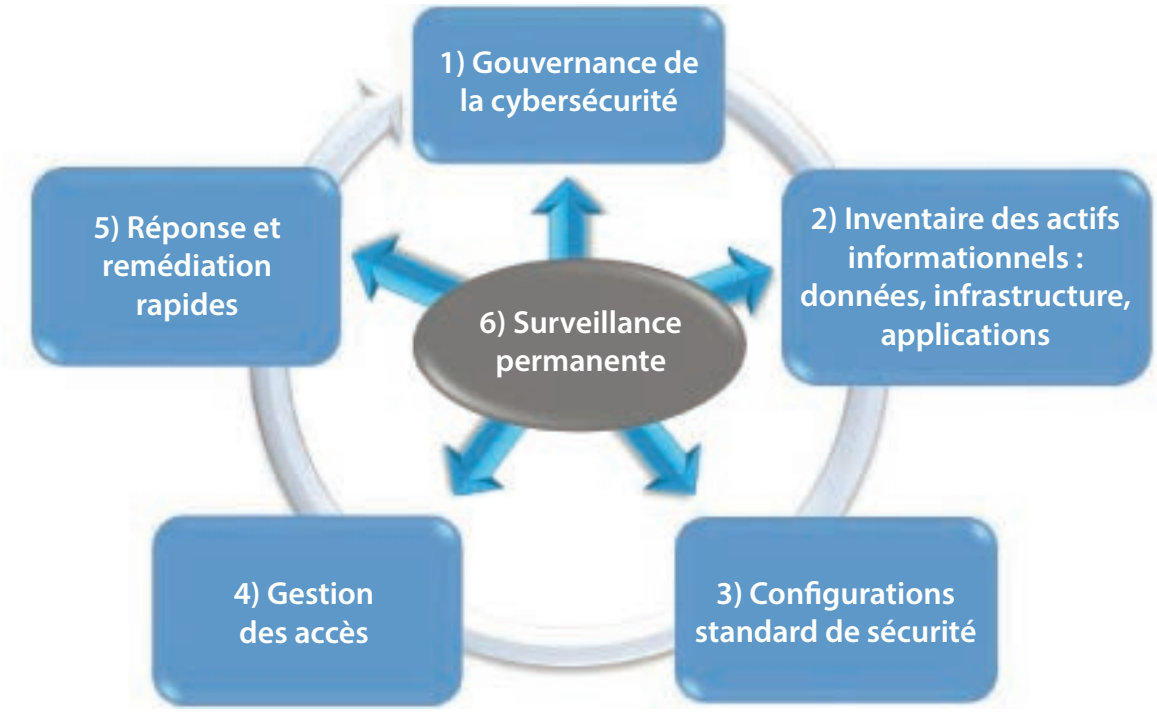
- Quels types de tests sont réalisés (intrusion, accès, suivi des modifications, etc.) ?
- Comment le risque de cybersécurité est-il contrôlé pour ceux qui ont un accès fonctionnel aux informations sensibles ?

Si ce n'est déjà prévu dans un plan de continuité d'activité ou de reprise après sinistre, le management doit envisager de réaliser une analyse de l'impact métier pour classer, hiérarchiser et documenter l'ensemble des systèmes, des données et des ressources sensibles. Le responsable de l'audit interne peut utiliser les résultats de l'analyse d'impact métier pour déterminer si le plan d'audit interne couvre suffisamment les systèmes qui abritent des informations sensibles. Le responsable de l'audit interne peut communiquer au Conseil les domaines pour lesquels des activités d'assurance existent ou pas et les plans de couverture du périmètre.

Une démarche d'évaluation des risques et des contrôles de cybersécurité

Le schéma constitué de six domaines interdépendants qui est présenté ci-après peut être utilisé pour évaluer la conception et l'efficacité opérationnelle des dispositifs de contrôles et de gouvernance de cybersécurité du manager. Les défaillances de l'une des composantes peuvent avoir un impact sur l'efficacité globale de la cybersécurité, en évaluant la façon dont chaque composante est conçue et comment elle fonctionne avec les autres, le responsable de l'audit interne dispose d'une base qui lui permet de déterminer si l'organisation est bien préparée à affronter les risques de cybersécurité. Quand les composantes ne sont pas bien conçues ou ne fonctionnent pas correctement ensemble, l'organisation n'est pas à même d'affronter les cybermenaces et les risques qui en découlent.

