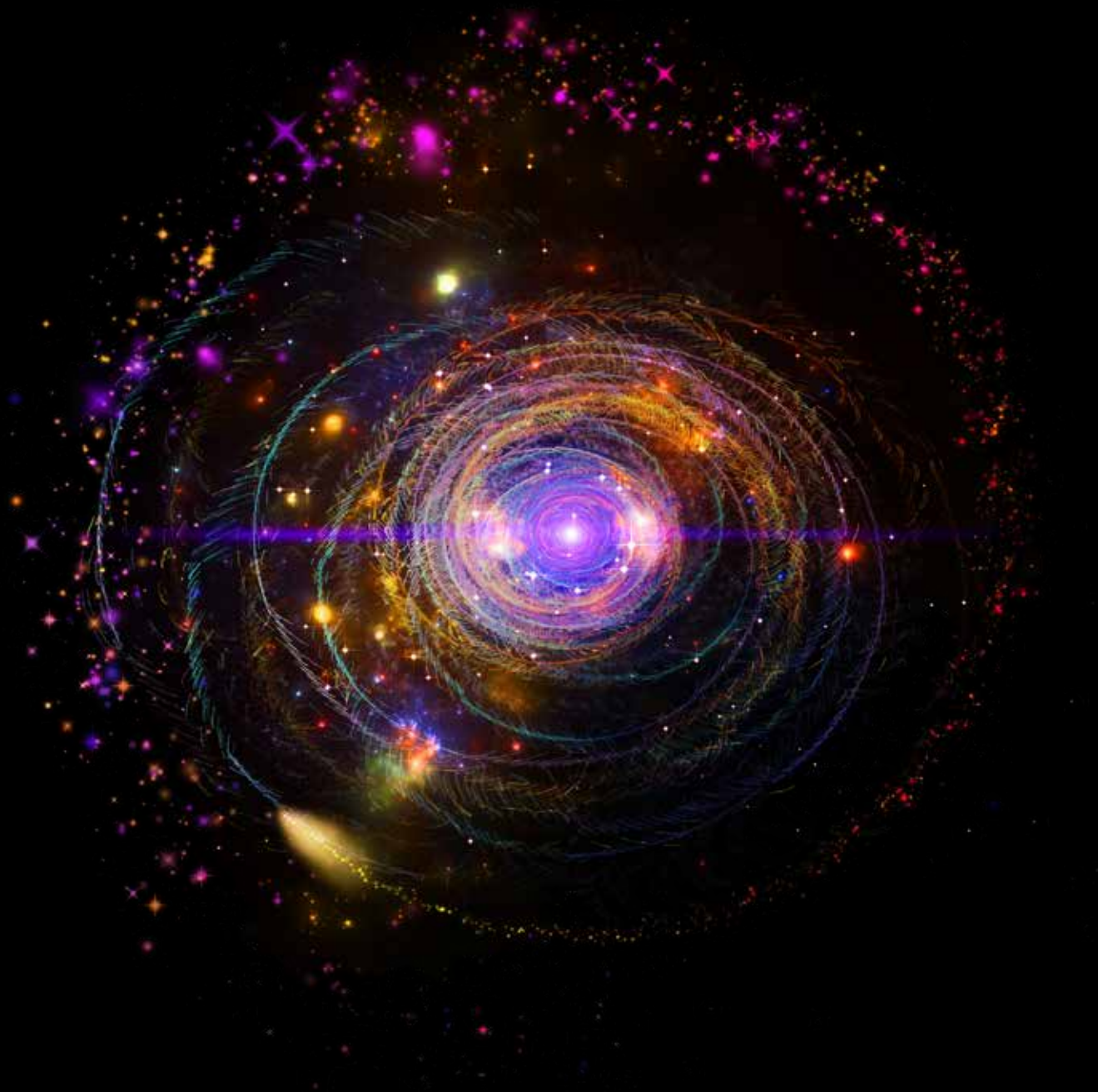
Deloitte.



