IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

Principes fondamentaux de la gestion du risque technologique

TABLE DES MATIÈRES

Sommaire

Qui devrait lire le présent guide?

Le guide s'adresse principalement aux PME membres de l'OCRCVM.

Les sociétés sont-elles tenues de suivre le présent guide?
Non, elles ne le sont pas. Le guide fournit de l'information utile aux sociétés membres de l'OCRCVM qui souhaitent élaborer un programme de gestion du risque technologique.

Qu'apprendrez-vous?
Dépendre de façon importante de la technologie vient avec son lot de risques pour les sociétés, notamment en ce qui a trait à la sécurité et à la confidentialité, à l'intégrité et à l'exactitude, à la durabilité et à la disponibilité, et à l'efficacité et à l'efficience. Si elles veulent améliorer leur résilience opérationnelle, les sociétés doivent gérer le risque technologique dans toutes ses dimensions.

Y a-t-il des points importants à prendre en considération?
La gouvernance est au cœur d'une gestion efficace du risque technologique. Les personnes responsables de la gouvernance devraient travailler en collaboration avec l'équipe de direction à l'élaboration et à la supervision de la stratégie technologique et du programme de gestion du risque technologique de la société.

1. Comment utiliser le guide

Le présent guide a été élaboré en tant que document général, à la suite de recherches indépendantes, de discussions et de consultations menées auprès de diverses sociétés membres[1]. Son objectif est d'aider principalement les PME membres de l'OCRCVM à prendre les premières mesures visant à évaluer et à gérer le risque technologique. Pour les grandes sociétés membres, la gestion du risque technologique est généralement intégrée dans un cadre en bonne et due forme de gestion des risques d'entreprise (GRE) qui comprend une fonction d'audit interne pour valider la gouvernance, les risques et les contrôles de la société.

Le guide décrit les principes généraux de la gestion des risques et certains contrôles recommandés, maisil ne dicte pas de cadre ou de règle que les sociétés membres doivent suivre. Les sociétés membres devraient donc envisager de faire appel aux services d'experts en gestion des risques en général et en

[1] Le Groupe consultatif sur la cybersécurité et la technologie (GCT) est un regroupement de cadres et de professionnels de la technologie et de la sécurité triés sur le volet, en provenance de diverses PME membres de l'OCRCVM dans tout le pays.

gestion du risque technologique en particulier pour concevoir et mettre en œuvre un plan de gestion adapté aux circonstances, au modèle d'affaires et aux parties intéressées propres à leurs activités.

Pour plus d'informations sur certains cadres de gestion du risque technologique largement acceptés, veuillez vous reporter à l'annexe A, « Guides et références ».

2. Aperçu

La définition de la technologie et de ce qu'elle englobe ne cesse d'évoluer. Dans sa forme la plus élémentaire, la technologie comprend les éléments suivants :