Référentiel d'évaluation des risques de cybersécurité



Composante 1 : Gouvernance de la cybersécurité

L'audit interne doit comprendre la gouvernance de la cybersécurité de l'organisation. La Norme 2100 exige que l'audit interne évalue les processus de gouvernance, de gestion des risques et de contrôle de l'organisation et contribue à leur amélioration. Le processus de gouvernance peut inclure une clarification des rôles et des responsabilités, le devoir de rendre compte, l'adoption d'une stratégie pluriannuelle et la priorisation de plans d'action permettant une collaboration stratégique entre les diverses parties prenantes.

Une gouvernance robuste de la cybersécurité repose sur :

- La collaboration et la collecte de renseignements ou d'expertise sur les risques de cybersécurité, fondées sur les menaces qui pèsent sur l'organisation.
- La détermination de l'appétence et de la tolérance au risque.
- La planification de la continuité et de la reprise d'activité en cas de sinistre conduisant à une interruption d'activité.
- Le traitement rapide des incidents de sécurité.
- Le développement d'une culture de la sensibilisation aux risques et aux menaces de cybersécurité.

Une gouvernance efficace se matérialise par des politiques clairement définies, des outils pertinents, un effectif suffisant et des formations adaptées.

Des parties prenantes multiples, avec des perspectives diverses, renforcent la qualité de la gouvernance. Habituellement, un comité de gouvernance cybersécurité réunit la direction générale et des représentants des trois lignes de maîtrise ; les responsables des processus et de la technologie, et éventuellement des parties prenantes externes clés, telles que des fournisseurs, des clients, des prestataires de services et des organisations similaires.

Les équipes d'intervention en cas d'incident de sécurité rendent compte régulièrement au management et au Conseil du type d' incident rencontrées afin de fournir des points de vue complémentaires sur des failles jusqu'ici inconnues. Le management peut alors suivre les problémes identifiés jusqu'à leur remédiation.

Composante 2 : Inventaire des actifs informationnels

Le département SI doit disposer d'un inventaire actualisé de l'ensemble des actifs informationnels et identifier ceux qui sont les plus indispensables à l'atteinte des objectifs de l'organisation et à la continuité de ses opérations. Pour répondre aux initiatives stratégiques et aux objectifs de l'organisation, ces actifs nécessitent plus que des contrôles généraux informatiques traditionnels et des évaluations périodiques. Des contrôles préventifs et détectifs conçus pour protéger les actifs les plus critiques doivent être réalisés en permanence pour en assurer l'efficacité continue.

Lors de l'évaluation des actifs informationnels de l'organisation, les aspects suivants doivent être pris en considération :

- Les données
  - Les types de données (par exemple, transactionnelles, configuration SI, non structurées)
  - La classification des données (permet la standardisation et la priorisation)
  - Les environnements de données (par exemple, entrepôts de données, principales bases de données)
- Les équipements d'inventaire des infrastructures informatiques
  - Les serveurs
  - Les équipements réseau
  - Le stockage
  - Les terminaux destinés aux utilisateurs (par exemple, ordinateurs portables, appareils mobiles)
- Les applications
- Les relations externes
  - Les environnements hébergés par des tiers
  - Le partage de fichiers de données avec des organisations externes (par exemple, fournisseurs, régulateurs, administrations publiques)

La capacité à identifier quels logiciels et quels appareils interagissent sur le réseau est fondamentale afin d'être en mesure de se défendre contre les cybermenaces. L'organisation ne peut pas lutter contre des attaques réseau visant des appareils ou des logiciels qui ne sont pas recensés. Les organisations qui autorisent leurs collaborateurs à utiliser leurs appareils personnels doivent faire face à un plus grand nombre et une plus grande variété d'appareils et de logiciels accèdant aux données *via* le réseau d'entreprise. Le management devrait porter une attention particulière au contrôle de ces appareils personnels et leur connexion au réseau. De plus en plus, on demande aux collaborateurs d'avoir un accès plus large et permanent aux données de l'organisation. La capacité à détecter, authentifier et inventorier les appareils inconnus permettra à l'organisation de suivre, contrôler et mesurer les changements subis par ces appareils afin de s'assurer que l'ensemble de la stratégie de cybersécurité est efficace.