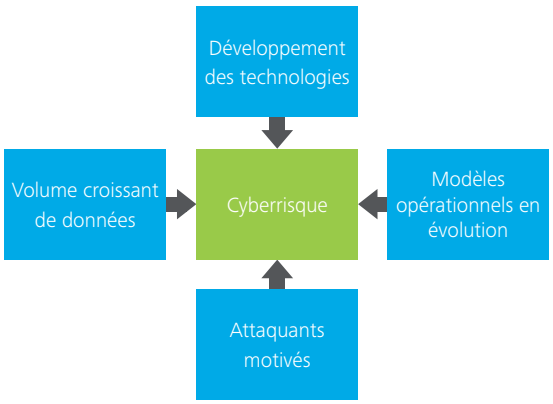
Le chemin des idées

Cybersécurité et rôle de l'audit interne :
Un appel urgent à l'action

Selon notre expérience, une première étape efficace consiste pour l'audit interne à effectuer une évaluation des cyberrisques et à en présenter les conclusions dans un résumé concis au comité d'audit et au conseil d'administration, ce qui mènera par la suite à l'établissement d'un plan pluriannuel d'audit interne de cybersécurité qui sera axé sur les risques.

Les cyberattaques représentent une menace sérieuse dont l'évolution est constante. Selon une estimation, le cybercrime pourrait coûter aux entreprises plus de 2 000 milliards de dollars d'ici 2019, soit près de quatre fois les dépenses estimées pour 2015[1]. De nombreux comités d'audit et conseils d'administration ont établi des attentes à l'égard de l'audit interne pour comprendre et évaluer les capacités des organisations à gérer les cyberrisques.

Figure 1. Facteurs de cybervulnérabilté



Importance croissante de la question

Les facteurs qui stimulent la croissance et l'efficacité d'une entreprise contribuent à l'expansion de la surface vulnérable aux cyberattaques (Figure 1). Internet ainsi que les technologies infonuagiques, mobiles et sociales, dont l'utilisation est maintenant largement répandue, sont des plate-formes intrinsèquement axées sur le partage d'information. L'impartition du travail, le recrutement d'employés contractuels et le travail à distance entraînent des changements aux contrôles opérationnels. La quantité de données s'accroît et les exigences visant à les protéger augmentent elles aussi. De plus, les attaquants, allant de pirates individuels à des États-nations, innovent et contournent continuellement les mécanismes de contrôle courants, certains d'entre eux étant parfois hors de la portée des organes nationaux d'application de la loi.

Les atteintes à la cybersécurité qui font les manchettes et l'importance croissante que le gouvernement accorde aux cybermenaces ont attisé les craintes des comités d'audit et des conseils d'administration des entreprises. En vertu des lignes directrices de la Securities and Exchange Commission (SEC), les sociétés ouvertes doivent aborder les risques liés à la cybersécurité et les cyberincidents potentiellement importants dans leur rapport de gestion[2]. En raison des préoccupations croissantes liées aux cyberattaques touchant l'infrastructure critique du pays, le décret 13636 signé par le président Obama, *Improving Critical Infrastructure Cybersecurity*, a mis l'accent sur le rôle des entreprises dans l'amélioration du cadre national de cybersécurité, ainsi que sur la nécessité de s'adapter rapidement à l'évolution des attentes et des mécanismes de surveillance des organismes de réglementation[3].

Trois lignes de défense

Les unités d'affaires et les services de technologie de l'information intègrent la gestion des cyberrisques dans les processus décisionnels et les activités courantes. Ils constituent la première ligne de défense d'une organisation. La deuxième ligne inclut les responsables de la gestion des risques liés à l'information et à la technologie, lesquels établissent les mécanismes de gouvernance et de surveillance, supervisent les opérations de sécurité, et mettent en place des mesures, au besoin, souvent sous la direction du chef de la sécurité de l'information.

Les entreprises sont de plus en plus nombreuses à reconnaître la nécessité de mettre en place une troisième ligne de cyberdéfense – soit un examen indépendant des mesures de sécurité et de leurs rendement par la fonction d'audit interne. L'audit interne devrait jouer un rôle central dans l'évaluation et l'identification des possibilités de renforcer la sécurité de l'entreprise. Parallèlement, les professionnels de l'audit interne ont le devoir d'informer le comité d'audit et le conseil d'administration que les mécanismes de contrôle dont ils sont responsables sont en place et fonctionnent correctement, ce qui représente une préoccupation croissante au sein des conseils d'administration, les administrateurs pouvant faire face à des obligations juridiques et financières.

