Audit des programmes relatifs aux menaces internes

The Institute of Internal Auditors | Global

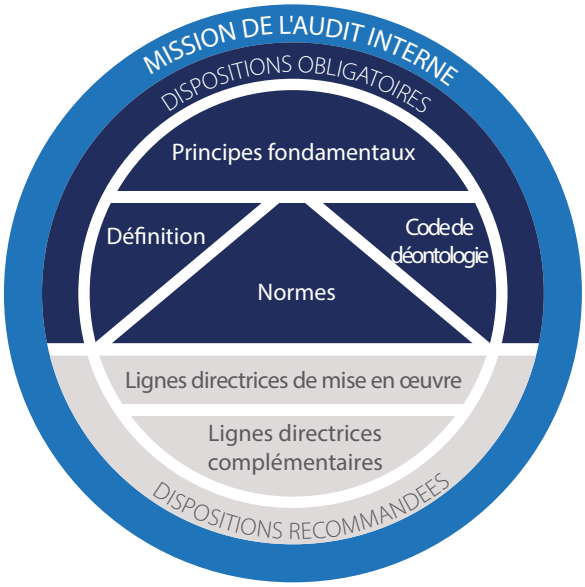
À propos du CRIPP

Le Cadre de Référence International des Pratiques Professionnelles de l'audit interne® (CRIPP®) comprend les lignes directrices approuvées par l'Institute of Internal Auditors. Instance internationale de normalisation, l'IIA fournit aux professionnels de l'audit interne du monde entier des orientations qui font autorité. Elles figurent dans les dispositions obligatoires ou recommandées du CRIPP.

Les dispositions obligatoires sont élaborées selon un processus de diligence raisonnable qui inclut une consultation publique pour la prise en compte des avis des parties prenantes. Les dispositions obligatoires du CRIPP comprennent :

- les Principes fondamentaux pour la pratique professionnelle de l'audit interne ;
- la Définition de l'audit interne ;
- le Code de déontologie ;
- les *Normes internationales pour la pratique professionnelle de l'audit interne.*

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



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. Elles viennent appuyer les Normes tout en offrant des orientations additionnelles sur des domaines spécifiques, comme des problématiques propres au secteur d'activité, les procédures y étant bien plus détaillées que dans les Normes ou les guides de mise en œuvre. Les lignes directrices complémentaires sont homologuées par l'IIA *(the Institute of Internal Auditors)* à l'issue d'un processus formalisé de revue et d'approbation.

Guides pratiques

Les guides pratiques constituent un type de lignes directrices complémentaires qui offrent des approches séquentielles, intégrant des processus, des procédures, des outils et des programmes, ainsi que des exemples de livrables.

Ils sont destinés à aider les auditeurs internes. Il existe aussi des guides pratiques ciblant :

- les établissements financiers ;
- le secteur public ;
- les systèmes d'information (GTAG® pour *Global Technology Audit Guide*).

Pour de plus amples informations sur les documents de référence proposés par l'IIA, vous pouvez consulter le site web www.globaliia.org/standards-guidance.

Table des matières

Synthèse 4

Introduction 5

- La menace interne : un aperçu 6
- Anatomie d'une menace interne 8
  - Source ou acteur de la menace 8
  - Cible 9
  - Motivations 9
  - Conséquences 10
- Le rôle de la fonction d'audit interne dans la gestion des menaces internes 10

Planifier les missions d'évaluation des programmes relatifs aux menaces internes 13

- Comprendre le contexte et l'objectif de la mission 13
- Comprendre le processus ou le domaine audité 14
  - Gestion de la menace interne 14
  - Élaborer un programme relatif aux menaces internes 14
  - Informations nécessaires à la planification de la mission 18
- Réaliser une évaluation préliminaire des risques 21
- Définir les objectifs de la mission 22
  - Exemples d'objectifs de mission 22
- Établir le périmètre d'intervention de la mission 22
  - Exemples de périmètre d'intervention de la mission 23
- Allocation des ressources 23
- Préparer le programme de travail de la mission 23
- Donner une assurance au Conseil 29

Annexe A. Normes et lignes directrices de l'IIA applicables 31

Annexe B. Glossaire 32

Annexe C. Évaluation de la menace interne à l'aide du référentiel cybersécurité du NIST 34

Annexe D. Bonnes pratiques du CERT pour minimiser les menaces internes 42

Annexe E. Organisations et agences émettrices de recommandations 43

Annexe F. Références et ressources complémentaires 46

Remerciements 48

Synthèse

À l'ère du numérique, les organisations devraient traiter les données de la même manière qu'elles traitent les liquidités : comme un actif qui doit être protégé des menaces, aussi bien internes qu'externes. La protection des actifs numériques de l'organisation contre des fuites de données qui peuvent se révéler désastreuses ne devrait plus être considérée comme relevant uniquement de l'autorité de la direction des systèmes d'information (SI). L'ultime responsabilité de la gestion des risques, à des niveaux qui permettent à l'organisation d'atteindre ses objectifs, incombe à la direction générale et au Conseil.

Qu'elles se révèlent malveillantes ou involontaires, les menaces internes n'attirent que rarement l'attention qu'elles méritent compte tenu du caractère significatif des risques auxquels elles exposent l'organisation. Les principaux risques associés aux menaces internes comprennent le sabotage, le vol de données, l'espionnage, la fraude et les actes criminels. De plus, les recherches tendent à indiquer que le panorama des menaces internes s'étend à mesure que les organisations deviennent plus dépendantes des SI, des processus automatisés, des applications en ligne, des données transmises par voie numérique et des espaces de stockage dématérialisés (*cloud* ou « informatique dans les nuages »).

Les organisations commencent à prendre conscience que l'investissement dans les technologies ne constitue qu'une partie de la solution ; il est tout aussi important d'évaluer si la gouvernance et la gestion de leurs dispositifs de contrôle (tels que les politiques SI, la formation et les campagnes de sensibilisation) sont capables de répondre aux menaces internes.

Les auditeurs internes sont bien positionnés pour aider :

- la direction générale et le Conseil à reconnaître l'importance de la mise en œuvre ou du renforcement d'un programme relatif à des menaces internes et,
- les organisations à améliorer leurs processus de gouvernance, de management des risques et de contrôle.

Introduction

La menace interne est définie comme la possibilité pour toute entité disposant d'un droit d'accès (c'est-à-dire au sein d'un espace sécurisé) de nuire à un système d'information ou à une entreprise par la destruction, la divulgation ou la modification de données, et/ou par déni de service.[1] Cette définition est large et comprend aussi bien les attaques malveillantes que les attaques involontaires contre les actifs de l'organisation, y compris contre son capital humain.

Note : Les termes en caractères gras sont définis dans le glossaire figurant à l'Annexe B. Ce guide contient un certain nombre de termes techniques dont les lecteurs maîtrisant la terminologie de la sécurité de l'information sont familiers. Si la définition recherchée ne figure pas dans le glossaire, veuillez consulter les références et les ressources complémentaires figurant à l'Annexe F.

A la différence d'une menace externe (c'est-à-dire venant d'une entité ne disposant pas d'un droit d'accès aux systèmes de l'organisation), les profils autorisés, tels que les salariés travaillant ou ayant travaillé dans l'entreprise, les prestataires et les partenaires possèdent déjà un certain niveau de connaissance et/ou un accès aux systèmes et aux données d'une organisation. Par conséquent, il est beaucoup plus facile pour ces individus de contourner plusieurs mesures de sécurité et d'abuser de ces droits d'accès afin de consulter, copier, télécharger, corrompre, supprimer ou transmettre des données sensibles en dehors du réseau de l'organisation.

Les **risques** liés aux menaces internes peuvent inclure :

- la fraude
- le sabotage
- le vol de propriété intellectuelle ou de secrets d'affaires
- la divulgation de données sensibles
- l'utilisation de ressources SI pour des activités illégales

En prenant conscience des menaces internes et des risques qui leur sont associés, et en s'informant sur les programmes les concernant, les auditeurs internes disposent d'une excellente occasion d'apporter une valeur ajoutée en aidant l'organisation à renforcer sa **gouvernance**, son management des risques et ses **processus de contrôle** afin de mieux gérer ces menaces.

Ce guide pratique d'audit des systèmes d'information (GTAG – *Global Technology Audit Guide*) vise à accompagner les auditeurs dans la compréhension des menaces internes en fournissant une vue d'ensemble de ces menaces, des principaux risques associés et de leurs impacts potentiels. De plus, ce guide présente des exemples de référentiels de sécurité généralement reconnus et admis, notamment ceux de l'université Carnegie Mellon *(Carnegie Mellon University Software Engineering Institute)*, du NIST *(National Institute of Standards and Technology)* et de l'INSA *(Intelligence and National Security Alliance)*, de dispositifs de contrôle et d'autres ressources pouvant contribuer à la planification et à la réalisation des missions d'audit. Les organisations devraient choisir leur référentiel en fonction de leur situation spécifique, en tenant compte de facteurs tels que leur secteur d'activité, leur taille, leur complexité et le caractère applicable du cadre choisi. Pour les orga-

[1] Committee on National Security Systems, *CNSS Instruction N° 4009*, Washington DC : National Security Agency, 26 avril 2010, p. 38 : https://www.hsdl.org/?view&did=7447.

nisations disposant déjà de programmes relatifs aux menaces internes, les auditeurs peuvent utiliser ces lignes directrices pour concevoir des missions d'assurance afin d'évaluer leur efficacité.

Le guide décrit également des approches que les auditeurs internes peuvent adopter dans des missions de conseil pour aider le management à identifier et à évaluer les risques qui devraient être pris en considération lors de la conception et de la mise en œuvre d'un nouveau programme concernant les menaces internes, ou pour tester et améliorer un programme existant. Enfin, le GTAG fournit des recommandations relatives à la manière de communiquer au **Conseil** l'importance de ces risques et la nécessité d'intervenir pour identifier, prévenir et détecter les **incidents liés à la sécurité des SI** causés par des menaces internes, y répondre et les surmonter.

Impact opérationnel

Les dommages causés par une menace interne peuvent se chiffrer en millions. Ces dernières années, trois collaborateurs d'une entreprise de fabrication de supraconducteurs ont volé des secrets d'affaires et les ont vendus à un concurrent pendant six ans. Bien que le coût estimé de ces secrets se soit élevé à 800 millions de dollars, la perte de valeur pour les actionnaires a presque atteint 1 milliard.[2]

La menace interne : un aperçu

Le terme menace peut être utilisé pour se référer aussi bien à l'auteur qu'à l'attaque en elle-même. C'est la raison pour laquelle il est important de définir les termes clés qui seront utilisés tout au long de ce guide :

Impact désigne le résultat ou l'effet, positif ou négatif, des risques.

Menace désigne toute circonstance ou événement pouvant avoir un impact négatif sur les opérations d'une organisation, sur ses actifs, sur les individus ou sur d'autres organisations.

Acteur de la menace désigne l'entité responsable de l'action (ou de l'inaction) ayant porté préjudice à l'organisation.

Source de la menace qualifie l'intention et la méthode visant à exploiter délibérément une vulnérabilité ou une situation et une méthode pouvant accidentellement exploiter une vulnérabilité.

Risque désigne la possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

Vulnérabilité qualifie une faiblesse dans un système d'information, des procédures du système de sécurité, des dispositifs de contrôle interne ou leur mise en œuvre qui pourrait être exploitée par une source de menace.

Les menaces internes peuvent être *malveillantes* lorsque l'utilisateur fait intentionnellement un usage abusif de son accès au réseau, au système ou aux données d'une organisation afin de nuire à la confidentialité, à l'intégrité ou à la disponibilité de ses informations ou de ses systèmes d'information. Toutefois, les menaces internes peuvent aussi être *involontaires* (non intentionnelles) lorsque l'acteur, par ses actions ou son inac-

[2] Christopher Burgess, « Sinovel Wind Group found guilty of IP theft, fined $1.5 million » , CSO magazine, 9 juillet 2018, https://www.csoonline.com/article/3256305/loss-prevention/sinovel-wind-group-found-guilty-of-ip-theft-valued-at-800-million.html

tion, sans intention malveillante, cause des dommages ou augmente considérablement la probabilité que l'organisation subisse un préjudice ultérieur quant à la confidentialité, à l'intégrité ou à la disponibilité de ses informations ou de ses systèmes d'information, comme décrit dans la **Figure n°1**.

Figure n°1 : Exemples de menaces internes

Malveillante	Sans intention malveillante
Un collaborateur vole des informations liées au secret des affaires puis les vend à un concurrent.[3]	Un administrateur système coupe accidentellement l'accès à un site Web.
Un ancien collaborateur endommage le réseau informatique de son ancien employeur.[4]	Un utilisateur supprime accidentellement des fichiers.
Un consultant utilise la carte de crédit de l'organisation pour commettre une **fraude**.	Un collaborateur est victime **d'ingénierie sociale** ou de hameçonnage *(phishing)*.

Une *collusion* a lieu lorsque :

- plusieurs acteurs œuvrent de concert pour commettre une attaque contre une organisation ;
- des profils autorisés sont visés par des personnes malveillantes extérieures à l'organisation (cybercriminels, pirates et hacktivistes), entraînant une collaboration involontaire ;
- des profils autorisés sont visés par des personnes malveillantes extérieures à l'organisation, entraînant une collaboration délibérée (souvent dans un but lucratif).

La collusion accroit le périmètre de l'attaque et augmente la probabilité d'une attaque réussie difficile à détecter. Pour les petites et moyennes entreprises, qui ne disposent généralement pas des ressources nécessaires pour surmonter de telles attaques, les impacts peuvent être particulièrement dévastateurs. Limiter les menaces peut se révéler très coûteux, mais la prévention ou la détection des attaques sont des investissements rentables sur le long terme comparés aux coûts associés à une reprise après un incident majeur de sécurité lié aux SI.

Le coût moyen du traitement des dommages liés aux menaces internes augmente considérablement en tenant compte des fuites de données résultant d'actes involontaires. De plus, il faut s'attendre à ce que ce coût continue à augmenter à mesure que les pirates malveillants deviennent plus efficaces dans leur manière de cibler des profils autorisés qui ne se doutent de rien.

Les actes involontaires pouvant entraîner une fuite de données sont notamment :

La divulgation accidentelle : un profil autorisé publie ou traite à mauvais escient, involontairement ou par erreur, des informations sensibles, ou se trompe de destinataire en les envoyant par mél, fax, courrier postal ou via un réseau social.

---

[3] Kacy Zurkus, « Former Apple Employee Charged with Data Theft », *InfoSecurity Magazine*, 11 juillet 2018, https://www.infosecurity-magazine.com/news/apple-filed-criminal-complaint-of/.