Composante 3 : Configurations standard de sécurité

Un logiciel de gestion automatisée et centralisée de la configuration peut être utilisé pour établir et maintenir les configurations de référence *(baselines)* concernant les appareils, les systèmes d'exploitation et les applications informatiques. Un logiciel de gestion s'avère souvent plus efficace que des systèmes administrés manuellement ou de façon non standardisée. L'équipe de sécurité informatique et l'audit nterne devraient passer en revue les configurations de référence pour s'assurer qu'une évaluation précise fondée sur les risques peut être réalisée (par exemple, des environnements Web accessibles de l'extérieur peuvent nécessiter des protections supplémentaires). Il est indispensable de mettre en place des processus de gestion des correctifs (*patches :* en particulier de sécurité) et de mises à jour des logiciels et des matériels pour maintenir la robustesse des configurations au fur et à mesure que de nouvelles menaces sont connues.

Composante 4 : Gestion des accès

Le management devrait envisager de mettre en place des contrôles préventifs tels qu'un processus standard de validation et d'approbation de l'accès des utilisateurs en fonction de leur profil. De plus, des mesures de détection des mobilités des collaborateurs au sein de l'organisation pourraient aider à s'assurer que les accès restent pertinents au regard de leurs nouvelles fonctions. L'audit interne peut réaliser une revue des droits d'accès aux données et aux systèmes clés pour confirmer que les autorisations accordées correspondent aux fonctions occupées.

Les accès privilégiés de type « administrateur »sont particulièrement importants. Les utilisateurs bénéficiant de la capacité d'accéder à des données et de les diffuser sont les plus susceptibles d'être concernés par le risque de cybersécurité. En dévoilant son mot de passe involontairement ou en téléchargeant un logiciel malveillant suite à une opération de hameçonnage *(phishing)*, un utilisateur laisse la porte ouverte au contournement des couches de contrôles systématiques conçues pour empêcher les accès non autorisés. La problématique des accès ne concerne pas uniquement les utilisateurs interne à l'organisation, mais aussi les utilisateurs externes. Il convient donc de faire attention aux collaborateurs, consultants et fournisseurs ayant accès aux données clés, que ces données soient hébergées en interne ou en externe. L'une des mesures phares de l'efficacité du programme de cybersécurité de l'organisation est de valider les contrôles préventifs visant à accorder et supprimer les accès ainsi qu'à évaluer le niveau de sensibilité et les comportements des utilisateurs bénéficiant d'accès privilégiés aux données.

Composante 5 : Réponses et remédiation rapides

La capacité de l'organisation à communiquer et à répondre rapidement aux risques indique l'efficacité et le niveau de maturité du programme de cybersecurité de l'organisation. Les programmes matures permettent de réduire en permanence le temps de réaction du management. La deuxième ligne de maîtrise a notamment pour rôle de :

- communiquer sur les risques significatifs ;
- déclencher les activités de remédiation ;
- suivre les problèmes identifiés jusqu'à leur remédiation ;
- rendre compte de la résolution dans l'entité.

Composante 6 : Surveillance permanente

Dernière composante de ce référentiel, l'audit en continu de chacune des cinq composantes décrites ci-dessus aidera à déterminer la façon dont le risque est géré et si les actions correctives sont efficaces. Une démarche d'évaluation efficace nécessite plus que de simples questionnaires de conformité aux règles de sécurité. La deuxième ligne de maîtrise devrait mettre en place une stratégie de surveillance visant à déclencher des changements dans les comportements, notamment :

- **L'évaluation et l'analyse fondées sur le niveau d'accès** qui implique de surveiller l'activité des utilisateurs bénéficiant d'un accès aux informations sensibles pour mesurer le risque de

cybersécurité associé. Pour un sous-groupe d'utilisateurs qui réalisent les opérations les plus sensibles, il apparait utile de développer des moyens systématiques de détection des vulnérabilités liés aux actifs concernés, aux configurations de sécurité, aux sites web exposés, aux incidents causés par les logiciels malveillants et le vol de données.