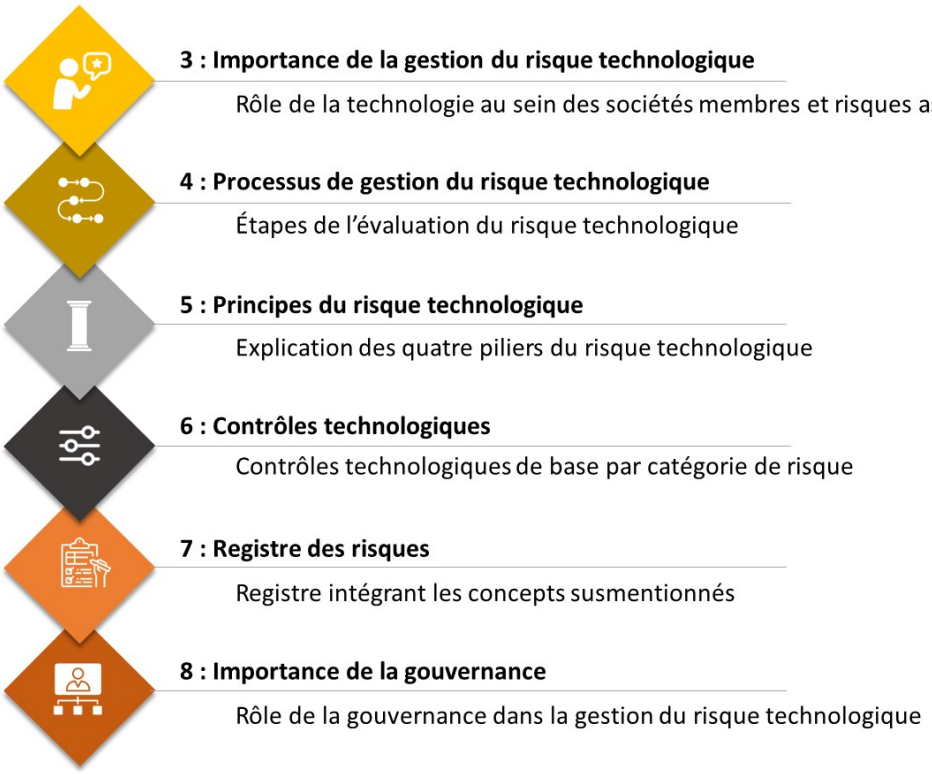
- Les réseaux, dispositifs et infrastructures;
- Les logiciels et applications;
- Les données et informations, y compris la technologie utilisée pour stocker et protéger les informations;
- Les ressources humaines telles que les développeurs, les utilisateurs, le personnel de soutien et toutes les autres personnes participant au fonctionnement et à l'exploitation de la technologie;
- Les processus, c'est-à-dire les procédures automatisées et manuelles qui interviennent dans le fonctionnement de la technologie.

Le risque technologique correspond au risque commercial associé au déploiement de la technologie et de l'automatisation dans une entreprise, et à la dépendance qui s'ensuit. S'il n'est pas adéquatement géré, il peut représenter un risque commercial important et potentiellement nuire grandement à la société et à sa viabilité future.

Bien que l'OCRCVM n'ait pas de règles particulières en tant que telles concernant la gestion du risque technologique, l'utilisation de la technologie pourrait avoir un impact sur le respect des règles de l'OCRCVM par une société membre. De plus, le Service de la conformité des finances et des opérations (la CFO) de l'OCRCVM effectue actuellement une évaluation globale du risque technologique des sociétés membres et l'intègre dans leur cote de risque globale[2].

[2] Le modèle d'évaluation des risques de la CFO intègre plusieurs facteurs en prenant en ligne de compte l'ensemble du secteur. Une modification dans l'évaluation des risques associés à un seul facteur n'a pas nécessairement d'incidence sur la cote de risque définitive d'une société membre établie par la CFO.

Le guide aborde les principes généraux de la gestion du risque technologique dans les sections suivantes :



3. Importance de la gestion du risque technologique

Toutes les sociétés membres de l'OCRCVM dépendent de la technologie et de l'automatisation sous une forme ou une autre. La technologie peut revêtir un caractère essentiel et contribuer à compenser les risques traditionnellement associés à l'intervention manuelle de nombreuses manières, notamment celles-ci :

- Amélioration de l'expérience du client;
- Accroissement de l'efficacité;
- Augmentation de l'exactitude;
- Réduction des coûts;
- Renforcement de l'engagement des employés.

