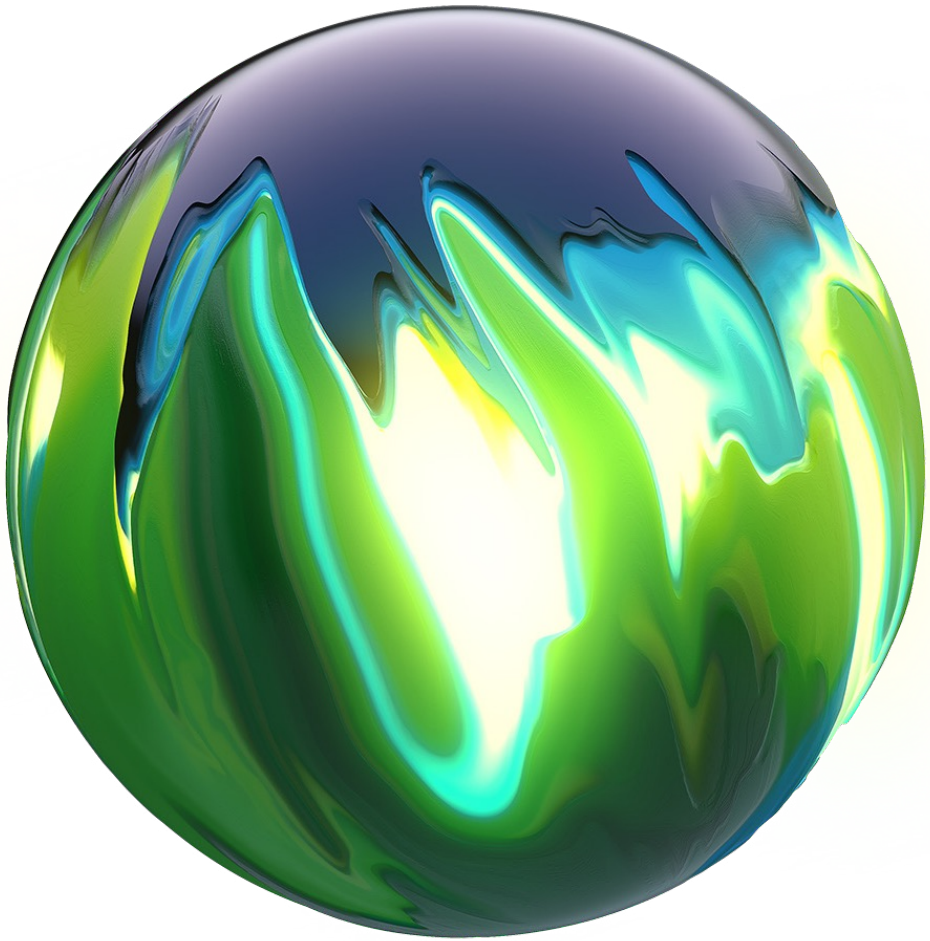
Deloitte.



Prêts pour demain

Préparation au projet de décision de la SEC sur la gestion des risques, la stratégie, la gouvernance et le signalement des cyberincidents

UNE INFLUENCE MARQUANTE depuis 1845

Table des matières

Contexte

La Securities and Exchange Commission (SEC) a proposé des améliorations aux informations à fournir concernant la gestion des risques, la stratégie et les mesures d'intervention en cas de cyberincident dans sa décision, *Cybersecurity Risk Management, Strategy, Governance, and Incident Dosclosure*, publiée le 9 mars 2022[1].

Cette décision s'appuie sur les documents d'interprétation publiés en 2011 et 2018 et fait partie des récents projets de décision de la SEC[2] sur les risques liés à la cybersécurité et aux changements climatiques, entre autres, qui peuvent orienter les priorités actuelles de cybersécurité et être déterminants dans la définition de la stratégie future.

Bien que ce projet de décision impose aux organismes publics un fardeau supplémentaire de conformité, il va de pair avec l'occasion d'adopter de meilleures mesures d'intervention et de reprise, d'améliorer la gouvernance, d'optimiser les programmes de cybersécurité et de mettre en œuvre des mesures intelligentes sécurisées, dont l'économie et les investisseurs seraient susceptibles de tirer parti. Pour saisir ces occasions, les chefs d'entreprises et les dirigeants des organisations de sécurité devraient envisager d'actualiser leurs modèles d'affaires et de façonner leurs futurs produits et services en plaçant la cybersécurité et la gouvernance au centre de leur projet.