- **L'évaluation de la vulnérabilité :** une analyse régulière des systèmes est indispensable pour identifier les vulnérabilités au sein de l'environnement. Une fois ces vulnérabilités identifiées, catégorisées (par exemple, selon qu'elles sont critiques, majeures, modérées) et prises en charge (par exemple, résoudre les vulnérabilités critiques sur les systèmes à haut risque dans un délai de 30 jours), les activités de remédiation doivent être conduites pour les vulnérabilités identifiées.
- **La priorité accordée aux systèmes accessibles de l'extérieur** qui présentent souvent les risques les plus élevés pour les organisations. Cependant, la remédiation est plus efficace quand elle ne se limite pas à ces environnements. La première et la deuxième lignes de maîtrise peuvent définir et s'accorder sur les niveaux de services (SLA) à travers l'organisation. L'audit interne peut contribuer en évaluant le respect de ces niveaux de services (SLA) par le management .
- **L'évaluation et le contrôle des risques liés à des tiers :** les programmes de cybersécurité peuvent aider à l'évaluation des risques liés à des fournisseurs tiers et des risques de sécurité liés aux types de services proposés. Par exemple, si le fournisseur héberge des données sensibles de l'organisation, le management doit envisager de se doter de programmes de surveillance tels que :
  - le suivi actif des niveaux de services (SLA) ;
  - les changements dans la configuration de sécurité de l'information ;
  - les conclusions des missions indépendantes dédiées à l'analyse de la cybersécurité ;
  - les rapports sur les contrôles des sociétés de services (SOC) ;
  - l'évaluation de la vulnérabilité et tests d'intrusion ;
  - les procédures de remontée d'information auprès de la direction du fournisseur ;
  - l'évaluation des configurations de référence *(baseline)* pour inspecter les contrôles de sécurité clés ;
  - les évaluations permanentes qui analysent l'architecture technique et les contrôles en place pour protéger les données de l'organisation ;
  - le suivi des ressources des tiers bénéficiant d'un accès au réseau et aux systèmes de l'organisation pour garantir que ces ressources ne sont pas impliquées dans des activités inappropriées ou n'exposent pas l'organisation à des risques inutiles.
- **Tests d'intrusion :** la deuxième ligne de maîtrise peut réaliser des tests d'intrusion concernant les vulnérabilités connues afin d'évaluer l'efficacité des contrôles techniques préventifs, ainsi que la capacité du management à détecter et répondre à ces attaques. Les tests d'intrusion incluent des vérifications inopinées pour fournir une évaluation plus fiable et plus objective de la préparation et des capacités de réaction de l'organisation face à des situations de cyberattaques réelles. Toutefois, le champ des tests doit être raisonnable, ne pas perturber les opérations, et être approuvé en amont par la hiérarchie concernée. Par exemple, le test d'un scénario d'attaque par déni de services, c'est à dire visant une interruption de réseau avec une intention malveillante, doit être coordonné avec la direction pour ne perturber les opérations courantes.

- **Logiciel malveillant :** les vulnérabilités pouvant être découvertes après l'envoi de l'appareil ou du logiciel au client, une procédure doit être mise en place pour analyser régulièrement les appareils et les produits, identifier les vulnérabilités et corriger le système en respectant l'ordre des priorités (par exemple, les actifs critiques avec des correctifs critiques en premier). Certains systèmes et correctifs peuvent tomber sous un seuil de risques défini, et donc être contrôlés et identifiés, sans actions supplémentaires.
- **Surveillance des incidents et réponse :** En cas d'incident, la combinaison de ces processus permet à une organisation de détecter, répondre, remédier, rétablir et communiquer au management. Les systèmes de journalisation et de surveillance, ainsi qu'une équipe experte en charge de la résolution des incidents sont essentiels pour s'assurer que ces contrôles permettent d'atteindre les objectifs.

Les risques de cybersécurité émergents du secteur ainsi que les incidents rencontrés par l'organisation ou par d'autres organisations semblables nécessitent des ajustements de la stratégie de contrôle permanente au fil du temps.

L'annexe D reprend chaque composante de ce référentiel et les activités du management, y compris le contrôle en continu, que l'audit interne peut souhaiter prendre en considération dans la mise en œuvre d'audit et d'assurance en continu.

Rôle du responsable de l'audit interne dans la communication au Conseil et aux autres organes dirigeants de l'assurance relative à la cybersécurité

Alors que le panorama des risques évolue et que le recours aux services de *cloud*, aux appareils mobiles et aux médias sociaux augmente, les cybermenaces s'accroissent. Les responsables de l'audit interne devraient s'entretenir régulièrement avec la direction générale et le Conseil à propos de l'appétence pour le risque de l'organisation. Ils doivent également rencontrer régulièrement les responsables ou le comité en charge de la gestion des risques de l'organisation et prioriser les menaces et les risques de cybersécurité afin de s'assurer que les ressources sont bien affectées aux enjeux les plus importants. Il est donc essentiel que le management choisisse et développe une stratégie dédiée aux systèmes d'information et aux données les plus sensibles de l'organisation et que le responsable de l'audit interne, confirme cette stratégie avec la direction générale et le Conseil.