[4] « Former Employee of Transcontinental Railroad Company Found Guilty of Damaging Ex-Employer's Computer Network », ministère américain de la Justice, 10 octobre 2017, https://www.justice.gov/usao-mn/pr/former-employee-transcontinental-railroad-company-found-guilty-damaging-ex-employer-s.

L'ingénierie sociale/hameçonnage : une personne extérieure à l'organisation obtient un accès électronique grâce à une méthode d'ingénierie sociale (comme une attaque par hameçonnage, ou via une clé USB non autorisée ou contenant un virus) afin d'obtenir les identifiants d'un profil autorisé ou d'utiliser un programme malveillant dans le but d'obtenir cet accès.

L'accès non autorisé à des documents physiques : un utilisateur non autorisé ou malveillant accède à des documents non électroniques perdus, jetés ou volés, tels que des documents papier.

L'accès non autorisé à du matériel portable : un utilisateur non autorisé ou malveillant accède à des périphériques de stockage de données perdus, jetés ou volés, tels qu'un ordinateur portable, un smartphone, un périphérique de stockage, un CD, un disque dur ou une bande de données.

Coût des incidents liés à une menace interne sur une période de 12 mois

- Nombre total d'incidents : 3 269.
- Coût total moyen : 8,76 millions de dollars.
- Incidents liés à une négligence : 64 %.
- Incidents liés à une source criminelle abusant de ses autorisations : 23 %.
- Incidents liés au vol des identifiants d'un utilisateur : 13 %.

Source : Recherche : Ponemon Institute© et Sponsorship, « 2018 Cost of Insider Threats: Global » ObserveIT, avril 2018.

Anatomie d'une menace interne

Pour dresser le profil d'une menace interne, il est important de prendre en compte les multiples facteurs (dimensions) qui la composent, tels que les personnes représentant cette menace, les actifs qui peuvent être ciblés, les motivations de l'attaque et les conséquences potentielles pour l'organisation.

Source ou acteur de la menace

Les auteurs de menaces internes ne sont pas nécessairement des pirates ou des cybercriminels, ce qui rend leur identification difficile. Par définition, les profils autorisés désignent des individus ou des entités disposant ou ayant disposé d'un droit d'accès aux informations de l'organisation et aux systèmes d'information (physique ou logique). Parmi les acteurs d'une menace qui devraient être pris en considération lors de l'élaboration de profils de menace interne ou de scénarios de risque, on trouve :

- les collaborateurs actuels et les anciens employés ;
- les collaborateurs à temps plein et à temps partiel ;
- les collaborateurs temporaires et les prestataires ;
- les **partenaires** qui ont la confiance de l'organisation.

Bien qu'il soit difficile d'identifier les individus présentant le plus de risques de se livrer à des activités malveillantes, il peut se révéler utile de comprendre certaines de leurs caractéristiques afin de définir des comportements typiques d'acteurs d'une menace interne. La **Figure n°2** présente une liste élaborée par le *National Cybersecurity and Communications Integration Center* répertoriant certaines des caractéristiques qui devraient servir de signaux d'alerte. Notez que l'ordre de ces caractéristiques ne représente en rien leur importance ou leur probabilité.

Figure n°2 : Caractéristiques d'un profil autorisé pouvant devenir une menace

Introversion.	Volonté exacerbée d'éviter, de dissimuler ou de corriger des erreurs.
Cupidité/difficultés financières.	Incapacité à assumer la responsabilité de ses actes.
Vulnérabilité au chantage.	Intolérance à l'égard de la critique.
Comportement compulsif et destructeur.	Excessive estime de soi.
Attitudes rebelles, comportement passif-agressif.	Manque d'empathie.
« Souplesse » déontologique.	Frustration et déception.
Arrogance - narcissisme (égo/image de soi).	Antécédents de gestion inefficace de crises.

Source : National Cybersecurity and Communications Integration Center, « Combating the Insider Threat », page 1.

Cible

Les cibles incluent les actifs ou les biens de valeur qui peuvent être touchés par une menace avec un impact négatif sur l'organisation. Il s'agit notamment des :

- Personnes
- Informations
- Technologies
- Installations

Motivations

Les motivations d'une personne sans intention malveillante, à l'origine d'une menace interne, sont nombreuses et variées. Des soucis personnels aussi bien que des problèmes avec des collègues et la direction, ou encore une simple opportunité ou l'ennui peuvent mener un individu à ce type d'activité.

Les motivations des attaques malveillantes peuvent notamment inclure :

- L'appât du gain
- La fraude
- Le méfait
- La malveillance
- La revanche
- L'espionnage
- Le vol
- L'association avec des malfaiteurs

Exemples d'indicateurs de l'exploitation d'une vulnérabilité

- Téléchargements vers un espace de stockage sur le *cloud*.
- Utilisation d'un périphérique de stockage portable.
- Horaires inhabituels sans qu'une autorisation ait été accordée.
- Courriels envoyés à des personnes externes ou vers un compte personnel.
- Impression ou copie excessive de documents propriétés de l'organisation ou classifiés.
- Demande d'accès à des zones ou systèmes précédemment refusés.

Conséquences

Les conséquences de l'exploitation d'une vulnérabilité par un profil autorisé peuvent être classées selon le Cadre de référence du management des risques de l'entreprise (ERM - *Enterprise Risk Management Framework)* du COSO *(Committee of Sponsoring Organizations of the Treadway Commission)* en quatre catégories : finance, opérations, conformité et clients. Il est fréquent qu'une même attaque ait un impact sur plus d'une de ces catégories. Par exemple, le sabotage des systèmes d'information critiques peut avoir des conséquences financières (coût de restauration des systèmes), opérationnelles (perte de productivité), ainsi que sur la relation avec les clients (service de mauvaise qualité durant l'arrêt des systèmes).

Des profils de menace interne, comme illustré dans la **Figure n°3**, peuvent être établis en utilisant les facteurs mentionnés dans la section précédente.

Figure n°3 : Définition de profils de menace interne

	Profil 1	Profil 2
Menace	Sabotage des systèmes d'information	Vol de propriété intellectuelle
Acteur de la menace	Ancien collaborateur	Collaborateur actuel
Cible	Réseau informatique	Secret des affaires
Motivations	Malveillance (revanche)	Appât du gain
Conséquences	Interruption des opérations	Perte d'avantage concurrentiel

De plus, il est important que les organisations classent les risques potentiels liés aux menaces internes à l'aide de facteurs tels que la probabilité d'occurrence, la vélocité et la persistance afin d'établir un profil de risque reflétant l'**appétence** et la tolérance au risque de l'organisation.

Les risques devraient également être rapprochés de la typologie des acteurs potentiels pour définir des profils de risque inhérent selon les fonctions (par exemple les administrateurs système, les opérateurs du *help desk*, les prestataires) qui ont accès à des données considérées comme sensibles, cruciales ou confidentielles. Créer des profils de risque selon la fonction devrait permettre au management de mettre en place des dispositifs de contrôle moins coûteux pouvant contribuer à prévenir et à détecter les attaques, qu'elles soient délibérées ou non.

Le rôle de la fonction d'audit interne dans la gestion des menaces internes

L'**audit interne** utilise une approche systématique, méthodique et fondée sur les risques permettant de délivrer une assurance, des conseils et des points de vue objectifs. En ce qui concerne les menaces internes, la principale responsabilité incombant à l'audit interne est de fournir une assurance et des conseils qui aident l'organisation à atteindre ses objectifs en évaluant les processus de gouvernance, de management des risques et de contrôle, et en contribuant à leur amélioration, comme décrit dans la Norme 2100 - Nature du travail.

Les missions d'assurance ont pour objectif d'évaluer l'efficacité des dispositifs de contrôle et peuvent mettre en évidence des opportunités d'amélioration. Elles peuvent également permettre à la direction générale et au Conseil de mieux comprendre les risques et la nécessité d'intervenir. Par ailleurs, les missions de conseil peuvent aider l'organisation à développer ou améliorer un programme relatif aux menaces internes (par exemple, dès les phases amont de ce programme), ou peuvent être utilisées pour évaluer la pertinence du programme (par exemple, en effectuant une étude comparative).

Missions de conseil

La Norme 2010.C1 stipule que, lorsqu'on lui propose une mission de conseil, le **responsable de l'audit interne**, avant de l'accepter, devrait considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée, d'améliorer le management des risques et le fonctionnement de l'organisation.

Les missions de conseil peuvent s'avérer utiles lorsque les personnes en charge de la gestion opérationnelle des systèmes d'information ne peuvent consacrer suffisamment de temps et de ressources pour évaluer les risques liés aux menaces internes et identifier les dispositifs de contrôle nécessaires. Les auditeurs internes peuvent apporter un appui aux collaborateurs chargés de l'administration des systèmes et des réseaux en évaluant les risques en matière de menaces internes et en identifiant les problématiques à côté desquelles les administrateurs de sécurité ont pu passer ou les domaines dans lesquels les politiques ne sont pas correctement appliquées. Dans ce rôle de conseil, les auditeurs internes peuvent faire des recommandations pour combler ces lacunes et apporter des perspectives et des connaissances objectives.

Indépendamment du type de mission, les auditeurs internes doivent évaluer et formuler des recommandations appropriées en vue d'améliorer les processus de gouvernance (Norme 2110 - Gouvernance). Bien souvent, les organisations possèdent des dispositifs de contrôle des systèmes d'information, mais aucun cadre de gouvernance n'a été formalisé afin de diriger, gérer et piloter les activités essentielles à la réussite de leurs opérations. Un exemple de ce cas de figure est l'absence de règles ou de procédures cohérentes concernant l'attribution et la gestion des accès utilisateur. Dans ce scénario, des privilèges injustifiés peuvent être octroyés et ainsi augmenter les risques qu'une menace interne survienne en dépit de l'existence de dispositifs de contrôle permettant de gérer les accès utilisateur.

Gouvernance des SI

Pour de plus amples informations concernant la gouvernance des systèmes d'information, référez-vous au GTAG de l'IIA, « Auditer la gouvernance des SI ».

Les risques devraient être évalués et les programmes relatifs aux menaces internes réévalués au moins une fois par an ou lors de changements majeurs dans la technologie ou les pratiques opérationnelles. Selon la taille de l'organisation et la complexité de l'environnement SI, l'évaluation d'un programme à l'échelle de l'entité peut se révéler difficile à mener. Il peut donc être préférable d'effectuer plusieurs missions afin d'évaluer les différentes composantes de ce programme (par exemple, la gouvernance, la sécurité des données, la sécurité physique, ou les pratiques de recrutement) ou de les intégrer dans les missions d'audit interne portant sur des actifs numériques sensibles. Par exemple, les auditeurs internes peuvent déterminer si les fonctions de surveillance de la sécurité disposent des mécanismes nécessaires de détection des anomalies internes pouvant indiquer que des identifiants ont été compromis ou que des profils autorisés abusent de leurs privilèges. Si l'organisation a déjà mis en place des dispositifs permettant de surveiller l'environnement

interne et externe, les auditeurs internes peuvent en évaluer l'efficacité et l'efficience, et contribuer à promouvoir leur amélioration continue (Normes 2120 - Management des risques et 2130 - Contrôle).

Le responsable de l'audit interne doit déterminer si la fonction possède collectivement les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de ses missions (Norme 1210 - Compétence). En ce qui concerne les missions d'assurance, les auditeurs internes doivent posséder des connaissances suffisantes des principaux risques et contrôles relatifs aux systèmes d'information. Toutefois, ils ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique (Norme 1210.A3). Selon la Norme 1210.A1, si la fonction d'audit interne ne possède pas les compétences nécessaires lui permettant de s'acquitter d'une mission d'assurance relative aux menaces internes, le responsable d'audit doit alors obtenir l'avis et l'assistance de personnes qualifiées. Les auditeurs internes devraient collaborer avec les personnes en charge de la gestion opérationnelle des SI et de la sécurité de l'information afin de tirer parti de l'expertise technique requise pour assurer une évaluation approfondie des menaces internes. De plus, le responsable de l'audit interne devrait coordonner les activités et partager des informations avec ces fonctions afin de tirer profit de leurs compétences, d'assurer une couverture adéquate et de minimiser les doubles emplois, comme décrit dans la Norme 2050 - Coordination et utilisation d'autres travaux.

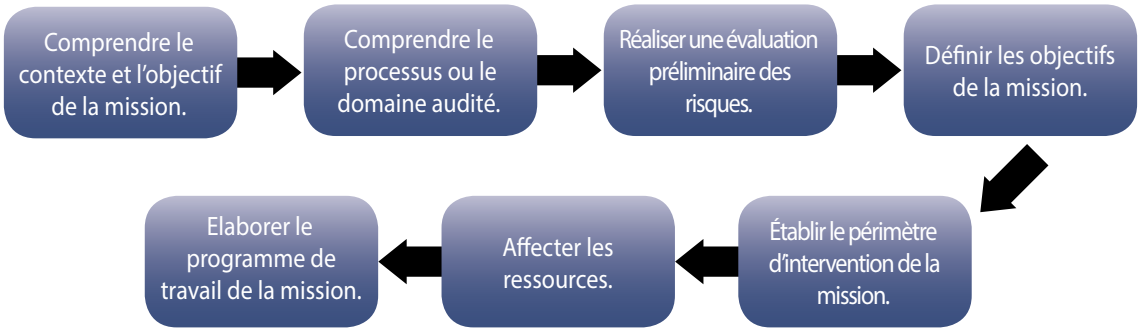
Planifier les missions d'évaluation des programmes relatifs aux menaces internes

La Norme 2200 - Planification de la mission stipule que les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. La Norme 2201 - Considérations relatives à la planification précise que les auditeurs internes doivent prendre en compte :

- la stratégie, les objectifs de l'activité auditée et la manière dont elle pilote sa performance ;
- les risques significatifs liés aux objectifs de l'activité, à ses ressources et à ses opérations, ainsi que les moyens par lesquels l'impact potentiel des risques est maintenu à un niveau acceptable ;
- la pertinence et l'efficacité des processus de gouvernance, de management des risques et de contrôle de l'activité, en référence à un cadre ou un modèle approprié ;
- les opportunités d'améliorer de manière significative les processus de gouvernance, de management des risques et de contrôle de l'activité.

Comme l'illustre la **Figure n°4**, la planification de la mission est généralement constituée de plusieurs étapes aidant les auditeurs internes à comprendre le domaine ou le processus audité et à documenter le plan de mission ainsi que le programme de travail. La revue et la documentation des informations étant un processus continu, il se peut que les étapes ne soient pas totalement distinctes et séquentielles.

Figure n°4 : Étapes de planification de la mission d'audit interne



Note : Plusieurs des étapes mentionnées dans la Figure n°4 ont été détaillées dans d'autres guides pratiques publiés par l'IIA (voir l'Annexe A).