Méthode d'évaluation des cyberrisques et mécanismes de défense

L'examen des cyberrisques d'une organisation commence par trois questions clés.

Qui peut attaquer? Les auteurs de l'attaque sont-ils des criminels, des concurrents, des fournisseurs indépendants, des employés internes mécontents, des pirates informatiques poussés par divers intérêts, ou quelqu'un d'autre?

Que cherchent-ils et quels sont les risques d'entreprise qu'il faut atténuer? Souhaitent-ils obtenir de l'argent ou une propriété intellectuelle? Ont-ils pour objectif de perturber les activités ou de ruiner la réputation de l'entreprise? Leurs actions pourraient-elles entraîner des risques en matière de santé et de sécurité?

Quelles tactiques peuvent-ils employer? Feront-ils de l'hameçonnage, mettront-ils à l'épreuve les vulnérabilités des systèmes, utiliseront-ils des profils d'accès volées, ou accéderont-ils au réseau par l'entremise d'un tiers compromis?

Deloitte a établi une approche en trois volets afin d'aider ses clients à faire face aux menaces cernées lors de l'examen des questions précédentes :

Sécurité. La plupart des organisations ont mis en place des mécanismes de contrôle, comme les défenses du périmètre la gestion de l'identité et les mesures de protection de données, afin de se prémunir contre les menaces connues et émergentes.

Les programmes axés sur la gestion risques permettent de prioriser les contrôles liés aux principaux risques d'affaires.

Vigilance. Les renseignements sur les menaces, les systèmes de surveillance de la sécurité et les analyses du comportement ainsi que des risques permettent de détecter les activités malveillantes ou non autorisées, comme les modifications de la configuration d'une application ou les transferts inhabituels de données, et aident l'organisation à s'adapter au contexte changeant des cybermenaces.

Résilience. La mise en place de protocoles d'intervention en cas d'incident, d'outils d'enquête et des plans de continuité des affaires et de relève permet de redresser la situation dans les plus brefs délais et de réduire l'impact.

La réalisation d'un examen axé sur les questions « qui, quoi et comment » présentées précédemment permet à une organisation sécurisée, vigilante et résiliente d'établir le fondement de son cadre général d'audit interne et d'évaluation de la cybersécurité, lequel fera partie intégrante de ses initiatives de cyberdéfense.

Cadre d'évaluation de la cybersécurité – une approche globale

Par le passé, de nombreuses fonctions d'audit interne ont mis en œuvre des procédures visant à évaluer les éléments du plan de préparation en cybersécurité d'une organisation. Ces audits ciblés, comme les procédures liées aux attaques et aux intrusions, sont utiles, mais ne permettent pas d'assurer une protection contre l'ensemble des risques de cybersécurité. L'audit interne devrait par ailleurs appliquer une approche globale afin d'obtenir une vue d'ensemble du mécanisme de cybersécurité et éviter de donner un faux sentiment de sécurité en ne réalisant que des audits ciblés.
La figure 2 représente un cadre d'évaluation de la cybersécurité élaboré en fonction de notre concept recommandé : Sécurité. Vigilance. Résilience. Comme le démontre le tableau, de nombreux domaines de sécurité soutiennent chacun des trois thèmes. Dans le cadre d'une évaluation de la préparation de cybersécurité, l'audit interne aurait avantage à comprendre les capacités associées à chacun des 12 domaines, la façon dont on les aborde aujourd'hui, et les lacunes potentielles au sein de l'organisation.

Figure 2. Cadre représentatif de cybersécurité[4]

Il convient de noter que les rôles et les responsabilités s'inscrivant dans ce cadre ne s'appliquent pas exclusivement à la structure des TI, mais à l'ensemble de l'entreprise. À titre d'exemple, on confie la gestion et la protection des données, soit des éléments de vigilance de la figure 2, à des gestionnaires et des employés de tous les secteurs de l'entreprise afin que ces derniers définissent en quoi consistent leurs données. Cette responsabilité incombe aux employés de tous les échelons de l'organisation et même aux chefs de la direction qui sont tenus d'évaluer l'exposition aux risques dans leurs notes de service et autres communications.