Les cyberattaques varient grandement d'une entreprise à l'autre et peuvent comprendre le vol d'actifs financiers, de propriété intellectuelle ou de renseignements confidentiels d'une entreprise (ou de ses clients ou fournisseurs), l'interruption des activités d'une entreprise ou le ciblage d'entreprises qui opèrent dans des secteurs responsables des infrastructures essentielles et de la sécurité nationale, notamment les secteurs de l'énergie et des services publics. Les coûts et les conséquences d'un cyberincident peuvent comprendre des frais de reprise, des pertes de revenus, des litiges, une augmentation des primes d'assurance, une atteinte à la réputation ainsi qu'une réduction de la valeur pour les actionnaires.

Sur près de 600 hauts dirigeants interrogés dans le cadre du sondage *2021 Future of Cyber Survey*[3] réalisé par Deloitte, plus de 72 % ont indiqué que leur organisation a connu entre un et dix incidents ou violations de cybersécurité, en 2020 seulement.

1 Security Exchange Commission, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, communiqué de presse publié le 9 mars 2022.

2 Kruti Modi et al., Deloitte, SEC Proposes New Requirements for Cybersecurity Disclosures, 2022.

3 Deloitte, 2021 Future of Cyber survey, 2021. Ce sondage a permis de recueillir les commentaires de plus de 600 hauts dirigeants dans le monde.

Ce que nous savons du projet de règlement

Les modifications proposées visent à fournir sans délai aux investisseurs des informations plus complètes sur les risques et les incidents importants en matière de cybersécurité, ainsi que sur les questions d'évaluation, de gouvernance et de gestion de ces risques pour les organisations. Elles toucheront toutes les sociétés ouvertes assujetties aux obligations d'information en vertu de la *Securities Exchange Act of 1934*, ainsi que les émetteurs privés étrangers (foreign private issuers) qui sont tenus de mettre à jour le formulaire 20-F.

En résumé, les modifications visent à :

renforcer la confiance des investisseurs dans la gouvernance des organisations en matière de cybersécurité et de signalement des incidents, à réduire la mauvaise évaluation des titres et à faciliter la prise de décision en favorisant l'uniformité dans les déclarations.

améliorer les déclarations actuelles à l'égard des incidents importants liés à la cybersécurité et les informations périodiques sur les politiques et les procédures relatives à la cybersécurité, le rôle de la direction et l'expertise du conseil d'administration dans la mise en œuvre d'un programme sur les risques liés à la cybersécurité.

Qui sera touché?

Tous les types de sociétés inscrites à la SEC seront concernés par le règlement proposé, notamment les sociétés américaines inscrites, les émetteurs privés étrangers, les petits émetteurs (SRC) et les sociétés émergentes en croissance.

Description détaillée du projet de décision

Signalement accéléré
Les informations relatives à un cyberincident doivent être communiquées dans les quatre jours ouvrables qui suivent la détermination de l'importance.

Détermination de l'importance relative
L'importance relative de tout incident doit être déterminée rapidement et avec diligence. L'importance relative sous-entend la modification des informations actuellement disponibles ou ce qui est important pour les actionnaires.

Uniformité dans le caractère spécifique
Les signalements d'incident doivent indiquer le moment de la découverte, la nature et l'ampleur, l'incidence sur les données et sur les opérations, ainsi que les mesures de reprise.

Regroupement important
Signaler les incidents sans importance singuliers ayant une incidence globale importante.

Gestion des risques
Fournir périodiquement les informations sur les politiques et les procédures permettant de repérer les risques et les cybermenaces et de les gérer.

Gouvernance
Fournir périodiquement les informations sur la structure de gouvernance, y compris le rôle de surveillance du conseil d'administration et de la direction concernant les risques liés à la cybersécurité.

Expertise en cybersécurité
Fournir les informations pertinentes si le conseil d'administration de l'entité inscrite dispose d'une expertise en matière de cybersécurité grace à son expérience professionnelle ou à une certification en matière de sécurité.