Comprendre le contexte et l'objectif de la mission

Il s'agit d'une étape nécessaire pour s'assurer que les buts et objectifs fixés dans le plan annuel d'audit sont atteints et que les attentes des parties prenantes sont prises en compte dans le plan de mission. Dans le cadre de missions ponctuelles ou effectuées à la demande de la direction générale ou du Conseil, ou encore à la suite d'un changement important dans les activités ou dans l'environnement technologique, cette phase est également essentielle pour s'assurer que les auditeurs internes comprennent entièrement les besoins. Par exemple, après une fusion ou une acquisition, la direction générale peut avoir besoin d'évaluer si des risques ont pu être introduits dans l'environnement et s'ils sont couverts par le programme existant en matière de menaces internes.

Comprendre le processus ou le domaine audité

Lorsqu'il planifie une mission d'évaluation de l'efficacité de la gestion des risques liés aux menaces internes, l'auditeur doit précisément comprendre deux domaines critiques. Il devrait tout d'abord saisir la nature des menaces internes ainsi que les pratiques qui peuvent être mises en œuvre afin d'identifier, prévenir et détecter les incidents liés à la sécurité des SI, y répondre et les surmonter. Pour améliorer leurs connaissances, les auditeurs internes peuvent envisager d'utiliser des référentiels, programmes et recommandations. L'Annexe E est une liste de ressources et d'agences qui fournissent des conseils et une aide en matière de sécurité de l'information ; l'Annexe F propose des ressources supplémentaires. Les auditeurs internes peuvent s'appuyer sur ces informations au début de leur mission, mais ils devraient par la suite identifier les cadres de référence et recommandations spécifiques au secteur d'activité, au marché et aux zones géographiques dans lesquels opère leur organisation.

Risque de fraude

Parce que les fraudes font partie des principaux risques liés à des menaces internes, il est important d'obtenir des informations concernant toute allégation, occurrence ou enquête à ce sujet.

Pour des informations détaillées sur la manière d'intégrer les risques de fraude lors de la planification de la mission, référez-vous au Guide pratique de l'IIA, « Planification de la mission : l'évaluation des risques de fraude ».

Ils devraient également comprendre l'organisation ainsi que ses objectifs. La compréhension des objectifs opérationnels est fondamentale dans l'identification des risques à inclure dans l'évaluation préliminaire des risques au niveau de la mission (comme l'exige la Norme 2210.A1).

Gestion de la menace interne

Les menaces internes ne peuvent pas être totalement éradiquées, mais elles peuvent être gérées de manière à prévenir et diminuer leur impact si elles se matérialisent. Un programme relatif aux menaces internes est un ensemble de règles, procédures et dispositifs de contrôle permettant d'identifier, de prévenir et de détecter un incident lié à la sécurité des SI, d'y répondre et de le surmonter.

L'objectif principal de la mise en œuvre d'un tel programme est de protéger les actifs critiques, qui peuvent être physiques et logiques, y compris les personnes, les installations, les systèmes et les informations. Il peut se révéler coûteux et décourageant de tenter de protéger tout ce que l'organisation considère comme un actif, il est donc important de débuter ce processus en identifiant et en répertoriant les actifs critiques.

Élaborer un programme relatif aux menaces internes

Pour améliorer les chances de succès du programme, l'organisation devra formaliser le programme et gérer son élaboration et sa mise en œuvre d'une manière systématique (comme pour tout autre projet) en décrivant clairement les attentes, les rôles, les responsabilités ainsi que le calendrier et les activités. Un plan d'action ou une feuille de route, permettra de présenter la situation actuelle (analyse des écarts) ainsi que les ressources

Intégrer le facteur humain

Un programme relatif aux menaces internes efficace prend en compte les contrôles automatisés ou manuels. De solides programmes de gouvernance des SI et ERM (management des risques à l'échelle de l'organisation) peuvent servir de fondement à la gestion et à la maîtrise du facteur humain.

nécessaires (notamment les effectifs, le budget, le temps et les technologies) pour mener à bien le projet. Une des clés du succès de la gestion d'une menace interne réside dans la collaboration des fonctions assurant la surveillance (en particulier, la direction générale et le Conseil) et de celles responsables de la mise en œuvre du programme (par exemple, les responsables des ressources humaines, des services juridiques, des opérations, de la sécurité de l'information, de l'ingénierie logiciel, et les propriétaires de données).

Plutôt que de repartir d'une feuille blanche, les organisations peuvent tirer parti des référentiels de gestion des menaces internes développés par des entités privées, publiques et à but non lucratif, et les personnaliser pour qu'ils répondent à leurs besoins spécifiques. Ce faisant, l'organisation pourra accélérer le développement et la mise en œuvre de son propre programme.

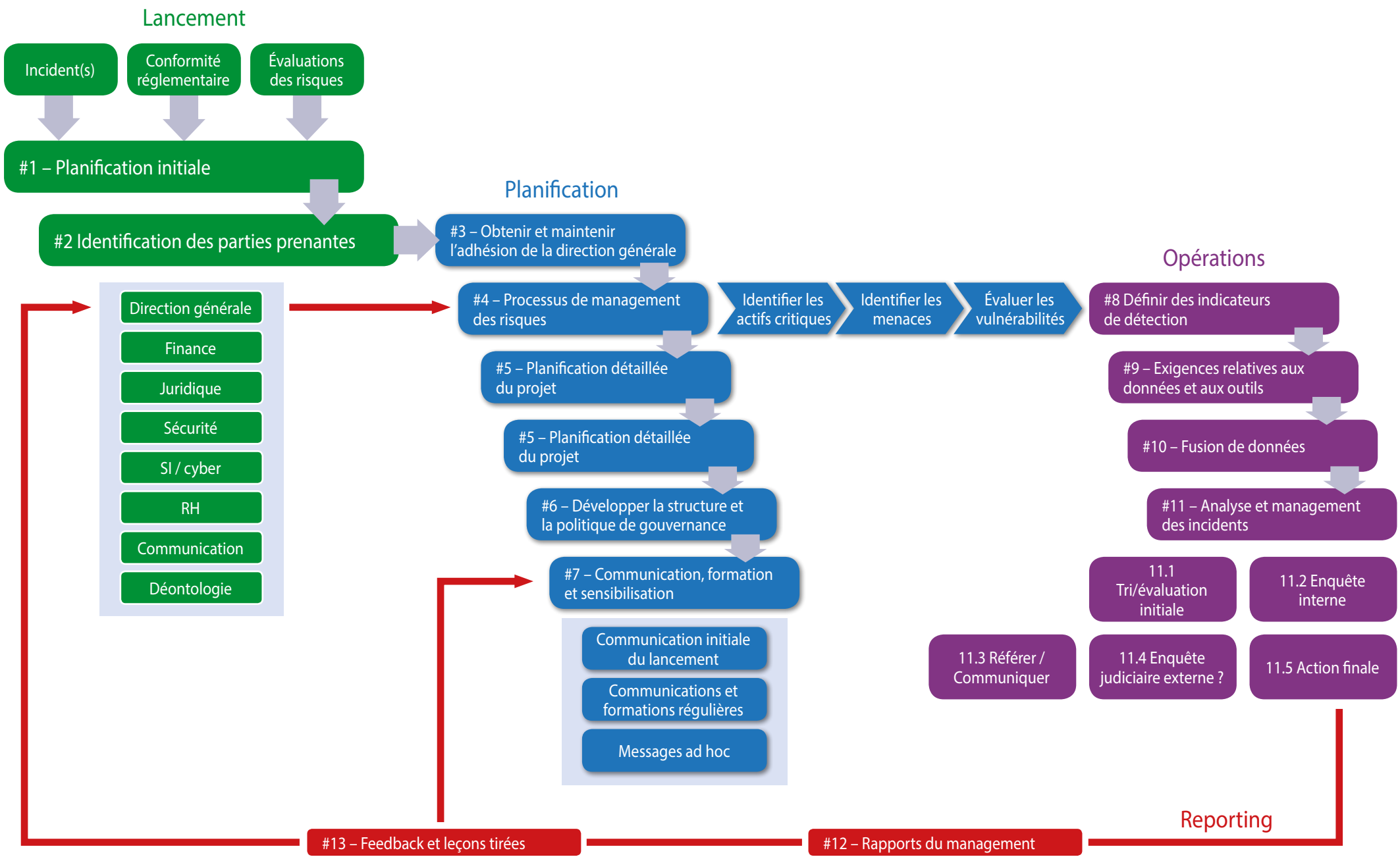
Voici quelques exemples de référentiels qui peuvent être utilisés pour développer un programme relatif aux menaces internes :

- Le référentiel du NIST *(National Institute of Standards and Technology)* « Framework for Improving Critical Infrastructure Cybersecurity », repris en Annexe C, décrit un ensemble d'activités permettant d'identifier, de prévenir et de détecter des cyberattaques, d'y répondre et de les surmonter. Le principal objectif de ce référentiel est d'aider les organisations à gérer des programmes de cybersécurité, mais les activités mentionnées peuvent également s'appliquer à la gestion des menaces internes.
- Le guide de l'université Carnegie Mellon, « Common Sense Guide to Mitigating Insider Threats, Fifth Edition », disponible à l'Annexe D, décrit 20 pratiques recommandées qui peuvent aider les organisations à développer un programme visant à atténuer (identifier, détecter et traiter) les risques de menace interne.
- Le guide de l'INSA *(U.S. Intelligence and National Security Alliance)* « Identifying and Countering Insider Threats Study » fournit une feuille de route en 13 étapes (ou points clés) pour développer, mettre en œuvre et superviser un programme relatif aux menaces internes, comme l'illustre la **Figure n°5**.

Référentiels d'audit interne

Au cours de leurs missions d'assurance et de conseil, les auditeurs internes peuvent utiliser des référentiels similaires comme critères d'évaluation de l'efficacité du programme relatif aux menaces internes de leur organisation.

Figure n°5 : Feuille de route de l'INSA pour l'élaboration d'un programme relatif aux menaces internes



Source : INSA *(U.S. Intelligence and National Security Alliance)* en partenariat avec le DHS, le FBI et l'ODNI, « Insider Threat Program Roadmap », https://www.insaonline.org/insider-threat-roadmap/. Reproduit avec la permission du NIST (National Institute of Standards and Technology), ministère américain du Commerce. Non soumis aux droits d'auteur aux États-Unis.

Phase de lancement

Au cours de cette phase, l'organisation évalue les besoins en matière de gestion des menaces internes, définit le champ d'application du programme et identifie les principales parties prenantes. Voici quelques questions qui peuvent l'aider à cibler et à prioriser ses actifs critiques :

- Quels sont nos actifs critiques ?
- Connaissons-nous le statut de chacun de ces actifs critiques ?
- Comprenons-nous l'importance de chaque actif critique et pouvons-nous expliquer en quoi ils sont importants pour notre organisation ?
- Pouvons-nous prioriser ces actifs critiques ?
- Disposons-nous de l'autorité, du budget et des ressources nécessaires pour les surveiller efficacement ?

Phase de planification

La phase de planification commence habituellement avec l'obtention de l'adhésion de la direction générale et l'identification des actifs à protéger. Voici quelques-unes des mesures que l'organisation peut prendre pour la mener à bien :

- Identifier les systèmes et les actifs numériques.
- Identifier les exigences réglementaires.
- Effectuer une évaluation des risques.
- Établir un plan formel de déploiement du projet.
- Créer, le cas échéant, une structure et des politiques de gouvernance.
- Élaborer des plans de communication, de formation et de reporting.

Phase opérationnelle

Au cours de cette étape, l'organisation analyse les besoins et les écarts, et priorise les activités à mettre en place pour y répondre. Voici quelques-unes des activités habituellement effectuées durant cette phase :

- Effectuer une analyse coûts-bénéfices.
- Élaborer des profils de menace interne.
- Identifier/mettre en place les contrôles nécessaires pour faire face aux menaces internes (des exemples courants de dispositifs de contrôle de la sécurité des SI figurent dans la Figure n°6).
- Élaborer des indicateurs clés de performance.
- Formaliser les procédures de gestion des incidents liés à la sécurité des SI.

Figure n°6 : Dispositifs courants de contrôle de la sécurité des SI

Administratif	Physique	Technique
Règles et procédures. Politiques RH. Politiques de gestion des mots de passe. SLA *(Service level agreements* ou Accords de niveau de service). Sensibilisation et formation en matière de sécurité. Gestion du changement. Gestion des configurations. Gestion des *patchs* (correctifs). Procédures d'archivage, de sauvegarde et de récupération.	Dispositifs de lutte contre les incendies. Chauffage, ventilation et climatisation. Protection électromagnétique (EMI-*Electromagnetic interference*). Surveillance environnementale. Vidéosurveillance. Clôtures, portes et murs. Éclairage. Cartes d'accès. Gardiens. Serrures, tourniquets et sas de sécurité.	Cryptographie. Réseau virtuel privé (VPN). Zone démilitarisée. Pare-feu. Listes de contrôle d'accès. Serveurs proxy. Transcription d'adresses. Détection/prévention des intrusions (IDS/IPS). Leurres *(Honeypots).* Segmentation de réseau.

Source : CERT® du *Software Engineering Institute* de l'université Carnegie Mellon « Model-Driven Insider Threat Control Selection and Deployment ».

Phase de reporting

La surveillance et le reporting sont d'une grande importance pour s'assurer que l'organisation reste capable de faire face aux menaces internes à mesure que les environnements interne et externe changent. Dans le cadre d'une approche d'amélioration continue, il est possible de réitérer les étapes du plan de mise en œuvre autant de fois que nécessaire.

Informations nécessaires à la planification de la mission

Les activités que les auditeurs internes peuvent mener pour mieux comprendre le programme relatif aux menaces internes de l'organisation incluent notamment :

Les revues documentaires

Elles consistent à évaluer :

- les plans d'activité *(business plans)* actuels et les résultats de l'évaluation des risques ;
- les évaluations précédentes (internes et externes) ;
- les organigrammes pour identifier les parties prenantes concernées ;

Considérations juridiques

Des dispositifs de surveillance des collaborateurs sont essentiels pour la gestion des menaces internes, mais ils peuvent exposer l'organisation à des risques juridiques liés aux lois locales, fédérales et transfrontalières protégeant la vie privée. Le règlement général sur la protection des données (RGPD), qui vise à protéger la vie privée des résidents de l'Union européenne, en est un exemple.

Pour gérer ce type de risques juridiques, il est important de coordonner les activités avec les services juridiques et les RH afin de s'assurer que les droits individuels sont pris en compte dans les pratiques de surveillance.

- toute règle ou procédure liée à la gestion des utilisateurs, des accès, à l'administration des accès à distance (pour les fournisseurs par exemple), ainsi que les guides de configuration des systèmes ;
- les inventaires des biens et des données afin d'identifier les systèmes et données critiques de l'organisation ;
- les listes de contrôle d'accès et les restrictions de pare-feu qui limitent l'accès aux systèmes et aux données sensibles du réseau interne ;
- les lois et règlements applicables dans le contexte de la mission d'audit.