Il existe d'autres considérations importantes, comme la portée limitée des audits des TI actuels et l'absence d'examens internes de certaines capacités. Les champs surlignés du cadre indiquent que les tests relatifs à la *Loi Sarbanes-Oxley*, les tests d'intrusion et de vulnérabilité, et les tests de continuité des affaires et de relève portent respectivement sur certains éléments du cadre Sécurité. Vigilance. Résilience.MC Toutefois, de nombreux autres risques pourraient ne pas être relevés dans le cadre des tests sur les contrôles généraux informatiques comme les fonctions non surlignées de vigilance associées à la modélisation des menaces et à la surveillance des incidents de sécurité, et les fonctions de résilience associées aux tests de relève informatique. L'évaluation des risques cybernétiques par l'équipe d'audit interne permettrait de relever ces lacunes et, par conséquent, d'élaborer des scénarios de jeu de guerre et des exercices visant à mettre en lumière des questions cruciales. Qui doit être contacter quand une menace est identifiée? De quelle façon l'organisation doit-elle intervenir? Si une rançon est demandée, devrait-on la payer?

Les professionnels de l'audit interne doivent tenir compte de plusieurs facteurs lorsqu'ils envisagent ou effectuent une évaluation de la cybersécurité.

Tout d'abord, il est essentiel de faire appel à des personnes possédant l'expérience et les compétences nécessaires. Les professionnels de l'audit interne possèdent le savoir-faire requis pour effectuer les évaluations. Toutefois, afin de déterminer si le service des TI ou le chef de la sécurité de l'information modélisent les menaces de façon efficace, il faut peut-être faire appel à des spécialistes en la matière qui connaissent les questions qui sont pertinentes de poser. Un professionnel en audit axé sur les technologies, connaissant bien le cyberespace, peut représenter une ressource indispensable.

Il est également important d'évaluer l'ensemble du cadre de gestion de la de cybersécurité, plutôt que des éléments distincts. Une telle évaluation exige que l'on détermine l'état actuel de la situation en fonction des caractéristiques du cadre, et que l'on comprenne les objectifs de l'organisation et quelles sont les pratiques minimales attendues en matière de cybersécurité au sein de l'industrie et du secteur d'activité.