Toutefois, la dépendance à l'égard de la technologie comporte son propre ensemble de risques. Les sociétés membres abordent habituellement les risques liés à l'utilisation de la technologie au cas par cas, autrement dit en mettant en œuvre des contrôles propres aux applications ou aux processus. Cette solution à elle seule, c'est-à-dire l'absence de plan de gestion du risque technologique, n'est généralement plus suffisante pour les raisons suivantes :

- La prédominance de l'automatisation et de la technologie dans tous les aspects des affaires et la dépendance qui en découle, ainsi que l'interdépendance et l'interconnectivité des technologies;
- L'essor des mégadonnées;
- L'élaboration de nouvelles règles et de nouveaux règlements en matière de protection de l'information et de la vie privée;
- L'évolution et la prolifération des cybermenaces;
- L'adoption des technologies nuagiques;
- L'accélération de l'adoption des technologies et de l'automatisation en raison de la pandémie, ce qui comprend la mise en place du travail à domicile et des services d'accès à distance, les technologies de communication, ainsi que l'acceptation et la livraison électroniques des documents.
- L'expansion des grandes entreprises et des fournisseurs du secteur de la technologie financière qui offrent des services et des solutions technologiques sous diverses formes (plateformes en tant que service ou PaaS, logiciels en tant que service ou SaaS, etc.).

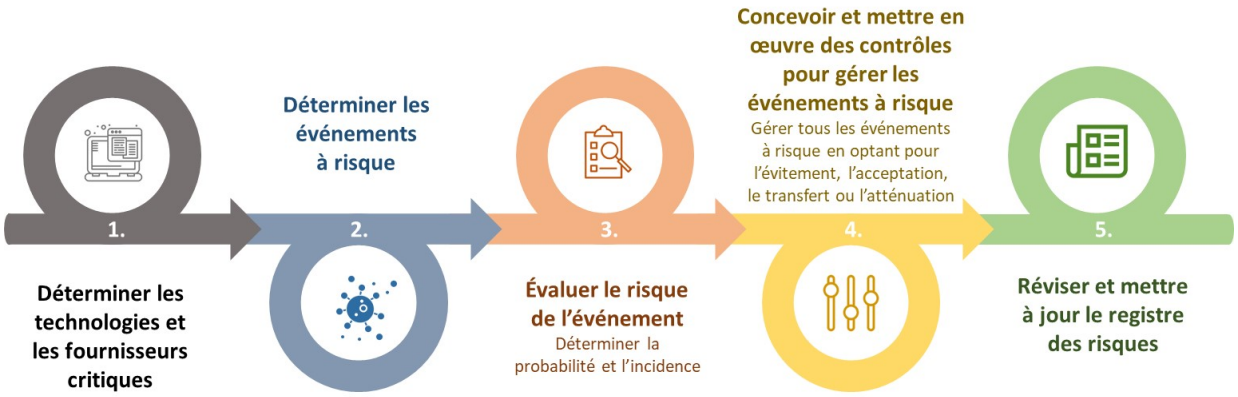
La gestion du risque technologique peut être vitale pour la survie d'une société. À ce titre, toutes les sociétés membres devraient envisager d'élaborer un plan de gestion du risque technologique qui tient compte de leur modèle d'affaires unique et de leurs parties intéressées, et donc de la meilleure façon de gérer les risques. Grâce à un plan efficace de gestion en la matière, les sociétés membres pourront se concentrer sur les principaux changements à apporter afin de réduire de manière importante leur exposition globale aux risques.

4. Processus de gestion du risque technologique[3]

Le risque technologique est généralement considéré comme un risque non financier ou comme une composante du risque opérationnel. Contrairement aux risques financiers (p. ex., risque de crédit, risque de marché, etc.) – où les sociétés peuvent choisir leur niveau d'exposition –, le risque technologique ne peut être éliminé.

[3] Bien que cette section traite spécifiquement de la gestion du risque technologique, le processus peut également être utilisé pour gérer tous les autres types de risques au sein de la société membre.

En général, les sociétés membres devraient envisager de mettre au point un processus de gestion des risques :



Un processus efficace englobe non seulement le personnel chargé de la technologie, des risques ou de la conformité, mais aussi tous les membres de l'organisation. En effet, ce sont ces derniers qui utilisent la technologie, qui connaissent le mieux son fonctionnement et qui s'y fient pour accomplir leurs tâches. En définitive, les sociétés devraient envisager de faire examiner les risques et les contrôles par la haute direction et le conseil d'administration pour s'assurer que la technologie et les fournisseurs critiques, ainsi que les événements à haut risque, sont déterminés, évalués avec précision et gérés de manière appropriée.