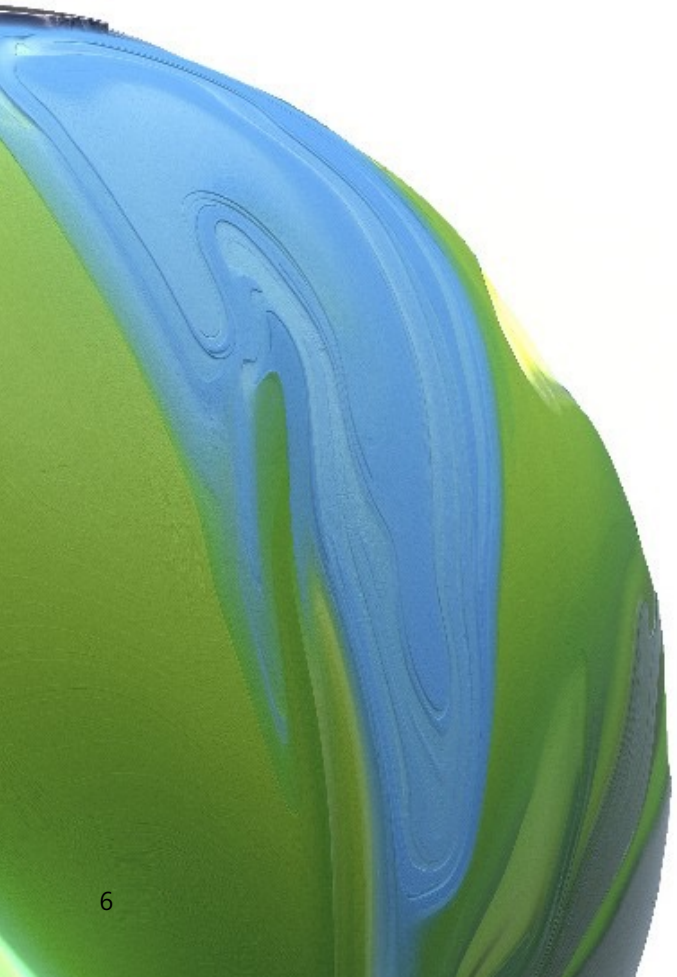
Surveillance par les tiers
Communiquer le processus de sélection et les risques liés à la cybersécurité associés à l'utilisation de tout fournisseur de services tiers.

Peu importe où vous êtes dans votre cyberparcours, nous pouvons vous aider à planifier et à mettre en œuvre en toute confiance une cyberstratégie intégrée favorisant la croissance de votre entreprise grace à l'innovation transformatrice, tout en permettant de vous adapter au contexte réglementaire dynamique.

Favoriser le changement grâce à des mesures planifiées et stratégiques

Bien que le projet de décision ne soit pas définitif, les organisations devraient prendre en considération les meilleures pratiques suivantes pour intégrer leur stratégie d'affaires et de cybersécurité, améliorer la gestion des risques et la gouvernance, et actualiser les processus de gestion des incidents pour suivre l'évolution du contexte réglementaire.

Meilleures mesures d'intervention et de reprise



1. **Définir et mettre en œuvre un cadre de gestion des incidents** comportant des éléments de gouvernance, de stratégie, de technologie, d'opérations, de risques, de conformité et de rétablissement.

2. **Définir, mettre à jour et maintenir des solutions et des plans d'intervention** en cas d'incident en fonction du contexte des cybermenaces.

3. **Établir un modèle de catégorisation des incidents et de classement par ordre de priorité** afin de déterminer leur importance relative selon les informations sur le plan quantitatif et qualitatif.

4. **Définir les processus permettant de mener à bien une analyse de l'incidence** fondée sur les personnes, les processus et les outils technologiques concernés afin de comprendre les coûts et les efforts nécessaires à la reprise.

5. **Examiner et suivre le plan stratégique** des risques pour coordonner le signalement de cyberincidents et de gérer les demandes d'informations aux responsables des relations publiques (établir une capacité de réaction) :

- *Réviser les contrats avec les fournisseurs concernant les obligations de rétablissement et vos polices d'assurance des risques liés à la cybersécurité en vigueur.*
- *Réviser les dispositions du fournisseur de services tiers concernant le signalement des cyberincidents.*

6. **Effectuer fréquemment des cyberexercices interfonctionnels**, tels que des jeux de guerre ou des séances de simulation, afin d'améliorer les délais d'intervention, avec la participation de la haute direction.

7. **Mettre en place une surveillance continue** au moyen de solutions de gestion des informations et des événements de sécurité, de systèmes de surveillance des intrusions, de fils d'actualité de renseignements sur les menaces provenant de diverses sources, y compris de la communauté des services de sécurité et des sources des fournisseurs.

Cybergouvernance et optimisation

1. **Établir une stratégie de cybersécurité** fondée sur les risques en concordance avec la stratégie commerciale et informatique globale.

2. **Définir des politiques, des normes et des procédures de cybersécurité à l'échelle de l'organisation** en concordance avec les objectifs stratégiques et commerciaux.