Les entretiens avec les parties prenantes concernées

Pour collecter des informations, les auditeurs internes peuvent interroger les collaborateurs en charge des tâches liées au programme relatif aux menaces internes, les membres du management responsables de la supervision et les personnes disposant de l'autorité nécessaire pour prendre des décisions. Vous trouverez dans la **Figure n°7** certaines des parties prenantes à prendre en compte.

Considérations relatives à la mission d'audit interne

La liste des 20 pratiques émise par le CERT *(Computer Emergency Response Team)* du *Software Engineering Institute* de l'université Carnegie Mellon, disponible en Annexe D, peut être utilisée durant la phase de planification de la mission pour élaborer les questionnaires de contrôle interne qui servent à recueillir les informations sur les activités de contrôle, ou pour définir des questions à poser aux parties prenantes lors des entretiens.

Figure n°7 : Parties prenantes du programme relatif aux menaces internes

Parties prenantes « métier »	Parties prenantes SI
Dirigeants	Responsables des SI (DSI, responsable des infrastructures informatiques)
Sécurité (physique, des personnes et de l'information)	Architectes de données (ou fonctions liées)
Ressources humaines	Architectes réseaux
Juridique/protection des données personnelles	Experts en prestations d'assurance relatives aux SI
Déontologie et conformité	Experts en sécurité des SI
Acquisition/sous-traitance/achats	Gestion opérationnelle des SI
Secteurs d'activité critiques (produits, services, propriétaires de données, partenaires le cas échéant)	Développement de logiciels
Relations publiques	Equipe de réaction aux incidents informatiques (CIRT-*Computer incident response team*)

Dans le cadre de ces entretiens, ou dans un autre contexte, les auditeurs internes peuvent mener des séances de *brainstorming* avec les parties prenantes afin d'identifier les risques inhérents. La liste qui en résultera pourra ensuite être intégrée à une évaluation des risques plus détaillée pour déterminer le risque résiduel et prioriser les menaces selon leur caractère significatif.

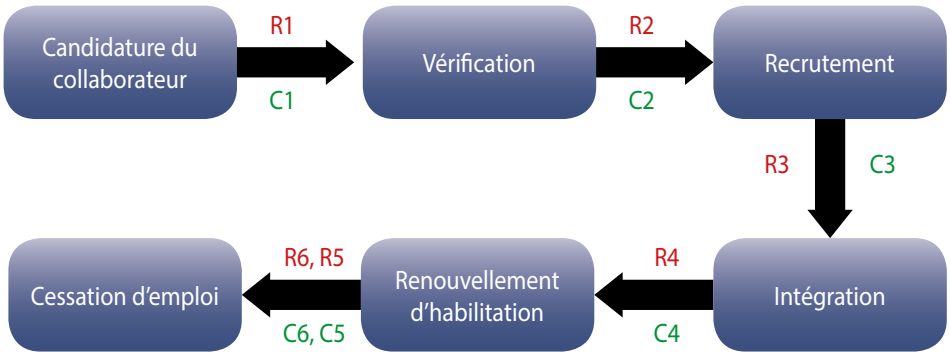
Anticiper les menaces

Le panorama des menaces se transforme rapidement. Les auditeurs internes devraient donc fréquemment vérifier les ressources mentionnées aux annexes C à E pour se tenir informés de toute mise à jour.

La cartographie des processus et sous-processus

Une des façons d'identifier les risques et les contrôles consiste à élaborer une cartographie des processus décrivant les données d'entrée, de sortie, les interfaces et les dispositifs de contrôle. Il peut se révéler difficile de cartographier l'intégralité d'un programme relatif aux menaces internes, mais les auditeurs peuvent se concentrer sur les processus présentant les risques les plus élevés. Pour mieux comprendre les risques et systèmes de contrôle clés, les auditeurs internes peuvent, par exemple, cartographier les processus RH, fournisseurs, fusions - acquisitions, gestion des identités et des contrôles d'accès ainsi que la classification et la priorisation des actifs. La **Figure n°8** fournit un exemple de cartographie d'un processus clé.

Figure n°8 : Exemple de cartographie d'un processus clé : le processus RH



Sous-processus	Risques	Contrôles
Candidature du collaborateur	R1 : Des collaborateurs ayant précédemment travaillé pour les principaux concurrents sont engagés, augmentant ainsi les risques de vol de propriété intellectuelle et de perte d'avantage compétitif.	C1 : Les antécédents sont évalués dans le cadre du processus de recrutement, et des contrôles supplémentaires sont effectués afin de déterminer si les candidats peuvent constituer une menace.
Vérification	R2 : Des collaborateurs ayant des antécédents judiciaires sont engagés, augmentant ainsi les risques de fraude.	C2 : Les antécédents judiciaires sont vérifiés dans les limites autorisées par les lois sur la protection de la vie privée.
Recrutement	R3 : Des collaborateurs ayant des intérêts dans d'importantes organisations concurrentes sont engagés à des postes traitant des données sensibles.	C3 : Les collaborateurs doivent déclarer tout conflit d'intérêts durant le processus de recrutement, et chaque année par la suite.
Intégration	R4 : Le processus d'intégration ne comprend pas de formation de sensibilisation aux menaces internes et aux protocoles permettant de faire face aux éventuels incidents touchant les SI.	C4 : Chaque collaborateur doit suivre une formation de sensibilisation dans le cadre du processus d'intégration. Les collaborateurs ne devraient se voir accorder l'accès au réseau qu'après avoir suivi une formation obligatoire.
Renouvellement habilitation	R5 : Les collaborateurs n'ont pas de nouvelles habilitations après avoir changé de fonction au sein de l'organisation, entraînant un accès injustifié aux systèmes.	C5 : Les accès sont a minima examinés tous les six mois et chaque fois qu'un collaborateur change de fonction. L'accès est automatiquement révoqué si le collaborateur n'est pas dûment habilité de nouveau.
Cessation d'emploi	R6 : Lors de la cessation d'emploi, l'organisation ne révoque pas immédiatement l'accès au réseau.	C1 : Les RH informent le service d'assistance immédiatement après la démission ou la cessation d'emploi d'un collaborateur. Le service d'assistance déclenche un processus de suppression d'accès à tous les systèmes concernés.

Réaliser une évaluation préliminaire des risques

En raison de contraintes de temps et de ressources, tous les risques ne peuvent pas être passés en revue pendant une mission. Par conséquent, les auditeurs internes sont tenus de réaliser une évaluation préliminaire des risques et de les prioriser en fonction de leur importance mesurée selon plusieurs facteurs de risque. La **Figure n°9** présente une évaluation des risques associés aux menaces internes les plus courantes.

Figure n°9 : Exemples de menaces internes et de risques associés

Menace	Risques	Impact potentiel
Fraude	Le fait pour un profil autorisé d'utiliser les systèmes d'information d'une organisation pour des ajouts, modifications, suppressions non approuvés de données afin d'en tirer un gain personnel ou de voler des informations pouvant mener à une usurpation d'identité.	Perte de confiance des actionnaires à la suite d'inexactitudes dans les informations financières. Atteinte à la réputation.
Sabotage des systèmes d'information	Le fait pour un profil autorisé d'utiliser les systèmes d'information pour porter un préjudice direct à une organisation ou un individu.	Arrêt du système et perte de productivité. Déni de service.
Vol de propriété intellectuelle	Le fait pour un profil autorisé d'utiliser les systèmes d'information d'une organisation pour voler la propriété intellectuelle de l'organisation. Cela comprend l'espionnage industriel impliquant des collaborateurs internes.	Perte d'avantage compétitif. Perte de revenus potentiels.
Vol ou divulgation de données critiques/ sensibles	Le fait pour un profil autorisé d'utiliser les systèmes d'information d'une organisation pour voler des données confidentielles, propriété de l'organisation ou personnelles, afin d'en tirer un bénéfice pécuniaire.	Perte de confiance des clients. Pertes financières dues aux dédommagements versés aux clients.
Vol de données personnelles	Le fait pour un profil autorisé d'utiliser les systèmes d'information d'une organisation pour voler ou divulguer des données personnelles.	Perte de confiance des clients. Pertes financières dues aux dédommagements versés aux clients. Pertes financières dues aux frais juridiques.
Activités illicites	Le fait pour un profil autorisé d'utiliser les actifs numériques d'une organisation pour en tirer un bénéfice pécuniaire (en envoyant des spams par exemple), effectuer des paris ou se livrer à d'autres activités pouvant ne pas être sanctionnées par la loi.	Atteinte à la réputation. Pertes financières dues aux frais juridiques.

Définir les objectifs de la mission

Les objectifs dépendent du contexte et du but de la mission. Pour les missions d'audit de conformité, ils découlent des exigences de conformité qui doivent être examinés. En ce qui concerne les missions d'assurance visant d'autres aspects, ils sont basés sur l'objectif initial de la mission et sur les résultats de l'évaluation des risques associés à ce domaine. Pour ce qui est des missions de conseil, les objectifs doivent répondre aux processus de gouvernance, de management des risques et de contrôle dans la limite convenue avec le client (Norme 2210.C1).

Supports à la planification de la mission

Pour des instructions détaillées sur l'élaboration des éléments mentionnés ci-dessous, référez-vous au Guide pratique de pratique de l'IIA : « Planification de la mission : Définir les objectifs et le périmètre d'intervention »

- Scénarios de risque
- Matrice des risques et des contrôles
- Cartes de priorisation des risques (ex : cartes des points critiques)

Exemples d'objectifs de mission

Mission d'assurance (conformité) : par exemple, une mission d'évaluation de la conformité au RGPD, qui exige la protection des données à caractère personnel. Dans cet exemple, les critères d'évaluation, requis par la Norme 2210.A3, sont les exigences et dispositifs de contrôle applicables en matière de protection de la vie privée définis par le RGPD.[5]

Mission d'assurance (au-delà de la conformité) : par exemple, une mission d'évaluation de l'efficacité du programme relatif aux menaces internes au regard du référentiel du NIST (« Improving Critical Infrastructure Cybersecurity »). Dans cet exemple, le critère de référence, requis par la Norme 2210.A3, serait le référentiel du NIST, présenté en Annexe C en tant que programme de travail de la mission.

Mission de conseil : par exemple, une mission d'évaluation de l'efficacité du processus d'identification et de classification des actifs numériques. Le cas échéant, la fonction d'audit interne formulera des recommandations quant à la manière d'améliorer le processus. Dans cet exemple, les critères d'évaluation, requis par la Norme 2210.A3, sont définis par la partie prenante ayant demandé la revue.

Établir le périmètre d'intervention de la mission

Le périmètre d'intervention de la mission fixe les bornes de la mission et précise ce qui sera inclus dans l'audit. Il définit des éléments comme les processus et/ou les domaines spécifiques, les lieux géographiques, les périodes (par exemple : une période déterminée, un trimestre fiscal ou une année civile) couverts par la mission, compte tenu des ressources disponibles.

Une fois les objectifs de la mission définis, l'auditeur interne doit établir un périmètre d'intervention suffisant pour atteindre ces objectifs (Norme 2220 - Périmètre d'intervention de la mission), en tenant compte des systèmes, des données, des personnes et des biens concernés, y compris ceux qui se trouvent sous le contrôle de tiers (Norme 2220.A1).

[5] Pour de plus amples renseignements concernant le RGPD, vous pouvez consulter le site https://gdpr-info.eu

Exemples de périmètre d'intervention de la mission

Les exemples de périmètre d'intervention de la mission ci-après ont été établis selon les objectifs indiqués dans la section précédente.

Mission d'assurance (conformité) : le périmètre d'intervention de cette mission comprendra typiquement toutes les installations, les systèmes et les processus traitant des données de résidents européens.

Mission d'assurance (au-delà de la conformité) : ce type de mission pourra couvrir la revue de la documentation concernant la conception du programme relatif aux menaces internes au niveau d'une entité. Cette évaluation pourra, par exemple, se faire au regard du référentiel du NIST *(« Improving Critical Infrastructure Cybersecurity »).*

Mission de conseil : le périmètre d'intervention de cette mission pourra correspondre au processus mis en œuvre pour identifier et classifier les actifs numériques dans le département informatique.

Allocation des ressources

Les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission (Norme 2230 - Ressources affectées à la mission). Pour ce faire, il convient de procéder à une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles. L'interprétation de la Norme 2230 clarifie ce que l'on entend par *appropriées*, c'est-à-dire la combinaison de connaissances, des savoir-faire et autres compétences nécessaires à la réalisation de la mission. On entend par *suffisantes*, la quantité de ressources nécessaires pour réaliser la mission avec conscience professionnelle.

> **Compétences de l'auditeur interne**
>
> Les compétences minimales d'un auditeur interne doivent comprendre la maîtrise des quatre composantes obligatoires du CRIPP : les Principes fondamentaux, la Définition de l'audit interne, le Code de déontologie et les *Normes internationales pour la pratique professionnelle de l'audit interne.*

La compétence la plus importante pour les auditeurs évaluant la gestion des menaces internes réside dans la connaissance de l'organisation et de ses objectifs stratégiques, des menaces, des risques, des vulnérabilités, et de leurs impacts potentiels sur la capacité de l'organisation à atteindre ses objectifs.

En raison de la technicité de certains des dispositifs de contrôle utilisés pour identifier, prévenir et détecter un incident lié aux SI, y répondre et le surmonter, il est parfois nécessaire d'avoir recours à des auditeurs internes qui maîtrisent les principes de la sécurité des SI. Si l'organisation ne dispose d'aucun auditeur ayant les compétences nécessaires, le responsable de l'audit interne peut faire appel à des ressources extérieures complémentaires ou à des collaborateurs internes des SI qui œuvreront en tant qu'experts permettant de récolter des informations sans compromettre la capacité de la mission d'audit interne de fournir une assurance objective.

Préparer le programme de travail de la mission

Le programme de travail de la mission est le fruit de la phase de planification. Pour les missions d'assurance, il devrait décrire les objectifs, le périmètre d'intervention, les risques, les contrôles et les procédures qui seront

utilisés pour identifier, analyser, évaluer et documenter les informations lors de la mission (Norme 2240 - Programme de travail de la mission et Norme 2240.A1). En ce qui concerne les missions de conseil, les programmes de travail peuvent varier, dans leur forme et leur contenu, selon la nature de la mission.

La liste ci-dessous **(Figure n°10)** comprend les activités et dispositifs de contrôle recommandés pour la mise en place d'un programme relatif aux menaces internes selon la feuille de route de l'INSA décrite dans la section « Élaborer un programme relatif aux menaces internes ». Ces activités et dispositifs ont été rapprochés des 20 pratiques du CERT (listées à l'Annexe D) et avec les définitions des différentes fonctions des dispositifs de contrôle, telles que présentées dans le référentiel cybersécurité du NIST (Annexe C).