Le Conseil et la direction générale s'en remettent au responsable de l'audit interne pour obtenir une assurance relative à la gestion et au contrôle des risques, y compris à l'efficacité globale des activités réalisées par la première et la deuxième lignes de maîtrise pour la gestion et l'atténuation des menaces et des risques de cybersécurité. Le Conseil doit avoir une bonne compréhension des données et des SI les plus importants pour l'organisation et obtenir de la part du directeur des systèmes d'information, du responsable de la sécurité des systèmes d'information, du responsable de la sécurité, du responsable des infrastructures informatiques et du responsable de l'audit interne une assurance quant à la mise en œuvre de contrôles pour prévenir, détecter et atténuer les cyber-risques à un seuil de tolérance acceptable.

Le responsable de l'audit interne doit s'assurer que les membres du Conseil sont bien informés des cybermenaces spécifiques à leur secteur et de l'impact possible des incidents de cybersécurité sur leur organisation. Il peut être intéressant pour le Conseil et la direction générale de participer à des sessions de sensibilisation et de formation afin de mieux cerner le type de cybermenaces qui pourraient peser sur l'organisation. En augmentant en permanence son niveau de sensibilisation, le Conseil sera doté des connaissances nécessaires pour confirmer la structure de gouvernance appropriée est en place et est capable de protéger et de contrôler les données et les systèmes vitaux de l'organisation. Les sujets techniques de cybersécurité, traduits en information concrète, permettent au Conseil d'exercer ses fonctions de surveillance et d'assurer, au fil du temps, le suivi du cyber-environnement et des risques qui y sont associés.

Une communication efficace entre les trois lignes de maîtrise et le Conseil est essentielle. L'établissement d'une communication régulière aide à s'assurer que le Conseil a bien reçu les informations nécessaires à la réalisation de son rôle de surveillance du contrôle interne. Le Conseil aura besoin aussi du responsable de l'audit interne pour obtenir l'assurance que le management dispose d'une stratégie et des mesures adéquates pour informer le Conseil, les autorités de contrôle, les clients et le public en cas de d'incident majeur. Les dispositifs de remontée d'informations et de commu-

nication doivent être établis et revus par le Conseil afin de garantir une notification adaptée et en temps opportun en cas d'incident.

La stratégie et le plan de communication devraient être clairement formalisés avec les rôles et les responsabilités de chacun en cas de survenue d'un événement de cybersécurité. Le plan doit être testé et des projets de communication officielle et de communiqués de presse revus, à l'avance, par un conseiller juridique. Une stratégie de réponse et de remédiation globale et bien préparée aidera à réduire l'impact sur l'organisation et à maintenir la confiance des clients et des autres parties prenantes en cas d'incident.

Annexe A - Principales normes IIA concernées[4]

Les extraits suivants des *Normes internationales pour la pratique professionnelle de l'audit interne* (Les *Normes*) de l'IIA, sont pertinents pour la cybersécurité.

Norme 1210 – Compétence
Les auditeurs internes doivent posséder les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités.

> **1210.A3 –** Les auditeurs internes doivent posséder des connaissances suffisantes des principaux risques et contrôles relatifs aux systèmes d'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique.

Norme 2050 – Coordination et utilisation d'autres travaux
Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations, coordonner les activités, et envisager d'utiliser les travaux des autres prestataires internes et externes d'assurance et de conseil.

Norme 2110 – Gouvernance
L'audit interne doit évaluer et formuler des recommandations appropriées en vue d'améliorer les processus de gouvernance de l'organisation pour :

- les prises de décisions stratégiques et opérationnelles ;
- la surveillance des processus de management des risques et de contrôle ;
- la promotion des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- la communication aux services concernés des informations relatives aux risques et aux contrôles ;
- la coordination des activités et la communication des informations entre le Conseil, les auditeurs externes, les auditeurs internes, les autres prestataires d'assurance et le management.

> **2110.A2 –** L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation.

Norme 2120 – Management des risques
L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration.

[4] Il s'agit de la version actualisée au 1er janvier 2017.