3. **Définir un cadre de gouvernance et un modèle organisationnel** pour renforcer les capacités en lien avec :

- *La prestation complète des services dans l'ensemble du cadre de cybersécurité;*
- *La participation active de la haute direction et du conseil d'administration à la conduite des activités de gestion des risques comprise dans la stratégie de cybersécurité;*
- *L'expertise du conseil d'administration dans les domaines de la sécurité pour stimuler l'innovation au sein de la fonction de cybersécurité.*

4. **Mettre en place des fonctionnalités internes de cybersécurité** et retenir les services de tiers afin de renforcer les capacités de cybersécurité, au besoin.

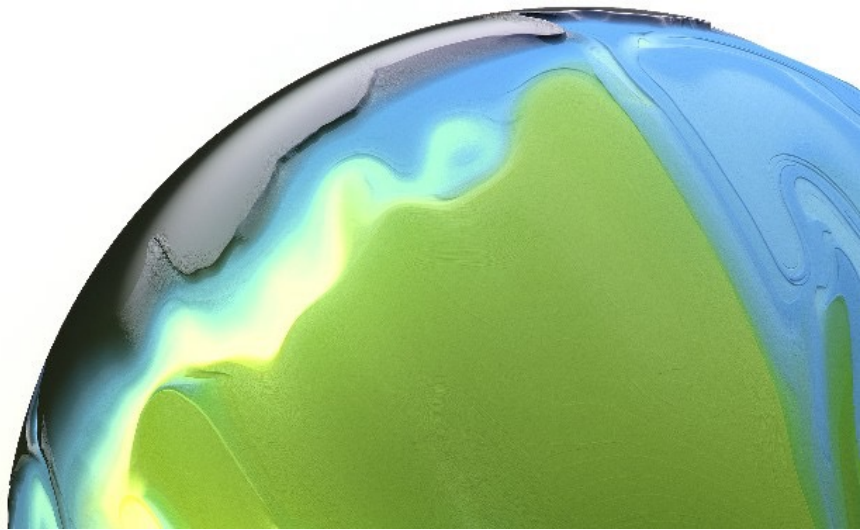
5. **Définir le poste du chef de la sécurité de l'information** ou un poste équivalent de la personne qui sera responsable de la stratégie, de la mise en œuvre et du suivi de la cybersécurité au sein de l'organisation.

6. **Instaurer une discipline de gestion des risques liés à la cybersécurité :**

- *Faire participer activement le conseil d'administration à l'examen périodique des risques pour les infrastructures essentielles;*
- *Définir et mettre en œuvre des méthodologies d'évaluation des risques pour soutenir le cycle de vie de la gestion des risques;*
- *Obtenir une visibilité des risques émanant de l'organisation élargie (par exemple, des tiers, des fournisseurs, des sous-traitants) grace à une analyse améliorée et à une attention particulière portée aux tiers essentiels et à risques élevés;*
- *Définir des stratégies d'atténuation des risques, y compris les assurances des risques liés à la cybersécurité;*
- *Intégrer la gestion des risques liés à la cybersécurité à la fonction de gestion des risques de l'entreprise.*

7. **Définir et adopter les tolérances aux risques** en déterminant l'appétit au risque de cybersécurité de l'organisation; valider sans délai cette donnée auprès des parties prenantes pour une intervention simplifiée à leur égard.

8. **Définir les paramètres des risques et une structure de signalement** afin de fournir des mises à jour périodiques sur la gestion des risques à des publics internes et externes, avec des fonctionnalités automatisées de regroupement et de visualisation des données.



Que pouvez-vous faire?

Les organisations doivent se préparer à un avenir caractérisé par une plus grande transparence de leur programme de gouvernance de la cybersécurité et par une approche simplifiée de signalement des incidents qui continue à inspirer la confiance des investisseurs. L'attention accordée au maintien des prouesses techniques et de l'expertise en matière de cybersécurité dans une organisation, sous la direction du conseil d'administration et de la direction, leur permet de mieux se positionner pour renforcer les relations avec les investisseurs, les clients, les partenaires et les employés, et favorise la souplesse et la résilience pour exploiter les atouts de la révolution numérique.

Aspects clés

Maintenant

Investir dans un bassin de candidats : acquérir une expertise au niveau des cadres et du conseil d'administration ainsi que des talents possédant des compétences clés et émergentes en cybersécurité, et investir dans ces derniers, afin de jeter les bases d'une solide organisation en matière de cybersécurité.