Cette liste n'est pas exhaustive ; elle vise à démontrer l'utilité des multiples ressources disponibles dans la préparation d'un programme relatif aux menaces internes qui réponde aux besoins des organisations. Ces dernières devraient développer une feuille de route correspondant à leurs besoins spécifiques, en fonction de la taille, du secteur d'activité, de la réglementation, de la zone géographique et des autres facteurs entrant dans le cadre du traitement des risques liés à des menaces internes.

De plus, l'Annexe C présente une liste des dispositifs de contrôle et de leurs objectifs, basée sur le référentiel relatif à la cybersécurité du NIST. Accompagné des pratiques du CERT indiquées à l'Annexe D, ce référentiel peut être utile pour concevoir une évaluation des risques propre à une organisation donnée, déterminer les dispositifs de contrôle à mettre à l'épreuve, et identifier les procédures de test à utiliser pour évaluer leur efficacité. Pour les organisations déjà dotées de programmes relatifs aux menaces internes, ces ressources peuvent être utilisées pour évaluer le fonctionnement de ces programmes.

Figure n°10 : Activités et dispositifs de contrôle clés d'un programme relatif aux menaces internes

Phase de lancement		
Activité/dispositifs de contrôle	Pratique CERT	Fonction
Obtenir l'adhésion de la direction générale.	2	Identifier
Identifier les référentiels de menaces internes pouvant être utilisés comme points de repère.	2	Identifier
Évaluer le niveau actuel de la sécurité de l'information.	2	Identifier
Tirer parti des programmes qui traitent de la sécurité de l'information, de la sécurité de l'organisation et de la gouvernance des données pour identifier et comprendre les actifs critiques.	2	Identifier
Identifier les principales parties prenantes et établir des dispositifs de gouvernance.	2	Identifier

Phase de planification		
Activité/dispositifs de contrôle	**Pratique CERT**	**Fonction**
Évaluer et définir le périmètre du projet.	2	Identifier
Connaître et protéger les actifs critiques.	1	Identifier
Assurer l'intégration avec le management des risques à l'échelle de l'organisation.	2,6	Identifier
Développer des politiques, des procédures et des pratiques ayant l'assentiment des principales parties prenantes et prenant en compte la culture de l'organisation. Quelques exemples : ■ Politique d'utilisation acceptable ■ Code de conduite ■ Procédures RH de cessation d'emploi ■ Politique de non-respect ■ Politique de vigilance *(« See something; say something »)* ■ Procédures de signalement des activités suspectes ■ Procédures de résolution des incidents ■ Politique en matière de séparation des tâches ■ Définition des niveaux de gravité des incidents ■ Protocole de communication avec les forces de l'ordre	3	Identifier Protéger Répondre
Dès le recrutement, observer et réagir aux comportements suspects ou perturbateurs des collaborateurs.	4	Identifier Répondre
Coordonner avec les RH la mise en œuvre d'un processus de suivi couvrant les 30 jours précédant et suivant le départ de l'organisation d'un collaborateur clé détenant des informations concernant les actifs critiques de l'organisation. C'est durant cette période de 60 jours que les dommages les plus importants semblent survenir.	9	Protéger
Coordonner avec les RH l'élaboration d'un programme de formation pour sensibiliser aux menaces internes, aux risques qui y sont associés et à leurs impacts potentiels sur l'organisation.	9	Protéger
Collaborer avec les conseils juridiques, en amont et de manière régulière, afin de répondre aux exigences en matière de protection des données personnelles et de conformité dans le cadre des transferts internationaux de données.	4	Protéger
Anticiper et gérer, en coordination avec les RH et le service juridique, les problèmes pouvant affecter l'environnement de travail.	5	Identifier
Collaborer avec les parties prenantes pour développer un plan de communication.	2	Identifier Répondre Rétablir
Identifier les partenaires et les tiers ayant accès aux actifs numériques de l'organisation.	6	Identifier
Mettre en place des processus d'enquête et de résolution clairement définis pour s'assurer que les incidents sont traités selon un processus cohérent.	20	Identifier Protéger Répondre Rétablir
Vérifier régulièrement les profils des salariés et des prestataires, en particulier les collaborateurs occupant des postes à haut risque ou ayant accès à des actifs numériques critiques.	4,6	Protéger
Élaborer des processus reproductibles pour identifier, prévenir et détecter les menaces internes, ainsi que pour répondre aux incidents et les surmonter.	2	Identifier Protéger Détecter Répondre Rétablir
- Des processus de classification des actifs et des données ainsi que des processus de gouvernance sont mis en œuvre pour prioriser ces actifs jugés critiques/sensibles pour l'organisation. Ces actifs critiques devraient constituer une priorité absolue lors de l'application de dispositifs de contrôle des menaces internes.	1	Identifier

Phase de planification (suite)		
Activité/dispositifs de contrôle	**Pratique CERT**	**Fonction**
- La conformité aux réglementations étatiques, fédérales et transfrontalières sur la protection des données sensibles (comme l'HIPAA[6], la FERPA[7], le RGPD ou la norme PCI DSS[8]) devrait être prise en considération et mise en œuvre en conséquence. Ces réglementations nécessitent souvent des dispositifs de contrôle axés sur des accès limités au « privilège minimal » ou « sélectifs » *(need to know)*. Ce type d'évaluations ou de revues peut révéler des domaines dans lesquels l'acteur de la menace interne pourrait abuser de privilèges excessifs pour exposer des données auxquelles il n'a pas besoin d'avoir accès dans le cadre de sa mission.	2	Identifier Protéger Détecter
- Définir des accords de sécurité explicites pour les prestataires de service *cloud*, en particulier concernant les restrictions d'accès et les capacités de surveillance.	16	Protéger
- Un suivi du trafic sur le réseau interne, similaire à la surveillance du trafic externe entrant sur le réseau, devrait être mis en place. Les organisations déploient souvent des ressources de surveillance pour tenir compte des menaces externes, mais oublient de prendre le trafic interne en considération. Lorsque cela est associé à une segmentation incorrecte du réseau des systèmes critiques au niveau des stations de travail à usage général, les organisations risquent de passer à côté d'attaques internes utilisant le réseau.	12	Détecter
- Campagnes de sensibilisation permettant de faire savoir aux collaborateurs que l'organisation effectue une surveillance.	5,9	Protéger
- Campagnes de sensibilisation aux réseaux sociaux afin d'informer les collaborateurs sur les risques potentiels de divulgation.	7	Protéger
- Gestion des accès privilégiés (PAM - *Privileged Access Management*). Pour prévenir les menaces internes et se conformer à la réglementation, les organisations doivent surveiller et gérer les accès privilégiés de manière proactive. Le PAM peut aider à surveiller et à restreindre les comptes montrant des niveaux de privilège bien supérieurs aux autres utilisateurs. En règle générale, ce type de comptes est utilisé par les administrateurs système, les administrateurs de bases de données et les autres collaborateurs pouvant réaliser des tâches administratives et opérationnelles. Ces comptes pouvant être utilisés pour contourner certains dispositifs de contrôle, l'organisation doit mettre en œuvre des politiques, des procédures et des technologies afin de prévenir et de détecter tout usage abusif. L'objectif principal du PAM est de mettre en place une gestion automatisée des comptes et identifiants privilégiés, ainsi que des processus reproductibles afin d'assurer le suivi de l'ouverture et du retrait des droits des comptes critiques. Par exemple, il est possible de supprimer tous les accès aux systèmes de développement et de production, et d'accorder un accès limité dans le temps au moyen d'un processus de modification d'urgence qui implique d'ouvrir une session pour chaque activité.	10, 11, 12	Protéger
- Structurer le management et documenter les descriptions de postes afin de minimiser le stress et les erreurs involontaires.	8	Protéger
- La résolution des incidents est une approche méthodique permettant de répondre et de gérer les suites d'un incident de sécurité touchant les SI. Le plan de résolution des incidents (IRP - *Incident Response Plan*) est généralement un document contenant des instructions et des protocoles permettant de traiter les incidents touchant les SI ; une équipe de professionnels responsables de traiter, analyser et signaler ces incidents est souvent constituée (CSIRT - *Computer Security Incident Response Team*).	2	Répondre Rétablir

[6] HIPAA *(Health Insurance Portability and Accountability Act)* est une loi fédérale américaine qui définit des règles de confidentialité afin de protéger les dossiers médicaux des patients ainsi que tout autre renseignement fourni aux professionnels de santé.

[7] FERPA *(Family Educational Rights and Privacy Act)* est une loi fédérale américaine visant à protéger la confidentialité des dossiers scolaires des élèves.

[8] PCI DSS *(Payment Card Industry Data Security Standard)* du *PCI Security Standards Council* est une norme de sécurité internationale conçue pour protéger les données des détenteurs de cartes de paiement.

Phase opérationnelle		
Activité/dispositifs de contrôle	**Pratique CERT**	**Fonction**
Mettre en œuvre des dispositifs de contrôle physiques et logiques afin de se protéger, de détecter les incidents, d'y répondre et de les surmonter. Par exemple :		Protéger Détecter Répondre Rétablir
- Les contrôles physiques comprennent les systèmes de gestion de l'accès aux bâtiments et de vidéo-surveillance, qui peuvent être utilisés pour détecter les accès irréguliers ou non autorisés aux zones où l'information critique est accessible. Par exemple : ■ Prévention des incendies. ■ Chauffage, ventilation et climatisation. ■ Vidéosurveillance. ■ Cartes d'accès. ■ Serrures, tourniquets et sas de sécurité.	2	Protéger Détecter
- Gestion rigoureuse des dispositifs de contrôle des identités et des accès pour piloter l'accès aux applications, aux systèmes et aux données (copies papier ou numériques). Cette étape comprend l'octroi des droits aux utilisateurs (et leur annulation), la revue des accès utilisateurs en fonction des besoins métiers, l'examen et l'approbation des accès à distance (fournisseur ou salarié), les règles d'accès non partagé, ainsi que les contrôles à destination des utilisateurs internes, des fournisseurs et des tiers.	10, 11, 12, 15	Protéger
- Pare- feu situés en amont des systèmes critiques et configurés de manière à limiter aux seules personnes autorisées la connexion aux postes de travail.	13	Protéger Détecter
- La segmentation du réseau interne et le contrôle des restrictions relatives au réseau exigent une attention particulière. Les systèmes d'information hébergeant des données sensibles devraient avoir des accès restreints aux seules personnes justifiant d'un besoin métier. Cette segmentation pourra se manifester par des droits distincts pour le réseau local virtuel (VLAN - *Virtual Local Area Network*), des listes de contrôle des accès ou des paramétrages des pare-feu isolant ces systèmes ainsi que des dispositifs de sécurité physique pour protéger les serveurs de toute manipulation directe ou obstruction.	13	Protéger
- Segmentation du réseau externe et restrictions d'accès au réseau. Cette segmentation pourra inclure l'utilisation de zones démilitarisées (DMZ - *Dematerialized Zones*), de réseaux privés virtuels (VPN - *Virtual Private Network*), de leurres *(honeypots)* et de serveurs proxy afin de contrôler les interactions entre les environnements fiables et ceux qui ne le sont pas.	13	Protéger Détecter
- Les solutions logiciel SIEM *(Security Information and Event Management)* combinent la gestion des informations relatives à la sécurité du SI (SIM - *Security Information Management*) et celles des événements liés à la sécurité (SEM - *Security Event Management*) afin d'examiner rétroactivement et de consigner les actions spécifiques de chaque utilisateur sur un système, un ensemble de données ou l'activité globale sur le réseau (connexions partagées) et de créer des alertes. Ces registres devraient être examinés attentivement et les anomalies évaluées. En outre, ils devraient être suffisamment exhaustifs pour être utilisés en support des interventions post-incident.	13	Détecter Répondre
- Des programmes de surveillance de la sécurité complétés par des outils d'analyse de données tels que l'analyse du comportement des utilisateurs et des entités (UEBA - *User and Entity Behavior Analytics*) afin de déterminer les activités opérationnelles habituelles sur un système, un ensemble de données ou des ressources du réseau. Comprendre les tâches exécutées quotidiennement sur le réseau aidera les administrateurs à identifier les anomalies ou les comportements inhabituels qui peuvent être le signe d'une activité malveillante (signaux d'alerte).	12, 14	Détecter
- Des technologies d'alerte qui captent efficacement les changements, les ajouts ou les modifications touchant les ressources, les systèmes, les applications ou les dispositifs de contrôle de sécurité devraient être mises en place. Ces alertes devraient être adressées directement aux collaborateurs responsables du management de chaque technologie afin de distinguer rapidement les véritables menaces des faux positifs. Les systèmes de détection/prévention des intrusions (IDS/IPS) font partie de ce type de technologies.	17, 19	Détecter Répondre

Phase opérationnelle (suite)		
Activité/dispositifs de contrôle	**Pratique CERT**	**Fonction**
- Politiques et procédures d'escalade pour s'assurer que les alertes liées à des menaces plausibles sont communiquées aux groupes clés afin d'en minimiser l'impact. Par exemple, si une alerte est reçue d'un administrateur d'application indiquant qu'un nouveau compte utilisateur a été créé sans passer par le processus normal de vérification et d'approbation, cet élément devrait immédiatement être communiqué aux responsables, tels que les managers opérationnels, les propriétaires des données et les équipes de sécurité afin de prévenir un accès non autorisé aux droits plus étendus.	3	Répondre Rétablir
- Technologies de prévention des pertes de données mises en place en périphérie du réseau et dans les outils de messagerie électronique afin d'identifier tout envoi de données sensibles en dehors de l'organisation. En outre, une revue ou une évaluation des dispositifs de contrôle régissant l'accès au téléchargement de données depuis/vers tout prestataire de service *cloud* utilisé par l'organisation devrait également être conduite, ainsi qu'un examen de l'accès potentiel à ces services via un réseau public, tel qu'Internet. En effet, l'acteur de la menace interne pourrait tirer parti de cette activité légitime de l'organisation pour télécharger des données sensibles vers le *cloud*, et ensuite les récupérer dans un emplacement hors site non surveillé.	19	Protéger Détecter
- Les autres dispositifs de contrôle des technologies comprennent tous les mécanismes logiques et physiques utilisés pour prévenir, détecter les incidents touchant les SI et y répondre. Par exemple : ■ Gestion du changement. ■ Gestion des configurations. ■ Gestion des *patchs* (correctifs). ■ Procédures d'archivage, de sauvegarde et de récupération. ■ Tests de pénétration.	17, 18, 19	Protéger Détecter Rétablir
Utiliser l'analyse de données pour renforcer le programme.	12	Répondre
Mettre en œuvre le plan de réponse aux incidents.	12	Répondre Rétablir
Collecter des preuves et documenter les leçons tirées.	12	Identifier