Annexe B - Lignes directrices de l'IIA en la matière

Guide pratique, *« Business Continuity Management – Crisis Management »*
Guide pratique, *« Auditing Privacy Risks, 2nd Edition »*
GTAG, *« Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition »*
GTAG, *« Management of IT Auditing, 2nd Edition »*
GTAG, *« L'infogérance, 2e édition »*
GTAG, *« Gestion des identités et des accès »*
GTAG, *« Élaboration d'un plan d'audit des SI »*
GTAG, *« Gouvernance de la sécurité de l'information »*
GTAG, *« Audit de la gouvernance des SI »*
Prise de position, *« Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces »*

Annexe C - Définition des concepts clés

Cybermenace : Provient de personnes qui cherchent à accéder sans autorisation à un dispositif de contrôle et/ou à un réseau utilisant un canal de communication de données. Cet accès peut être piloté depuis l'intérieur d'une organisation, par des utilisateurs de confiance ou à distance, par des inconnus sur Internet. Les menaces contre les systèmes de contrôle peuvent provenir de nombreuses sources, y compris de gouvernements hostiles, de groupes terroristes, de collaborateurs mécontents ou d'individus malveillants.[5]

Cybersécurité : Protection des actifs informationnels contre les menaces visant les informations traitées, stockées et transportées par les systèmes d'information reliés en réseau.[6]

Profil de sécurité : Evaluation du niveau de sécurité (par exemple, effectif, matériel, logiciel, règles)du réseau, des informations et des systèmes basée sur les ressources d'audit interne et capacités de défense et de réaction, d'une organisation en cas d'évolution de la situation.[7]

Haktivistes : Petite population de pirates informatiques politiquement actifs constituant une menace de niveau modéré, susceptibles de lancer une attaque isolée mais préjudiciable. La plupart des groupes haktivistes internationaux cherchent à faire connaître leurs idées plutôt qu'à nuire aux infrastructures critiques. Leur but est de promouvoir leurs idées politiques. La propagande et les nuisances causées servent à mettre en avant leur cause.[8]

Logiciel malveillant : Conçu pour infiltrer, endommager et obtenir des informations d'un système informatique sans le consentement de son propriétaire.[9]

Patch : Correctifs de logiciels, contre les erreurs de programmation et les vulnérabilités.[10]

Phishing (hameçonnage) : Attaque *via* e-mail pour tenter de convaincre l'utilisateur de la sincérité de l'expéditeur mais avec l'intention d'obtenir des informations utilisables dans l'ingénierie sociale.[11]

Sécurité de l'information : Permet de s'assurer à travers l'organisation que l'information est protégée contre la communication à des utilisateurs non autorisés (confidentialité), contre une modification inappropriée (intégrité) et reste inaccessible si nécessaire (disponibilité).[12]

---

[5] Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, « *Cyber Threat Source Descriptions* ». https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (consulté le 20 juin 2016).

[6] ISACA, « *ISACA Glossary of Terms* », 29. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (consulté le 20 juin 2016). Tous droits réservés. Reproduction autorisée.

[7] Richard Kissel, Editor, « *Glossary of Key Information Security Terms, NSISTIR 7298, Revision 2* », 179. 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (consulté le 5 juillet 2016).

[8] Department of Homeland Security, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#hack (consulté le 20 juin 2016).

[9] ISACA, « *ISACA Glossary of Terms* », 59. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (consulté le 20 juin 2016). Tous droits réservés. Reproduction autorisée.

[10] Ibid., p. 69.

[11] Ibid., p. 70.

[12] ISACA, « *ISACA Glossary of Terms* », 49. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (consulté le 20 juin 2016). Tous droits réservés. Reproduction autorisée.

Annexe D - Considérations de l'audit interne en matière de risques de cybersécurité

Les composantes suivantes, organisées selon les activités décrites dans ce guide, fonctionnent ensemble pour répondre au risque de cybersécurité. Le contrôle de l'efficacité opérationnelle est également abordé.

Composante 1 : Gouvernance de la cybersécurité

- Un but stratégique clair, ainsi que des parties prenantes ayant un devoir de rendre compte et des responsabilités et des rôles bien définis.
- Un rattachement qui donne l'autorité adéquate et permet l'objectivité.
- Une expertise pour déployer les outils nécessaires à la sécurité et faire appliquer les règles.
- Les modalités pratiques telles que :
  - la définition et la communication de l'appétence pour le risque ;
  - la mise en place des règles de cybersécurité ;
  - l'évaluation et le contrôle du risque, fondés sur une logique cohérente et une méthodologie ;
  - la formation et le recrutement pour déployer une stratégie de contrôle de la sécurité durable au fil de l'évolution des besoins de l'organisation ;
  - des missions dédiées et indépendantes requises pour l'examen et la cybersécurité des tiers qui produisent ou fournissent des biens et des services spécifiques.
- La communication permanente, les indicateurs, le *reporting* et suivi des actions.
- La gestion des incidents.
- La planification de la continuité d'activité liée aux scénarios de cyberattaques.
- La visibilité et l'implication de la direction générale et du Conseil.