Dans l'exécution de ce processus, il est important d'être réaliste et pratique :

- Trop d'optimisme à l'égard des hypothèses rend l'exercice infructueux et exposera la société membre, les clients et les autres parties intéressées à des événements à haut risque. En revanche, un pessimisme trop marqué empêchera la société d'établir des priorités efficaces et efficientes pour la gestion des événements à haut risque.
- L'atténuation ou l'élimination complète du risque n'est pas possible en raison de l'omniprésence et de l'enracinement de la technologie et de l'automatisation dans les activités commerciales. L'objectif réalisable, c'est la gestion du risque, c'est-à-dire la réduction de l'incidence ou de la probabilité d'un événement à haut risque à un niveau que la société peut tolérer[4].

4.1 Déterminer les technologies et les fournisseurs critiques

La première étape consiste à dresser une liste de toutes les technologies utilisées à l'interne, à savoir qui et quel secteur d'activité les utilisent, et dans quel but. Cela permettra de déterminer les technologies

[4] Les principes généraux de la gestion des risques imposent aux entreprises de déterminer leur tolérance et leur appétit pour le risque afin de gérer efficacement les risques. Il s'agit d'une exigence distincte de celle de l'OCRCVM, qui impose à toutes ses sociétés membres de fixer des limites fondées sur le CRFR pour les fonctions et activités importantes qui utilisent du capital ([articles 4112 à 4116 des Règles de l'OCRCVM]).

critiques employées dans la société et sur lesquelles la société compte, ce qui est une première étape essentielle. Voici certains des aspects que les sociétés peuvent prendre en considération :

a. Le personnel du secteur d'activité et le personnel technologique doivent dresser la liste des technologies afin d'inventorier toutes celles qui sont utilisées par la société. Voir l'annexe B pour un résumé des applications pour lesquelles la technologie est généralement utilisée dans le secteur des placements.

b. Pour une gestion efficace du risque, cette première étape devrait également permettre de répondre aux questions suivantes :

    i. Comment la société accède-t-elle à la technologie? Par exemple, est-ce que la société membre la développe elle-même, est-ce qu'elle utilise une étiquette blanche/licence directe, ou est-ce qu'elle y accède par l'intermédiaire d'un fournisseur?

    ii. Quelle est la technologie sous-jacente?

4.2 Déterminer les événements à risque

L'étape suivante consiste à déterminer les événements à haut risque, c'est-à-dire ceux qui pourraient être néfastes – et la manière dont ils pourraient être néfastes – en dressant une liste des menaces et des vecteurs de menace (voir la section 5). Posez-vous ces questions :

a. Qu'est-ce qui pourrait mal tourner? (ce qui revient à déterminer les menaces) – Il s'agit de dresser la liste des incidents potentiels qui pourraient rendre la technologie, le fournisseur ou ses extrants non fiables, indisponibles, non sécurisés ou inefficaces.

b. Comment cela pourrait-il mal tourner? (ce qui revient à déterminer les vecteurs et les acteurs de la menace) – Il s'agit de dresser la liste des manières dont les incidents potentiels pourraient se produire. Il peut être utile de les classer par catégorie selon qu'il s'agit de menaces internes ou externes, et de pousser l'analyse plus loin, pour déterminer si elles sont de nature accidentelle ou intentionnelle. Tout contrôle conçu dépendra alors de la source de la menace.

Les sociétés membres qui se lancent dans ce processus trouveront peut-être utile de dresser une liste des menaces possibles avec les utilisateurs du secteur d'activité concerné et le personnel technologique. Cette mesure peut permettre de relever les événements à risque comportant une incidence plus grande et une probabilité plus élevée.