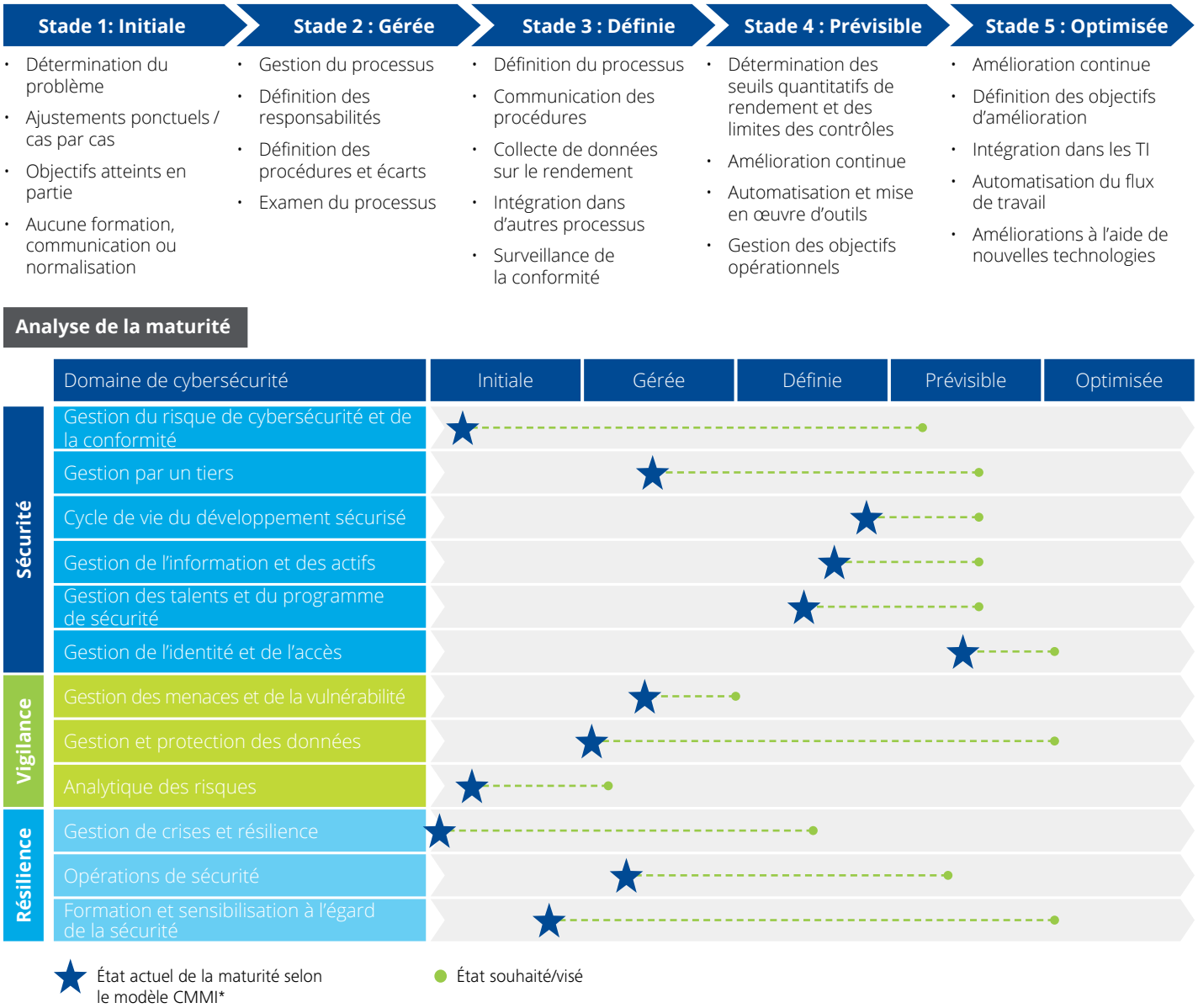
Enfin, l'évaluation initiale devrait être de nature générale. Il ne doit pas s'agir d'une analyse exhaustive qui exige la réalisation de tests poussés. L'évaluation initiale devrait plutôt mener à la tenue d'examens supplémentaires de la cybersécurité qui sont approfondis et axés sur les risques.

Évaluation des cyberrisques – un important point de départ

Le maintien et l'amélioration des capacités de sécurité peuvent contribuer à l'atténuation des cybermenaces et aider l'organisation à atteindre le niveau souhaité de maturité en matière de cybersécurité. En effectuant une évaluation approfondie des cyberrisques, l'équipe d'audit interne peut soumettre des points de vue et des résultats objectifs aux membres du conseil d'administration et du comité d'audit, et s'appuyer sur ces conclusions pour élaborer un plan général d'audit interne portant sur les domaines de cyberrisques auxquels fait face une organisation sur une base annuelle ou pluriannuelle. La réalisation d'une évaluation des risques peut représenter une stratégie pour certaines organisations, alors que d'autres pourraient décider d'employer une approche d'analyse de la maturité. Cette approche peut offrir une valeur ajoutée à la direction et aux responsables de la gouvernance d'entreprise, car elle fournit une référence visuelle rapide qui contient des indices clairs quant aux domaines nécessitant un examen plus approfondi. La participation des experts appropriés permet également de structurer une évaluation des cyberrisques de façon à générer une liste des lacunes de cybersécurité et à fournir à l'organisation une feuille de route pour les mesures correctives à court et à long terme.