Phase de reporting		
Activité/dispositifs de contrôle	**Pratique CERT**	**Fonction**
Évaluer régulièrement le programme et le mettre à jour si nécessaire. Ces domaines et indicateurs clés de performance sont généralement évalués sur une échelle de maturité afin de déterminer si l'organisation fait ce qu'il convient.	2	Rétablir
- Gouvernance, suivi et développement.	2	Rétablir
- Évaluations (risques de menace, tiers et actifs).	2	Rétablir
- Surveillance ■ Nombre d'anomalies étudiées. ■ Taux élevés ou croissants de données de sortie. ■ Nombre de faux positifs. ■ Nombre de faux négatifs. ■ Nombre de violations des règles de sécurité de la part du personnel SI.	2	Rétablir
- Protection des actifs.	2	Rétablir

Phase de reporting (suite)		
Activité/dispositifs de contrôle	Pratique CERT	Fonction
- Performance ■ Performance générale de l'équipe. ■ Taux de rotation des effectifs. ■ Gestion des ressources. ■ Auto-évaluations internes. ■ Évaluations externes. ■ Recommandations d'amélioration qui n'ont pas été mises en œuvre. ■ Collaborateurs faisant l'objet de plans d'amélioration de la performance. ■ Collaborateurs ou entités avec un nombre excessif de dossiers/plaintes RH.	2	Rétablir
- Gestion des incidents et des réponses ■ Type et nombre d'enquêtes menées au cours d'une période donnée. ■ Nombre d'enquêtes clôturées de manière satisfaisante. ■ Nombre d'enquêtes clôturées sur une période de 30 jours. ■ Qualité de la communication avec les parties prenantes internes et les forces de l'ordre.	2	Identifier Rétablir
- Formation et sensibilisation ■ Nombre d'utilisateurs, d'administrateurs, d'enquêteurs et de membres de la direction générale ayant suivi une formation au cours d'une période donnée. ■ Taux de succès aux questionnaires en fin de session de formation. ■ Périodicité des formations proposées. ■ Pourcentage de récurrence. ■ Nombre d'incidents liés aux SI reportés. ■ Nombre d'incidents liés aux SI détectés grâce aux mécanismes de surveillance.	2	Identifier Rétablir
Veiller à ce que l'analyse des retours d'expérience soit effectuée après un événement afin de déterminer les points à améliorer.	2	
Mettre en œuvre des plans de remédiation ou d'amélioration.	2	Répondre Rétablir

Donner une assurance au Conseil

Afin de communiquer de manière efficace les risques liés aux menaces internes au Conseil, les auditeurs internes doivent traduire leurs constats en termes de pertes financières, d'atteinte à la réputation, de perturbation des opérations et selon d'autres indicateurs de performance de l'organisation.

Pour illustrer les risques dans des termes significatifs pour la direction, les auditeurs internes peuvent s'appuyer sur des cas de violation de données et d'incidents causés, à travers le monde, par des menaces internes dans leur secteur d'activité. En effet, utiliser des données réelles permet de décrire toute l'ampleur et la profondeur des impacts et aide à dissiper l'illusion que les menaces internes et les violations qui en résultent ne peuvent pas se produire au sein de l'organisation.

Rapports d'audit

Pour des instructions détaillées sur la préparation des rapports d'audit interne, référez-vous au Guide pratique de l'IIA « Rapports d'audit : communiquer les résultats d'une mission d'assurance ».

Sensibiliser le Conseil signifie également faire comprendre à ses membres que la « sécurité absolue » est illusoire. Il est donc essentiel de s'attacher à renforcer les capacités de réponse de l'organisation aux incidents de sécurité liés aux SI tout en veillant à l'équilibre entre sécurité et efficience (la sécurité est gérée en fonction de l'appétence pour le risque définie par l'organisation). D'autres éléments clés permettent de donner une

assurance au Conseil, notamment :

- Entreprendre une démarche collaborative de reporting avec des parties telles que le responsable de la sécurité des systèmes d'information et le responsable du management des risques afin de prouver le niveau de maturité de la sécurité de l'organisation vis-à-vis des menaces internes.
- S'assurer que les risques liés aux menaces internes sont inclus dans l'évaluation des risques à l'échelle de l'organisation (ERM), et que les travaux et résultats sont communiqués au Conseil.
- Convenir d'un référentiel que toutes les fonctions d'assurance peuvent utiliser pour évaluer la maturité et l'efficacité des actions de maîtrise des menaces internes.
- Élaborer des scénarios de risques afin de décrire les acteurs potentiels ainsi que la probabilité d'occurrence et l'impact dans un langage se rapportant clairement aux objectifs opérationnels.
- Déterminer si la fonction d'audit interne possède les compétences nécessaires pour évaluer la gestion des menaces internes ou si elle peut être formée. Dans le cas contraire, sous-traiter l'expertise.
- Élaborer un plan annuel d'audit pour tirer parti des travaux d'autres fonctions d'assurance (conformité, auto-évaluations du management et résultats de la gestion des risques).

Afin de bénéficier des travaux d'autres fonctions, il est essentiel de définir clairement les rôles et les responsabilités des opérationnels, de la gestion des risques, de la conformité et d'autres parties prenantes de la fourniture d'assurance. Il convient également de déterminer les informations pouvant être utilisées ainsi que la manière dont la fonction d'audit interne évaluera la fiabilité des travaux effectués par la première et la deuxième ligne de maîtrise.

Utilisation d'autres travaux d'assurance

Pour des instructions détaillées sur la manière de créer une cartographie des prestations d'assurance, référez-vous au Guide pratique « Coordination et utilisation d'autres travaux : élaborer une cartographie des prestations d'assurance ».

Annexe A. Normes et lignes directrices de l'IIA applicables

Les ressources IIA suivantes sont mentionnées dans ce guide pratique. Pour en savoir plus sur l'application des *Normes internationales pour la pratique professionnelle de l'audit interne*, veuillez vous référer aux guides de mise en œuvre de l'IIA.

Normes
Norme 1210 – Compétence
Norme 2010 – Planification
Norme 2050 – Coordination et utilisation d'autres travaux
Norme 2100 – Nature du travail
Norme 2110 – Gouvernance
Norme 2120 – Management des risques
Norme 2130 – Contrôle
Norme 2200 – Planification de la mission
Norme 2201 – Considérations relatives à la planification
Norme 2210 – Objectifs de la mission
Norme 2220 – Périmètre d'intervention de la mission
Norme 2230 – Ressources affectées à la mission
Norme 2240 – Programme de travail de la mission

Lignes directrices
Guide pratique, « Coordination et utilisation d'autres travaux d'assurance : élaborer une cartographie des prestations d'assurance », 2018
Guide pratique, « Planification de la mission : évaluation des risques de fraude », 2017
Guide pratique, « Planification de la mission : définir les objectifs et le périmètre d'intervention », 2017
GTAG, « Évaluer le risque de cybersécurité : les rôles des trois lignes de maîtrise », 2016
GTAG, « Auditer la gouvernance des systèmes d'information », 2018

Annexe B. Glossaire

Les termes marqués d'un astérisque (*) sont issus du glossaire du *Cadre de référence international des pratiques professionnelles* de l'IIA.

Audit interne* : Fonction assurée par un service, une division, une équipe de consultants ou tout autre praticien, c'est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'audit interne aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité.

Appétence pour le risque* : Niveau de risque qu'une organisation est prête à accepter.

Conseil* : Le niveau le plus élevé des organes de gouvernance (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) responsable du pilotage, et/ou de la surveillance des activités de l'organisation et, envers lequel la direction générale a un devoir de rendre compte. Bien que les mécanismes de gouvernance varient selon les juridictions et les secteurs, le Conseil comprend généralement des membres qui ne font pas partie du management. Si un tel Conseil n'existe pas, le mot « Conseil » dans les Normes correspond à un groupe ou à une personne en charge de la gouvernance de l'organisation. En outre, « Conseil » dans les Normes peut renvoyer à un comité ou une autre instance auquel l'organe de gouvernance a délégué certaines fonctions (par exemple, un comité d'audit).

Fraude* : Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou lié à leur activité.

Gouvernance* : Le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

Incident de sécurité lié aux SI[9] : Evénement qui compromet réellement ou potentiellement la confidentialité, l'intégrité ou la disponibilité d'un système d'information, ou de l'information que le système traite, stocke ou transmet, ou qui constitue une violation ou une menace imminente de violation des politiques ou des procédures de sécurité, ou encore des politiques d'utilisation acceptable.

Ingénierie sociale[10] : Dans le contexte de la sécurité de l'information, il s'agit de la manipulation d'individus dans le but de les amener à accomplir, de manière involontaire, des actions portant préjudice (ou augmentant la probabilité de causer un préjudice futur) à la confidentialité, l'intégrité ou la disponibilité des ressources ou des actifs de l'organisation, y compris les informations, les systèmes d'information ou les systèmes concernant les aspects financiers.

---

[9] Glossaire du Committee on National Security Systems, *CNSS Instruction N° 4009, National Information Assurance Glossary*, (Washington D.C. : National Security Agency, 2010), p. 35.

[10] CERT® Insider Threat Center, « Unintentional Insider Threats: Social Engineering », https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf, p. xi.

Mission d'assurance* : Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernance, de management des risques et de contrôle.

Mission de conseil* : Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le périmètre d'intervention sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer les processus de gouvernance, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

Partenaires : Tous les tiers jouissant d'un droit d'accès aux réseaux, systèmes et données des clients, acheteurs ou fournisseurs de l'organisation.

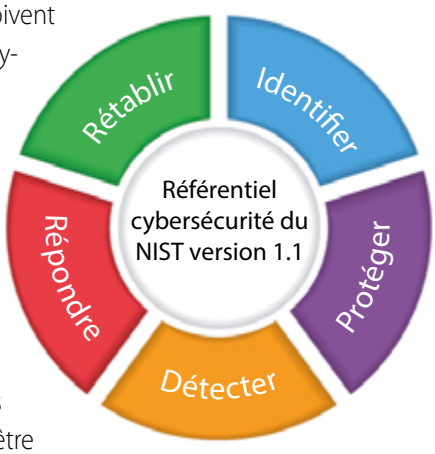
Processus de contrôle* : Les règles, procédures et activités (aussi bien manuelles qu'automatisées) faisant partie d'un cadre de contrôle interne, conçues et mises en œuvre pour s'assurer que les risques sont maintenus dans les limites que l'organisation est disposée à accepter.

Responsable de l'audit interne* : Désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de diriger efficacement la fonction d'audit interne conformément à la charte d'audit interne et aux dispositions obligatoires du Cadre de référence international des pratiques professionnelles de l'audit interne. Le responsable de l'audit interne ou des personnes qui lui sont rattachées de l'audit interne devront disposer des certifications et des qualifications professionnelles appropriées. L'intitulé exact du poste et/ou de la fonction du responsable de l'audit interne varie selon les organisations.

Risque* : Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

Annexe C. Évaluation de la menace interne à l'aide du référentiel cybersécurité du NIST

Conformément à la Norme 2240.A1, « les programmes de travail doivent faire référence aux procédures à appliquer pour identifier, analyser évaluer et documenter les informations lors de la mission ». Comme point de départ pour élaborer leur programme de travail, les auditeurs internes peuvent utiliser un référentiel des risques et des contrôles existants. Le tableau ci-dessous utilise le référentiel cybersécurité du NIST comme le critère auquel un programme relatif aux menaces internes peut être comparé. Les auditeurs peuvent adapter ces données en fonction de leur organisation et de ses missions spécifiques. Sur la base de ce tableau, ils peuvent concevoir une matrice des risques et des contrôles ainsi qu'une évaluation des risques qui pourront ensuite être transformées en un programme de travail.



Le référentiel cybersécurité du NIST a été créé pour fournir un langage commun permettant de comprendre, gérer et exprimer les risques liés à la cybersécurité, tant en interne qu'à l'extérieur. Ce référentiel aide les utilisateurs à identifier et prioriser les actions de maîtrise des risques liés à la cybersécurité, dont les menaces internes. Ce cadre peut facilement être traduit en actes permettant de réduire les risques de menace interne.

Il est organisé selon différentes fonctions (identifier, protéger, détecter, répondre et rétablir), catégories et sous-catégories. Dans ce programme de travail, les catégories sont les objectifs de contrôle, et les sous-catégories représentent les activités de contrôle. Les auditeurs internes peuvent utiliser la dernière colonne du document pour indiquer les dispositifs de contrôle en place dans leur organisation (*Réimprimé avec la permission du National Institute of Standards and Technology, ministère américain du Commerce. Non soumis aux droits d'auteur aux États-Unis).*

Fonction : Identifier	
Domaine de risque : Gestion des actifs	
Objectif de contrôle : Les données, collaborateurs, systèmes, installations et le matériel qui permettent à l'organisation d'atteindre ses objectifs sont identifiés et gérés selon leur importance relative au regard des objectifs opérationnels et de la stratégie de gestion des risques.	
Activités de contrôle	Évaluation
Le matériel et les systèmes physiques de l'organisation sont répertoriés.	
Les plateformes et applications logicielles de l'organisation sont répertoriées.	
La communication et les flux de données de l'organisation sont cartographiés.	
Les systèmes d'information externes sont répertoriés.	
Les ressources (par exemple, le matériel, les périphériques, les données, l'horodatage et les logiciels) sont priorisées selon leur classification, leur criticité et leur valeur.	
Les rôles et responsabilités en matière de cybersécurité sont établis pour l'ensemble des salariés et des tiers (tels que les fournisseurs, les clients et les partenaires).	