4.3 Évaluer le risque associé à l'événement

Les sociétés membres devraient envisager d'évaluer la gravité des événements à risque sous l'angle de leur probabilité et de leur incidence. Cela permet de relever les événements à risque qui nécessitent l'attention la plus urgente. Notez que cette évaluation sera différente pour chaque société en fonction de sa structure, de son modèle d'affaires, de ses parties intéressées et de ses objectifs stratégiques.

4.3.1 Probabilité

Dans l'évaluation de la probabilité d'un événement, il est utile d'envisager les différents niveaux de probabilité possibles. Par exemple, la probabilité qu'un événement se produise pourrait être :

- très faible;
- peu élevée;
- moyenne;
- élevée;
- très élevée.

4.3.2 Incidence

Dans l'évaluation d'un événement, il est également utile d'envisager les différents niveaux d'incidence possibles. Par exemple, si l'événement devait se produire, son incidence pourrait être :

- insignifiante;
- mineure;
- modérée;
- majeure;
- considérable/importante.

En conséquence, la société doit déterminer qui serait touché ainsi que la nature et l'ampleur de l'incidence :

- Qui serait touché?

  Quelles sont les parties intéressées qui dépendent de la technologie ou de ses extrants – par exemple, quels sont les employés, les services ou les fonctions commerciales, les clients, les organismes de réglementation, les relations de service, etc. qui seraient touchés si le risque se concrétisait?

- Quelle serait l'incidence sur les activités?

  Quel serait le coût de l'événement à risque pour la société membre s'il devait se produire? Exemples d'incidences possibles :

  - perte de revenus/de clients;
  - arrêt des activités;
  - coûts financiers de la reprise/ de l'intervention/du remplacement/ des mesures correctives/du redressement,
  - perte de réputation;
  - responsabilité civile ou contractuelle (p. ex., en raison du non-respect des délais ou de

l'incapacité à remplir les obligations de prestation de services),

- conformité et responsabilité réglementaire.

4.4 Concevoir et mettre en œuvre des contrôles pour gérer les événements à risque

Une fois que la probabilité et l'incidence des événements à risque ont été déterminées, l'étape suivante consiste à les trier par ordre décroissant, des événements ayant la plus grande probabilité et la plus grande incidence à ceux jugés comme ayant la plus faible probabilité et la plus faible incidence. De même, les contrôles visant à gérer les événements à risque seront priorisés de manière à ce que :

a. les événements à risque dont l'évaluation combinée révèle une probabilité et une incidence élevées – autrement dit, qui posent un risque technologique majeur pour la société – deviendront le principal point de mire pour la conception et la mise en œuvre de contrôles suffisants et appropriés;

b. les événements à risque dont l'évaluation combinée révèle une probabilité et une incidence faibles feront quant à eux l'objet d'une attention et de ressources moindres. Il se peut qu'il ne soit pas nécessaire de se concentrer sur les contrôles, si ce n'est pour veiller à ce que la probabilité et l'incidence évaluées soient exactes et n'aillent pas en grandissant.

Pour chacun de ces événements, la technique générale que les sociétés membres devraient envisager pour gérer le risque est l'une des suivantes : éviter, accepter, transférer ou atténuer le risque.

- **Évitement**

  Cette technique préconise d'éviter la technologie ou de s'en défaire si la probabilité associée à un événement est élevée ou moyenne et si son incidence est majeure ou importante. N'oubliez pas qu'il peut être difficile et onéreux d'éliminer une technologie qui a été entièrement mise en œuvre ou qui est utilisée depuis un certain temps. Dans de tels cas, l'acceptation pourrait être une meilleure solution.

- **Acceptation**

  Cette technique signifie ne rien changer ou ne rien faire. Il s'agit d'une option viable lorsque la société évalue la probabilité de l'événement comme étant très faible ou peu élevée, et que l'incidence est insignifiante ou mineure.