La figure 3 présente une analyse qui repose sur les thèmes de la sécurité, de la vigilance et de la résilience, ainsi que sur les 12 domaines de cybersécurité qui y sont associés. Les cinq stades de maturité – initiale, gérée, définie, prévisible et optimisée – rendent compte des progrès que l'organisation a accomplis en ce qui concerne le maintien et l'amélioration de ses capacités de sécurité afin d'atténuer les cybermenaces et d'atteindre le niveau souhaité de maturité. Les lignes pointillées vertes s'étendent jusqu'au niveau de maturité visé par l'organisation, éventuellement établi dans une feuille de route des mesures correctives. À mesure que les changements sont mis en œuvre, les résultats devraient correspondre à l'emplacement des points verts. Le conseil doit convenir du niveau de maturité souhaité une fois les travaux terminés, après quoi l'équipe de l'audit interne doit réaliser un autre test, puis confirmer au conseil que le niveau visé a été atteint.

Figure 3. Exemple d'analyse de la maturité et d'évaluation des risques



*Le modèle d'évaluation CMMI (Capability Maturity Model Integration) reconnu par l'industrie peut être utilisé pour l'analyse. Chaque domaine regroupe des capacités particulières qui sont évaluées, puis une moyenne correspondant à la maturité globale dans le domaine est établie.

Une carte de pointage distincte devrait soutenir l'évaluation de la maturité et mettre en évidence de manière détaillée les cyberrisques qui menacent les gens, les processus et la technologie. On doit par ailleurs consigner les résultats et formuler des recommandations visant à pallier les lacunes relevées.

Fondements d'un plan d'audit interne de cybersécurité

Comme mentionné précédemment, l'évaluation des cyberrisques sous-tend à la fois l'analyse de la maturité soumise au comité d'audit et au conseil d'administration et l'élaboration d'un plan pluriannuel d'audit interne de cybersécurité axé sur les risques. Le plan pluriannuel peut être établi en fonction des résultats de l'évaluation, certains audits pouvant être réalisés plus fréquemment que d'autres selon l'urgence et la nature des autres activités d'évaluation et des tests menés au sein de l'organisation.

Le plan d'audit interne de cybersécurité n'est pas coulé dans le béton. On peut y apporter des ajustements suivant l'émergence de nouveaux risques, de changements dans l'intensité et l'importance relatives des menaces actuelles, et d'autres modifications organisationnelles.

Rôle de l'audit interne dans le renforcement de la cybersécurité

La fréquence et la diversité des cyberrisques, et les dommages potentiels qu'ils peuvent causer aux entreprises, à leurs partenaires commerciaux et à leurs clients ne cessent de croître. La plupart des entreprises prennent ces risques au sérieux, mais de plus amples efforts doivent être déployés afin de lutter contre les dangers et de tenir les dirigeants d'entreprises informés de leur état de préparation de cybersécurité. La fonction d'audit interne joue un rôle crucial en soutenant les entreprises dans la lutte continue que représente la gestion des cybermenaces, en fournissant une évaluation indépendante des mécanismes de contrôle existants ou nécessaires, et en permettant au comité d'audit et au conseil d'administration de mieux comprendre et pallier les différents risques associés au monde numérique.

Personnes-ressources

Nous vous invitons à communiquer avec nous afin d'obtenir de plus amples renseignements sur le rôle de l'audit interne en matière de cybersécurité et la façon dont les Conseils en gestion des risques de Deloitte aide actuellement des organisations à satisfaire aux attentes des conseils d'administration et des comités d'audit.

Kareem Sadek
Associé, Conseils en gestion des riques
ksadek@deloitte.ca

Farzin Ismail
Directrice principale, Conseils en gestion des riques
fismail@deloitte.ca

Marco Spagnoli
Directeur principal, Conseils en gestion des risques
mspagnoli@deloitte.ca

Notes en fin de texte

[1] *Cybercrime Will Cost Businesses Over $2 Trillion by 2019*, Juniper Research, 12 mai 2015, http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[2] *CF Disclosure Guidance: Topic No. 2*, U.S. Securities and Exchange Commission, 13 octobre 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) – *21 Critical Infrastructure Security and Resilience*, U.S. Department of Homeland Security, mars 2013, http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

[4] Le cadre présenté à la figure 2 s'harmonise avec les normes de l'industrie, dont celles du National Institute of Standards and Technology (NIST), de l'Organisation internationale de normalisation (ISO), du Committee of Sponsoring Organizations (COSO) et de l'Information Technology Infrastructure Library (ITIL).

deloitte.ca

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 16-5103T