Fonction : Identifier (suite)	
Domaine de risque : Contexte opérationnel	
Objectif de contrôle : La mission, les objectifs, les parties prenantes et les activités de l'organisation sont compris et priorisés ; ces informations sont utilisées pour préciser les rôles, les responsabilités et les décisions en matière de management des risques dans le domaine de la cybersécurité.	
Activités de contrôle	Évaluation
Le rôle de l'organisation dans la chaîne d'approvisionnement est identifié et communiqué.	
La place de l'organisation dans les infrastructures critiques et au sein de son secteur d'activité est identifiée et communiquée.	
Les priorités de la mission, des objectifs et des activités de l'organisation sont établies et communiquées.	
Les liens de dépendance de l'organisation sont établis ainsi que les fonctions critiques nécessaires aux prestations de services critiques.	
Les exigences en matière de résilience pour soutenir les prestations de services critiques sont établies pour tous les états de fonctionnement (par exemple, en cas de contrainte/d'attaque, pendant la reprise, en fonctionnement normal).	
Domaine de risque : Gouvernance	
Objectif de contrôle : Les règles, procédures et processus de gestion et de suivi des exigences de l'organisation en matière réglementaire, juridique, environnementale, opérationnelle et de risques sont compris et alimentent le management des risques liés à la cybersécurité.	
Activités de contrôle	Évaluation
La politique de sécurité de l'information de l'organisation est établie.	
Les rôles et responsabilités en matière de sécurité de l'information sont coordonnés et en phase avec les rôles internes ainsi que ceux des partenaires externes.	
Les exigences juridiques et réglementaires concernant la cybersécurité, y compris la protection de la vie privée, les libertés civiles et les obligations, sont comprises et administrées.	
Les processus de gouvernance et de management des risques traitent les risques liés à la cybersécurité.	
Domaine de risque : Évaluation des risques	
Objectif de contrôle : L'organisation comprend les risques que la cybersécurité représente pour ses opérations (c'est-à-dire la réalisation de sa mission, ses activités, son image ou sa réputation), ses actifs et ses collaborateurs.	
Activités de contrôle	Évaluation
La vulnérabilité des actifs est identifiée et documentée.	
Des renseignements concernant les risques cyber et les vulnérabilités sont reçus depuis des forums et des sources de partage d'information.	
Les menaces, qu'elles soient internes ou externes, sont identifiées et documentées.	
Les impacts potentiels sur l'activité et les probabilités d'occurrence sont définis.	
Les menaces, les vulnérabilités, les probabilités et les impacts sont utilisés pour déterminer les risques.	
Les modalités de traitement des risques sont identifiées et priorisées.	

Fonction : Identifier (suite)	
Domaine de risque : Stratégie de management des risques	
Objectif de contrôle : Les priorités, les limites, la tolérance au risque et les hypothèses de l'organisation sont établies et utilisées dans les décisions relatives aux risques opérationnels.	
Activités de contrôle	Évaluation
Les processus de management des risques sont établis, gérés et acceptés par les parties prenantes de l'organisation.	
La tolérance au risque de l'organisation est définie et clairement exprimée.	
La détermination de la tolérance au risque de l'organisation s'appuie sur sa place dans les infrastructures critiques et l'analyse des risques propres à son domaine d'activité.	
Domaine de risque : Management des risques liés à la chaîne d'approvisionnement	
Objectif de contrôle : Les priorités, les limites, la tolérance au risque et les hypothèses de l'organisation sont établies et utilisées dans les décisions relatives au management des risques de la chaîne d'approvisionnement. L'organisation a mis en place des processus pour identifier, évaluer et gérer les risques de la chaîne d'approvisionnement.	
Activités de contrôle	Évaluation
Les processus de management des risques liés à la chaîne d'approvisionnement sont identifiés, établis, évalués, gérés et acceptés par les parties prenantes de l'organisation.	
Identifier, prioriser et évaluer les fournisseurs et partenaires des systèmes d'information, composantes et services critiques à l'aide d'un processus de management des risques liés à la chaîne d'approvisionnement.	
Les fournisseurs et les partenaires sont contractuellement tenus de mettre en œuvre des indicateurs appropriés conçus pour atteindre les objectifs du programme de sécurité de l'information ou du plan de management des risques liés à la chaîne d'approvisionnement.	
Les fournisseurs et les partenaires font l'objet d'évaluations afin de confirmer qu'ils ont remplis leurs obligations. Des revues des missions d'audit, des résumés des résultats des tests et d'autres évaluations équivalentes des fournisseurs/partenaires sont effectués.	
La planification et les tests de réponse aux incidents et de reprise sont effectués avec les fournisseurs/partenaires critiques.	

Fonction : Protéger	
Domaine de risque : Gestion des identités, authentification et contrôles d'accès	
Objectif de contrôle : L'accès aux actifs physiques et logiques ainsi qu'aux installations associées est limité aux utilisateurs, processus et périphériques autorisés, et est géré en cohérence avec l'évaluation des risques liés aux accès non autorisés à des activités et transactions.	
Activités de contrôle	Évaluation
Des identités et identifiants sont émis, gérés, vérifiés, révoqués et audités pour les périphériques, utilisateurs et processus autorisés.	
L'accès physique aux actifs est géré et protégé.	
L'accès à distance est géré.	
Les autorisations et permissions d'accès sont gérées selon les principes du privilège minimal et de la séparation des tâches.	
L'intégrité du réseau est protégée, en intégrant, le cas échéant, des segmentations de réseau.	
Les identités sont vérifiées, liées aux informations d'identification, et utilisées dans les interactions lorsque cela est nécessaire.	

Fonction : Protéger (suite)	
Domaine de risque : Sensibilisation et formation	
Objectif de contrôle : Les collaborateurs et les partenaires de l'organisation sont sensibilisés à la cybersécurité et sont formés pour être en mesure de s'acquitter de leurs rôles et responsabilités en matière de sécurité de l'information, conformément aux règles, procédures et contrats.	
Activités de contrôle	**Évaluation**
Tous les utilisateurs sont informés et formés.	
Les utilisateurs privilégiés comprennent leurs rôles et responsabilités.	
Les tiers (tels que les fournisseurs, les clients et les partenaires) comprennent leurs rôles et responsabilités.	
Les cadres dirigeants comprennent leurs rôles et responsabilités.	
Les collaborateurs chargés de la sécurité physique et de l'information comprennent leurs rôles et responsabilités.	
Domaine de risque : Sécurité des données	
Objectif de contrôle : Les informations et enregistrements (données) sont gérés conformément à la stratégie de management des risques de l'organisation afin de protéger la confidentialité, l'intégrité et la disponibilité de l'information.	
Activités de contrôle	**Évaluation**
Les données en transit sont protégées.	
Les actifs sont gérés de manière officielle tout au long du processus d'extraction, de transfert et de destruction.	
Les capacités nécessaires pour assurer la disponibilité sont maintenues.	
Des protections contre les fuites de données sont mises en place.	
Des dispositifs pour contrôler l'intégrité sont utilisés au niveau du logiciel, du micrologiciel *(firmware)* et des informations.	
Les environnements de développement et de test sont séparés de l'environnement de production.	
Des dispositifs de vérification de l'intégrité sont utilisés au niveau du matériel.	
Domaine de risque : Processus et procédures de protection de l'information	
Objectif de contrôle : Les politiques de sécurité (qui traitent de l'objectif, du champ d'application, des rôles, des responsabilités, de l'engagement de la direction générale et de la coordination entre les entités de l'organisation), les processus et les procédures sont maintenus et utilisés pour gérer la protection des systèmes et des actifs.	
Activités de contrôle	**Évaluation**
Une configuration de base des systèmes de contrôle de l'information/ opérationnel intégrant les principes de sécurité appropriés (comme le concept de fonctionnalité minimale) est créée et maintenue.	
Un cycle de développement est mis en place afin de gérer les systèmes.	
Des processus de contrôle des changements de configuration sont mis en place.	
Les informations sont sauvegardées, maintenues et testées de manière régulière.	
Les politiques et réglementations relatives à l'environnement physique d'utilisation des actifs sont respectées.	
Les données sont détruites selon les règles en vigueur.	
Les processus de protection sont sans cesse améliorés.	
L'efficacité des technologies de protection est communiquée aux parties concernées.	

Fonction : Protéger (suite)	
Activités de contrôle	Évaluation
Les plans de réponse (résolution des incidents et continuité d'activité) et de reprise (reprise après incident et reprise après sinistre) sont mis en place et administrés.	
Les plans de réponse et de reprise sont testés.	
La cybersécurité est intégrée dans les activités concernant les ressources humaines (par exemple, la suppression de comptes de collaborateurs, la vérification des profils de carrière).	
Un plan de gestion des vulnérabilités est élaboré et mis en œuvre.	
Domaine de risque : Entretien	
Objectif de contrôle : L'entretien et la réparation des composantes des systèmes de contrôle opérationnel et d'information sont effectués conformément aux règles et procédures.	
Activités de contrôle	Évaluation
L'entretien et la réparation des actifs de l'organisation sont effectués et enregistrés rapidement, à l'aide d'outils approuvés et contrôlés.	
L'entretien à distance des actifs de l'organisation est approuvé, enregistré et effectué de manière à éviter les accès non autorisés.	
Domaine de risque : Technologies de protection	
Objectif de contrôle : Les solutions de sécurité technique sont gérées de manière à assurer la sécurité et la résilience des systèmes et des actifs, conformément aux règles, procédures et contrats y afférents.	
Activités de contrôle	Évaluation
Les registres d'activité et de vérification sont définis, documentés, mis en œuvre et revus conformément à la politique en vigueur.	
Les supports amovibles sont protégés et leur utilisation est restreinte conformément à la politique en vigueur.	
Le principe de fonctionnalité minimale est intégré lors de la configuration des systèmes de manière à ne fournir que les capacités essentielles.	
Les réseaux de communication et de contrôle sont protégés.	
Les systèmes fonctionnent selon des états fonctionnels prédéfinis afin d'assurer leur disponibilité (en cas de contrainte, d'attaque, pendant la reprise et en fonctionnement normal, par exemple).	

Fonction : Détecter	
Domaine de risque : Anomalies et événements	
Objectif de contrôle : Les activités anormales sont détectées rapidement et l'impact potentiel des événements est compris.	
Activités de contrôle	Évaluation
Les événements détectés sont analysés afin de comprendre les cibles et les méthodes de l'attaque.	
Les données concernant les événements sont corrélées et agrégées à partir de multiples sources et capteurs.	
L'impact des événements est déterminé.	
Des seuils d'alerte en cas d'incident sont établis.	
Domaine de risque : Contrôle en continu de la sécurité	
Objectif de contrôle : Les systèmes d'information et les actifs font l'objet d'un suivi régulier afin d'identifier les événements liés à la cybersécurité et de vérifier l'efficacité des mesures de protection.	
Activités de contrôle	Évaluation
Le réseau est surveillé afin de détecter les potentiels événements liés à la cybersécurité.	
L'environnement physique est surveillé afin de détecter les événements potentiels liés à la cybersécurité.	
Les activités des collaborateurs sont suivies afin de détecter les potentiels événements liés à la cybersécurité.	
Les programmes malveillants sont détectés.	
Les codes mobiles non autorisés sont détectés.	
Les activités des prestataires externes sont surveillées afin de détecter les potentiels événements liés à la cybersécurité.	
Une surveillance des connexions personnelles, des appareils et des logiciels non autorisés est effectuée.	
Une analyse de vulnérabilité est effectuée.	
Domaine de risque : Processus de détection	
Objectif de contrôle : Les processus et les procédures de détection sont maintenus et testés afin d'assurer une sensibilisation rapide et appropriée aux événements anormaux.	
Activités de contrôle	Évaluation
Les rôles et les responsabilités en matière de détection sont bien définis afin d'assurer que le devoir de rendre compte est respecté.	
Les activités de détection sont conformes à toutes les exigences applicables.	
Les processus de détection sont testés.	
Les informations concernant la détection d'événement sont communiquées aux parties concernées.	
Les processus de détection sont sans cesse améliorés.	

Fonction : Répondre	
Domaine de risque : Planification des réponses	
Objectif de contrôle : Les processus et procédures de réponse sont exécutés et maintenus afin d'assurer une réponse rapide en cas de détection d'événements liés à la cybersécurité.	
Activités de contrôle	**Évaluation**
Le plan de réponse est exécuté durant ou après l'événement.	
Domaine de risque : Communication	
Objectif de contrôle : Les activités de réponse sont coordonnées avec les parties prenantes internes et externes pour inclure, s'il y a lieu, le soutien des forces de l'ordre.	
Activités de contrôle	**Évaluation**
Les collaborateurs connaissent leur rôle ainsi que la séquence des opérations à réaliser lorsqu'une réponse est nécessaire.	
Les événements sont reportés conformément aux critères qui ont été établis.	
L'information est partagée conformément aux plans de réponse.	
La coordination avec les parties prenantes se déroule conformément aux plans de réponse.	
Un partage volontaire de l'information a lieu avec les parties prenantes externes pour accroître une sensibilisation accrue au contexte de cybersécurité.	
Domaine de risque : Analyse	
Objectif de contrôle : Une analyse est conduite afin d'assurer une réponse appropriée ainsi que le soutien nécessaire aux activités de reprise.	
Activités de contrôle	**Évaluation**
Les notifications provenant des systèmes de détection sont analysées.	
L'impact de l'incident est compris.	
Des investigations sont menées.	
Les incidents sont catégorisés conformément aux plans de réponse.	
Domaine de risque : Maîtrise des risques	
Objectif de contrôle : Des activités sont réalisées afin de prévenir l'expansion de l'événement, d'en réduire les effets et d'enrayer l'incident.	
Activités de contrôle	**Évaluation**
Les incidents sont contenus.	
Les incidents sont maîtrisés.	
Les vulnérabilités nouvellement identifiées sont maîtrisées ou l'acceptation du risque est formalisée.	
Domaine de risque : Améliorations	
Objectif de contrôle : Les activités de réponse de l'organisation sont améliorées en intégrant les leçons tirées des précédentes activités de détection/réponse et de celles qui sont en cours.	
Activités de contrôle	**Évaluation**
Les plans de réponse intègrent les leçons tirées.	
Les stratégies de réponse sont mises à jour.	

Fonction : Rétablir	
Domaine de risque : Planification de la reprise	
Objectif de contrôle : Les processus et procédures de reprise sont exécutés et maintenus afin de garantir une restauration rapide des systèmes ou des actifs affectés en cas d'événements liés à la cybersécurité.	
Activités de contrôle	**Évaluation**
Le plan de reprise est exécuté durant ou après l'événement.	
Domaine de risque : Améliorations	
Objectif de contrôle : La planification et les processus de reprise sont améliorés en intégrant les leçons tirées aux activités futures.	
Activités de contrôle	**Évaluation**
Les plans de reprise intègrent les leçons tirées.	
Les stratégies de reprise sont mises à jour.	
Domaine de risque : Communication	
Objectif de contrôle : Les activités de restauration sont coordonnées avec les parties prenantes internes et externes concernées, telles que les centres de coordination, les prestataires de service Internet, les propriétaires des systèmes vecteurs d'attaques, les victimes, les autres équipes de résolution des incidents en matière de sécurité informatique et les fournisseurs.	
Activités de contrôle	**Évaluation**
Les relations publiques sont gérées.	
La réputation est rétablie suite à un événement.	
Les activités de reprise sont communiquées aux parties prenantes internes et à la direction générale.	

Réimprimé avec la permission du *National Institute of Standards and Technology*, ministère américain du Commerce.
Non soumis aux droits d'auteur aux États-Unis.

Annexe D. Bonnes pratiques du CERT pour minimiser les menaces internes

Le tableau suivant figure dans le guide sur la menace interne *(« Common Sense Guide to Mitigating Insider Threats, Fifth Edition »)* de l'*Insider Threat Center* (CERT® du *Software Engineering Institute* de l'université Carnegie Mellon). Ces 20 bonnes pratiques visent à être une référence pour les organisations qui doivent créer ou mettre à jour un programme relatif aux menaces internes, et elles devraient être adaptées aux besoins, à la culture et à l'appétence pour le risque de l'organisation. L'ordre dans lequel le CERT a organisé ces pratiques est destiné à faciliter le processus de mise en œuvre du programme.