- **Transfert**

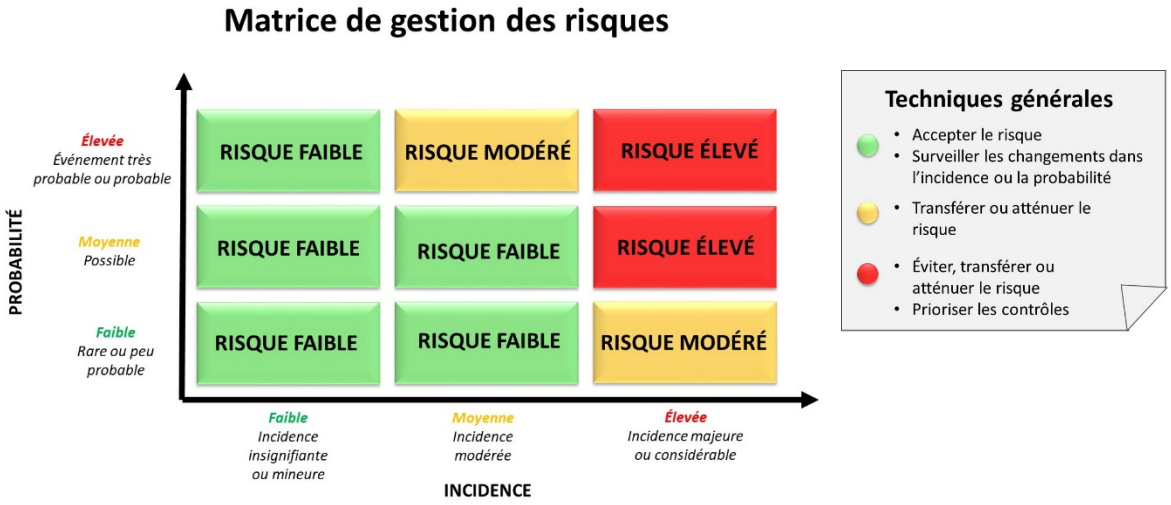
  Cette technique consiste à partager le risque avec une autre partie ou à le transférer à une autre partie . On peut transférer le risque au moyen d'une police d'assurance ou en ayant recours à l'impartition. Il convient de noter que le transfert du risque entraîne des coûts qui, en soi, peuvent rendre ce recours insuffisant. De plus, certains risques, tels que les risques réglementaires, juridiques, de conformité et d'atteinte à la réputation, peuvent ne pas être transférables.

- **Atténuation**

  Cette technique consiste à concevoir et à mettre en œuvre des contrôles généraux et particuliers pour réduire la probabilité ainsi que l'incidence d'un événement à risque. Dans les cas où l'acceptation, l'évitement ou le transfert sont des recours insuffisants ou impossibles, des contrôles doivent être mis en œuvre pour gérer un événement particulier à risque plus élevé.

4.4.1 Matrice de gestion des risques

Même s'il existe plusieurs méthodes selon la taille de l'organisation et le nombre de secteurs d'activité, la matrice suivante illustre la façon dont un événement à risque donné peut être géré en règle générale.