Comprendre votre état de préparation pour le signalement : explorer les programmes de détection des menaces, de surveillance et de réponse les mieux adaptés pour répondre à vos exigences de conformité en matière de signalement des incidents afin de générer des gains d'efficacité et de respecter votre budget.

Améliorer votre cadre de politiques et de procédures : rationaliser vos exigences réglementaires pour élaborer et maintenir un cadre de contrôle intégré, et des politiques et procédures pour répondre aux exigences réglementaires et refléter l'apprentissage et la sensibilisation par l'expérience et la situation.

Plus tard

Passer de la réaction à la résilience dans votre entreprise étendue : développer des outils d'évaluation des risques qui regroupent de l'information interne et externe sur les tiers afin de rationaliser la gestion des risques liés à ces derniers, et investir dans ces outils.

Adopter une attitude d'évaluation continue : intégrer les capacités techniques et d'affaires pour favoriser la gestion après les incidents, y compris l'analyse des regroupements d'incidents qui peut fournir des observations et des occasions d'optimisation.

Passer du risque numérique à l'avantage numérique : mener des efforts ciblés sur l'analytique, l'intelligence artificielle et l'automatisation afin d'accélérer la détection des menaces, renforcer et accroître le confinement et l'intervention en cas d'incident et favoriser l'adoption d'une posture de sécurité proactive.

Personnes-ressources

Nous contribuons à la protection de votre entreprise en vous fournissant les technologies nécessaires pour sécuriser votre cyberdomaine, en permettant l'exécution d'opérations sécurisées et intelligentes et en vous fournissant une main-d'œuvre efficace qui peut travailler pour vous. Ainsi, nous vous aidons à poursuivre vos activités tout en vous permettant de faire preuve d'agilité et de modernisation.

Amir Belkhelladi
Leader national – Cybersécurité
514 214-2336
abelkhelladi@deloitte.ca

Louis-Philippe Desjardins
Directeur principal – Services liés aux cyberrisques
514-390-0938
lodesjardins@deloitte.ca

Vignesh Krishnamoorthy
Associé – Services liés aux cyberrisques
416 435-5472
vigkrishnamoorthy@deloitte.ca

La voie à suivre : comment le groupe de cybersécurité de Deloitte peut vous aider

Deloitte aide les entreprises clientes à concevoir, à établir et à mettre en application des programmes de sécurité dynamiques et adaptés à leurs besoins à chaque étape de leur cyberparcours. Vous pouvez être assurés d'être bien équipés pour répondre aux exigences, tout en continuant à vous concentrer sur ce que vous faites le mieux : gérer votre entreprise.

Leadership à l'échelle mondiale : Deloitte a été désigné leader mondial en matière de services-conseils dans le domaine de la sécurité et de l'intervention en cas de cyberincident. Nous offrons un leadership distinctif dans le domaine et une solide expérience sectorielle.

Écosystèmes et alliances : nous avons forgé de solides alliances avec des fournisseurs de technologies de pointe, des organisations sectorielles et des entités de recherche afin de fournir des pistes de réflexion et des renseignements de premier plan et de favoriser le partage de l'information et la collaboration.

Quantification des risques liés à la cybersécurité : grâce à l'intégration des données et à des modèles statistiques conçus sur mesure pour la quantification des risques, nous aidons les organisations à bonifier leur expérience à l'aide des outils technologiques afin de développer des interventions en fonction de l'évaluation des risques.

Outils technologiques avancés de cybersécurité : les technologies émergentes que nous utilisons facilitent l'intégration des risques liés à la cybersécurité grâce à une transition sécurisée vers des technologies et des environnements de nouvelle génération.

Services de cybersécurité de Deloitte

Habiliter vos gens pour l’avenir

L’importance que nous accordons aux relations personnelles, à l’étendue et à la profondeur de notre expérience ainsi qu’à l’innovation à l’égard des technologies et des produits nous permet de réunir des parties prenantes pour accroître l’interopérabilité et l’incidence.

Quelles que soient les priorités d’affaires stratégiques de votre organisation, nous vous aiderons à améliorer votre sensibilisation aux menaces ainsi que votre visibilité à cet égard et à renforcer votre capacité à prospérer malgré les cyberincidents.

Peu importe la complexité de votre situation, nous serons toujours à votre écoute et nous continuerons de travailler avec vous pour répondre à vos questions et trouver les bonnes réponses à vos besoins uniques.

Deloitte.

À propos de Deloitte

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500 MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes.

Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 12 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.

Designed and produced by the Agency | Deloitte Canada. 22-6035103