Composante 2 : L'inventaire des actifs informationnels

- **Inventaire des données :** Le management a identifié et classé les différents types de données sensibles et critiques et leurs emplacements par rapport à l'organisation (interne ou externe).
- **Inventaire des appareils autorisés et non autorisés :** Les appareils autorisés peuvent accéder au réseau (ils sont inventoriés, suivis et contrôlés) et les appareils non autorisés sont supprimés.
  - Contrôle du nombre d'appareils non autorisés présents sur le réseau de l'organisation et délai moyen de suppression de chaque appareil non autorisé du réseau.
  - Suivi du pourcentage de systèmes sur le réseau de l'organisation qui n'utilisent pas une authentification utilisateur pour accéder au réseau de l'organisation.
  - Maintien à jour d'une liste de dispositifs réseau, de serveurs et d'appareils pour les utilisateurs finaux.

- **Inventaire des logiciels autorisés et non autorisés :** Assure que seuls les logiciels autorisés sont installés et exécutés sur le réseau (ils sont inventoriés, suivis et contrôlés) et que l'installation des logiciels non autorisés est impossible. Si un logiciel non autorisé est détecté, il doit être supprimé en temps opportun.
  - Nombre d'exemplaires de logiciels non autorisés présents sur le réseau et temps moyen nécessaire pour supprimer le logiciel non autorisé du réseau.
  - Pourcentage des systèmes de l'organisation n'utilisant pas un logiciel classé liste blanche ou liste noire.
  - Nombre d'applications logicielles bloquées par le logiciel de classification de l'organisation en liste blanche ou liste noire.
  - Pourcentage de systèmes protégés.

Composante 3 : Les configurations standards de sécurité

- **Configurations sécurisées des matériels et des logiciels sur les appareils mobiles, les ordinateurs portables et de bureau et les serveurs.** Création, mise en œuvre et gestion effective (ils sont inventoriés, suivis et contrôlés) des configurations de sécurité.
  - Pourcentage des systèmes de l'organisation non configurés selon la configuration standard validée.
  - Pourcentage des systèmes de l'organisation dotés de configuration de sécurité non validée par les applications de gestion de configuration technique.
  - Pourcentage des systèmes de l'organisation non mis à jour avec le dernier correctif de sécurité des logiciels du système d'exploitation disponible.
  - Pourcentage des systèmes de l'organisation non mis à jour avec les derniers correctifs de sécurité des applications logicielles métier disponibles.
- **Configurations sécurisées pour les dispositifs réseau tels que les pare-feu, les routeurs et les commutateurs :** Établir, mettre en oeuvre et gèrer de façon efficace (le suivi, le *reporting* et les correctifs) les configurations de référence.
  - Modification du volume et de la fréquence de la configuration sur le réseau.
  - Délai moyen d'alerte de l'administrateur de l'organisation d'une modification non autorisée de la configuration et délai moyen de blocage/ de mise en quarantaine des modifications sur le réseau.

Composante 4 : Gestion des accès aux informations

- **Usage contrôlé des privilèges administrateurs :** Contrôle de l'utilisation, l'attribution et la configuration des privilèges administrateurs sur les ordinateurs, les réseaux et les applications.
- **Contrôle et suivi des comptes :** Gèrer le cycle de vie des systèmes et des comptes (création, utilisation, inactivité et suppression).
- **Accès contrôlé fondé sur le besoin en savoir :** Suivi, contrôle, prévention et correction des accès sécurisés aux données sensibles (par exemple, information, ressources et systèmes).
- **Population d'utilisateurs :** Les processus d'accès des utilisateurs doivent concerner l'ensemble des personnes bénéficiant d'un accès aux données critiques, qu'ils s'agissent d'utilisateurs

internes ou externes. La plupart des organisations ont des collaborateurs, des consultants et des fournisseurs qui accèdent aux données en interne comme en externe. Ne pas oublier les tiers en cas d'envoi de fichiers.