Ces 20 bonnes pratiques sont des assertions ou des objectifs de contrôle, et chacune d'entre elles est décomposée en activités de contrôle plus spécifiques dans le guide.

Ordre	Normes
1	Connaître et protéger les actifs critiques.
2	Élaborer et formaliser un programme relatif aux menaces internes.
3	Formaliser clairement et appliquer de façon cohérente les politiques et les dispositifs de contrôle.
4	Dès le recrutement, être attentif et réagir aux comportements suspects ou perturbateurs.
5	Anticiper et gérer les problèmes pouvant affecter l'environnement de travail.
6	Tenir compte des menaces provenant des profils autorisés et des partenaires lors des évaluations des risques à l'échelle de l'entreprise.
7	Être particulièrement vigilant à l'égard des réseaux sociaux.
8	Structurer le management et les tâches afin de minimiser le stress et les erreurs involontaires.
9	Intégrer la sensibilisation aux menaces internes malveillantes et involontaires dans le cadre d'une formation régulière à destination de tous les collaborateurs.
10	Mettre en œuvre des règles et des pratiques strictes en matière de gestion des mots de passe et des comptes.
11	Instaurer des contrôles d'accès rigoureux et des politiques de surveillance des utilisateurs privilégiés.
12	Déployer des solutions pour surveiller les actions des collaborateurs et corréler des informations provenant de multiples sources.
13	Surveiller et contrôler l'accès à distance depuis tous les points d'accès finaux, dont les périphériques portables.
14	Établir des critères de référence du comportement normal pour les réseaux et les collaborateurs.
15	Imposer une séparation des tâches et la règle du « privilège minimal ».
16	Définir des accords de sécurité explicites pour tout service *cloud*, en particulier concernant les restrictions d'accès et les capacités de surveillance.
17	Formaliser les dispositifs de contrôle de changement de système.
18	Mettre en place des processus de sauvegarde et de récupération.
19	Bloquer les accès à toute exfiltration de données non autorisée.
20	Élaborer une procédure exhaustive pour gérer la cessation d'emploi des collaborateurs.

Source : CERT, « Common Sense Guide to Mitigating Insider Threats, Fifth Edition », 2016, Tableau 1, p. xii.

Annexe E. Organisations et agences émettrices de recommandations

Les ressources figurant ci-dessous peuvent fournir des informations permettant d'aider l'organisation à identifier, surveiller et gérer les menaces internes. Bien qu'elle ne soit pas exhaustive, cette liste contribuera à enrichir les connaissances et les compétences des auditeurs internes. De plus, les normes et réglementations en matière de sécurité, qu'elles soient locales ou sectorielles, doivent être prises en compte lors de la phase de planification de la mission d'audit afin de s'assurer que les ressources sont affectées aux risques les plus importants pour l'organisation en question.

American National Standards Institute (ANSI) / *International Society of Automation* (ISA)

L'ANSI est le porte-parole du système américain de normalisation et d'évaluation de la conformité, et le représentant officiel des États-Unis auprès de l'Organisation internationale de normalisation et, par le biais du *U.S. National Committee*, à la Commission électrotechnique internationale (CEI). La mission de l'ANSI est de renforcer la compétitivité mondiale des entreprises américaines tout en améliorant la qualité de vie aux États-Unis en promouvant et en facilitant l'adoption de normes volontaires issues d'un consensus ainsi que des systèmes d'évaluation de la conformité, et en préservant leur intégrité https://www.ansi.org/cyber/

Gouvernement australien : *Attorney General's department*

Le *Protective Security Policy Framework* (PSPF) comprend l'approche du gouvernement australien en matière de management des risques liés à la sécurité ainsi que des lignes directrices pour la mettre en œuvre efficacement. Il inclut trois exigences concernant la sécurité des collaborateurs essentielles pour réduire la menace posée par un profil autorisé ayant la confiance de l'organisation. https://www.protectivesecurity.gov.au/personnel/Pages/default.aspx

Center for Internet Security (CIS)

Le CIS est une entité à but non lucratif qui établit des normes internationales et des bonnes pratiques en matière de sécurité des systèmes d'information et des données afin de protéger les organisations privées et publiques contre les cyberattaques, grâce à une communauté mondiale d'experts SI. https://www.cisecurity.org

Gouvernement australien : CERT *(Computer Emergency Response Team)*

Le centre national de réponse aux urgences informatiques (CERT Australia) a été fondé en 2010. Il est le principal interlocuteur étatique des grandes entreprises australiennes, notamment pour ce qui est de :

- recenser et répondre aux incidents de cybersécurité déclarés ;
- bénéficier d'un soutien et de conseils en matière de réponse et de maîtrise des incidents liés à la cybersécurité ;
- surveiller les incidents liés à la cybersécurité ou les attaques afin d'avoir une meilleure vision des menaces existantes ;
- fournir des conseils et alerter ses partenaires pour renforcer leur résilience en matière de cybersécurité.

https://www.cert.gov.au/

CERT - SEI *(Software Engineering Institute)*

Le CERT est un département du *Software Engineering Institute* de l'université Carnegie Mellon qui étudie et résout les problèmes en matière de cybersécurité ayant des répercussions étendues. Il mène des recherches sur les failles de sécurité des logiciels, contribue à modifier les systèmes réseaux sur le long terme et fournit de la documentation et des formations de pointe afin d'améliorer la cybersécurité. Le CERT fournit des ressources qui permettent d'aider les organisations à élaborer et mettre en œuvre des programmes relatifs aux menaces internes. http://www.cert.org

Cyber Security Agency of Singapore (CSA)

La CSA est une agence nationale chargée de superviser la stratégie en matière de cybersécurité, sa mise en œuvre, la formation et la diffusion des informations, ainsi que le développement de l'écosystème. Elle est rattachée au Cabinet du Premier ministre de Singapour et gérée par le ministère des Communications et de l'Information. Entre autres activités, la CSA vise :

- *L'engagement et la sensibilisation :* entretenir les relations, au niveau local et mondial, ainsi que le leadership en matière de cybersécurité, accroître la prise de conscience au moyen de programmes de sensibilisation du public, et promouvoir la sécurité dès le stade de la conception *(security-by-design).*
- *Le développement de l'écosystème :* mettre en place un solide écosystème de cybersécurité (c.-à-d. un secteur dynamique doté de la main-d'œuvre nécessaire pour répondre aux cyberattaques et en maîtriser les effets).
- *La protection des secteurs critiques :* renforcer la cybersécurité dans nos domaines critiques, tels que l'énergie, l'eau et le secteur bancaire.
- *Les opérations :* assurer une coordination effective et un déploiement efficace des réponses en matière de cybermenaces.

https://www.csa.gov.sg

Intel® Corporation

Le livre blanc « Insider Threat Field Guide » identifie 60 vecteurs d'attaque les plus probables afin d'offrir aux organisations un moyen cohérent de partager les informations en interne et en externe, et leur permettre d'instaurer des stratégies plus efficaces en matière de sécurité et de réponse aux attaques venant de l'intérieur de l'organisation. https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html

Intelligence and National Security Alliance (INSA)

En partenariat avec le ministère américain de la Sécurité intérieure, le FBI et le renseignement national *(Office of the Director of National Intelligence),* l'INSA favorise les collaborations entre le secteur privé et les équipes d'analystes expérimentés du renseignement. Fournir des lignes directrices en matière d'identification et de lutte contre les menaces internes figure parmi les principales priorités de l'agence. https://www.insaonline.org

Organisation internationale de normalisation (ISO) / Commission électrotechnique internationale (CEI)

L'ISO est une organisation internationale non gouvernementale, indépendante, dont les 162 membres sont les organismes nationaux de normalisation. Par ses membres, l'Organisation réunit des experts qui mettent en commun leurs connaissances pour élaborer des Normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux. La CEI est le leader mondial en matière de développement et de publication de normes internationales dans le domaine de l'électrotechnologie (électricité, électronique et technologies apparentées). Lorsque cela se révèle pertinent, la CEI coopère avec l'ISO afin de s'assurer que les normes internationales sont parfaitement harmonisées et se complètent. https://www.iso.org

INTERPOL

Avec 194 pays membres, INTERPOL est la plus grande organisation de coopération policière internationale au monde. INTERPOL publie des lignes directrices générales sur la cybercriminalité et les infractions facilitées par les technologies de l'information et de la communication. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

National Institute of Standards and Technology (NIST)

Le référentiel cybersécurité du NIST est un ensemble de normes et de bonnes pratiques créées grâce à la collaboration entre les secteurs public et privé pour aider les organisations à gérer les risques liés à la cybersécurité. Le référentiel utilise un langage commun pour traiter et gérer les risques liés à la cybersécurité selon une approche coût-efficacité et selon les besoins métiers. https://www.nist.gov/cyberframework

Annexe F. Références et ressources complémentaires

Les ressources figurant ci-dessous peuvent fournir des informations permettant d'aider l'organisation à identifier, surveiller et gérer les menaces internes. Bien qu'elle ne soit pas exhaustive, cette liste contribuera à enrichir les connaissances et les compétences des auditeurs internes. De plus, les normes et réglementations en matière de sécurité, qu'elles soient locales ou sectorielles, doivent être prises en compte lors de la phase de planification de la mission d'audit afin de s'assurer que les ressources sont affectées aux risques les plus importants pour l'organisation en question.

Références

CERT Insider Threat Center, *Common Sense Guide to Mitigating Insider Threats, Fifth Edition,* Pittsburgh, Pennsylvanie, Carnegie Mellon University, 2016, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

CERT Insider Threat Center, *Unintentional Insider Threats: Social Engineering,* Pittsburgh, Pennsylvanie, Carnegie Mellon University, 2014, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

INSA, *Insider Threat Program Roadmap*, https://www.insaonline.org/insider-threat-roadmap/

National Cybersecurity and Communications Integration Center, ministère américain de la Sécurité intérieure, *Combating the Insider Threat*, Washington, DC, DHS/US-CERT, 2014. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

Ponemon Institute ©, *2018 Cost of Insider Threats: Global*, New York, NY, ObservIT 2018, https://www.observeit.com/ponemon-report-cost-of-insider-threats/

Gary Stoneburner, Alice Goguen et Alexis Feringa, National Institute of Standards and Technology (NIST), édition spéciale 800-30, *Risk Management Guide for Information Technology Systems*, juillet 2002.

Cadre de Référence International des Pratiques Professionnelles de l'audit interne, édition 2017, Lake Mary, Floride, The Institute of Internal Auditors, 2017.

Randy Trzeciak et Dan Costa, *Model-Driven Insider Threat Control Selection*, Pittsburgh, Pennsylvanie, Carnegie Mellon University, 2017, https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_509187.pdf

Ressources supplémentaires

American National Standards Institute/International Society of Automation, ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, https://tinyurl.com/ANSI-ISA-62443-2-1

American National Standards Institute/International Society of Automation, ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*, https://tinyurl.com/ANSI-ISA-62443-3-3

A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector, https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/

Australian Government Attorney-General's Department, *13 Ongoing assessment of personnel*, le 27 juin 2018, https://www.protectivesecurity.gov.au/personnel/ongoing-assessment-of-personnel/Pages/default.aspx

Center for Internet Security, *CIS Critical Security Controls™ for Effective Cyber Defense (CIS Controls),* https://www.cisecurity.org/controls/

CERT Australia, *Insider threat: Beyond technical controls*, 26 mars 2018, https://www.cert.gov.au/news/insider-threat-beyond-technical-controls

Daniel Costa, CERT « Definition of 'Insider Threat' – Update », *Insider Threat Blog,* Carnegie Mellon University Software Engineering Institute, SEI Insights, 7 mars 2017, https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

Intel® Corporation, *Insider Threat Field Guide*, https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html

Organisation internationale de normalisation/Commission électrotechnique internationale, *ISO/IEC 27001: 2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements*, https://www.iso.org/standard/54534.html

Sarah Miller, «The Frequency and Impact of Insider Collusion», *Insider Threat Blog*, Carnegie Mellon University Software Engineering Institute, SEI Insights, 22 juin 2016, https://insights.sei.cmu.edu/insider-threat/2016/06/the-frequency-and-impact-of-insider-collusion.html

National Institute of Standards and Technology, NIST SP 800-53 Rev. 4: édition spéciale du NIST 800-53 révision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, avril 2013 (dont les mises à jour du 15 janvier 2014), http://dx.doi.org/10.6028/NIST.SP.800-53r4

Ponemon Institute©, *2017 Cost of Cyber Crime Study*, New York, NY, Accenture, 2017, https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

Ponemon Institute©, *2016 Cost of Cyber Crime Study*, Traverse City, Michigan, Ponemon Institute, 2016 https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Remerciements

Équipe projet

Himi Tina Kim, CIA, CGAP, CRMA, Etats-Unis (Chairman)
Joseph Keating, Etats-Unis
Michael Lynn, CRMA, Etats-Unis
Sajay Rai, Etats-Unis
Terence Washington, CIA, CRMA, Etats-Unis

Contributeurs

Jared Hoffman, Etats-Unis
Yadeli Ibarra, CISA, Mexique
Brad McGary, Etats-Unis
Phillip Nemmers, CISA, Etats-Unis
Patricia Rowe Seale, CIA, CRMA, CISA, CRISC, Barbade
Andriy Rybalchenko, CISA, CISM, Ukraine
Deb Snyder, Etats-Unis

Collaborateurs de l'IIA Global en charge des Normes et des lignes directrices

Eva Sweet, CISA, CISM, IT and PS Director, (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Anne Mercer, CIA, QIAL, Director
Jeanette York, CCSA, FS Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

Réviseurs de la traduction française

Marie-Elisabeth Albert, CIA
Bouchra Bajjou
Jean-François Charbonnier
François Dumont , CISA, CISM
Vianney Dumont, CIA
Julien Cornuché, CIA, CISA
Béatrice Ki-Zerbo, CIA
Sébastien Lepers, CIA, CFE, CGAP, CRMA
Béatrice Vedrenne Robson

L'IIA souhaite remercier les instances suivantes pour leur soutien : Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

À propos de l'IIA

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, dont le siège mondial se situe à Lake Mary (Floride, États-Unis), compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires. Plus d'informations sont disponibles sur le site www.globaliia.org / www.theiia.org.

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 est seulement destinée à servir de guide. L'*Institute of Internal Auditors* vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'IIA dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

Copyright

Copyright© 2018 *The Institute of Internal Auditors, Inc.* Tous droits réservés. 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

Novembre 2018 – ISBN: 978-2-915042-96-2

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org