Composante 5 : Réponse et remédiation rapides

- Amélioration continue du programme de cybersécurité en tenant compte des recommandations et en menant des actions en temps opportun jusqu'à la résolution.
- Évaluation des vulnérabilités, analyse des renseignements relatifs aux menaces et identification des lacunes.
- Mesure de la performance et comparaison avec les références du secteur et les homologues.
- Identification des connaissances, des qualifications et des compétences spécifiques pour soutenir le programme.
- Quelques exemples d'indicateurs :
  - Quantité et pourcentage de remédiations durables en fonction des emplacements, du service, des collaborateurs.
  - Nombre de vulnérabilités informatiques et d'exception à la règle en fonction des emplacements, du service, des collaborateurs.
  - Travaux de conformité de la plateforme en fonction des emplacements, du service.

Composante 6 : Surveillance permanente

- **Défenses contre les logiciels malveillants *(malware)* :** Contrôler l'installation, la diffusion et l'exécution des codes malveillants ; mettre rapidement à jour la stratégie de défense, collecter des données et prendre les mesures correctives nécessaires.
- **Limitation et contrôle des ports réseaux, des protocoles et des services :** Suivi, contrôle et correction des utilisations opérationnelles des ports, des protocoles et des services sur les dispositifs réseaux.
- **Sécurité des logiciels applicatifs :** Prévenir, détecter et corriger les faiblesses de sécurité de l'ensemble des logiciels achetés ou développés en interne.
- **Contrôle des accès sans fil :** Suivi, contrôle et correction de l'utilisation des réseaux locaux sans fil, des points d'accès et des systèmes clients sans fil.
- **Défense aux frontières :** Détecter, prévenir et corriger le flux d'informations transitant par les réseaux à différents niveaux de confiance.
- **Tests d'intrusion, tests d'hameçonnage et exercices d'attaque totale :** Tester la résistance globale des défenses de l'organisation (technologie, processus et effectif).
- **Maintenance, contrôle et analyse des changements :** Collecter, gérer et analyser les changements et les incidents qui pourraient aider à détecter, comprendre et rétablir la situation après une attaque. Y compris l'analyse des systèmes de détection d'intrusion (SID : Intrusion Detection System) et l'activité des utilisateurs ayant des accès privilégiés.

- **Protection des données/prévention de la perte de données :** Prévenir et atténuer les effets de vol de données, garantir la protection des données personnels/l'intégrité. Déployer des outils d'aide si nécessaire.

Auteurs / Contributeurs

Bradley C. Ames, CRMA, CISA

Forrest R. Foster, CISA

Caroline Glynn, CIA, CISA

Mike Lynn, CRMA

Dean Nakama

Tim Penrose, CIA, CISA

Sajay Rai, CISM

Réviseurs de la traduction :

Bouchra Bajjou

José Bouaniche,

Béatrice Ki-Zerbo, CIA

À propos de l'Institute of Internal Auditors

Porte-parole mondial de la profession d'audit interne, l'Institute of Internal Auditors (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 185 000 membres dans plus de 170 pays et territoires. Son siège se situe à Lake Mary (Floride) aux États-unis. Plus d'informations sont disponibles sur le site www.globaliia.org ou www.theiia.org.

À propos des lignes directrices complémentaires

Les lignes directrices complémentaires font partie intégrante du Cadre de référence international des pratiques professionnelles (CRIPP) et proposent des recommandations supplémentaires (facultatives) pour la réalisation des activités d'audit interne. Si elles reflètent les *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*), ces lignes directrices complémentaires ne visent pas directement la mise en conformité aux dites *Normes*. Elles couvrent au contraire des domaines particuliers, ainsi que des questions sectorielles, et contiennent des procédures et processus détaillés. Ces lignes directrices ont été officiellement révisées et approuvées par l'IIA.

Guides pratiques

Les guides pratiques constituent un type particulier de lignes directrices complémentaires et détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Dans le cadre des dispositions du CRIPP, la conformité aux guides pratiques est recommandée (mais non obligatoire). Ces guides pratiques ont été officiellement révisés et approuvés par l'IIA.

Le Global Technologies Audit Guide (GTAG) est un type de guide pratique qui aborde, dans un langage courant, une question d'actualité liée à la gestion, au contrôle ou à la sécurité des systèmesd'information.

Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.globaliia.org/standards-guidance ou www.theiia.org/guidance ou www.ifaci.com.

Avertissement

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. À ce titre, il doit être utilisé uniquement à des fins d'orientation. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

Copyright

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française.

Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com.

- Février 2017 - ISBN 978-2-915042-79-5-