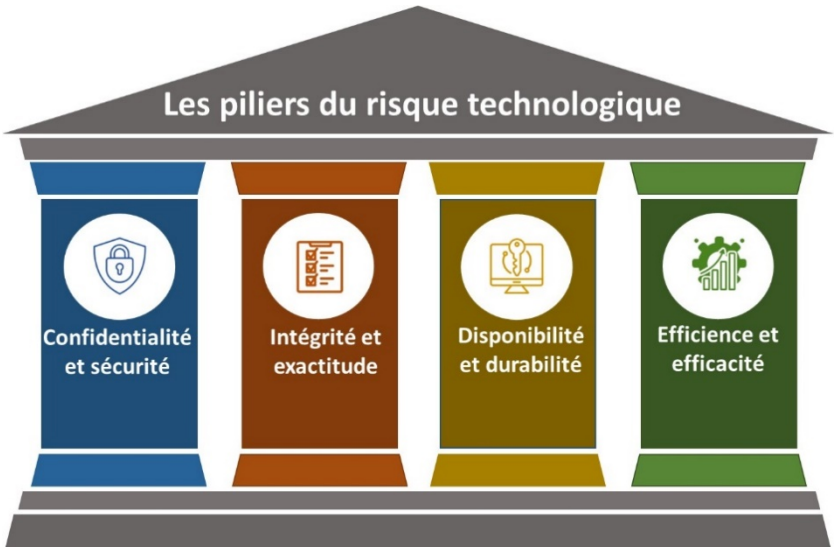
4.5 Réviser et mettre à jour le registre des risques

Les sociétés membres devraient envisager de compiler la liste de tous les événements à risque, les évaluations du risque et les contrôles dans un document ou un « registre des risques », tout en veillant à ce que celui-ci soit régulièrement révisé et mis à jour. La fréquence de la révision dépend du modèle d'affaires de la société, de ses caractéristiques et de l'introduction éventuelle de changements importants dans les technologies de l'information. Voir la section 7 pour plus d'informations.

5. Principes du risque technologique

Durant la mise en œuvre d'un plan de gestion du risque technologique et la réflexion sur les événements à risque, il importe de comprendre les principes du risque technologique.

Ainsi, les quatre piliers du risque technologique à prendre en ligne de compte sont : la confidentialité et la sécurité, l'intégrité et l'exactitude, la disponibilité et la durabilité, de même que l'efficience et l'efficacité.



5.1 Confidentialité et sécurité

La *confidentialité* fait référence à la nécessité de désigner les informations sensibles et d'en renforcer la protection tout au long de leur cycle de vie, c'est-à-dire depuis leur collecte ou leur création jusqu'à leur élimination finale et leur retrait du contrôle de l'entité. La confidentialité se distingue de la protection de la vie privée en ce sens que cette dernière s'applique aux informations expressément protégées par la législation sur la vie privée et assujetties à celle-ci – par exemple, les informations personnelles identifiables. Aux fins des présentes, la protection de la vie privée et la confidentialité sont traitées comme des synonymes.

La *sécurité* fait référence à la nécessité d'une protection globale des informations et des technologies contre l'accès non autorisé, la divulgation inappropriée et d'autres dommages qui pourraient compromettre leur disponibilité, intégrité, confidentialité ou caractère privé.

5.2 Intégrité et exactitude

L'*intégrité et l'exactitude* font référence à la nécessité, pour les traitements système, les services des fournisseurs et les données, d'atteindre le but ou l'objectif pour lequel ils ont été mis en œuvre, acquis en vertu d'un contrat ou bien recueillis, selon le cas. Cela signifie qu'il faut garantir l'exhaustivité, la validité, l'exactitude, le caractère opportun et la conformité du traitement ou des extrants générés.

5.3 Disponibilité et durabilité

La *disponibilité et la durabilité* font référence à l'importance d'un accès continu et à la nécessité que la technologie ou ses extrants, ainsi que les services des fournisseurs, restent disponibles tels qu'ils ont été conçus ou acquis en vertu d'un contrat. La disponibilité et la durabilité incluent également la capacité à se remettre des événements à risque applicables.

5.4 Efficience et efficacité

L'efficience fait référence à la nécessité pour la technologie ou le fournisseur de produire le résultat souhaité en temps utile et à moindre coût.

L'efficacité fait référence à la nécessité pour la technologie ou le fournisseur d'offrir la meilleure solution possible pour atteindre les buts et objectifs stratégiques de la société.

Il convient d'évaluer l'efficacité d'une technologie ou d'un fournisseur avant de déterminer son efficience.

6. Contrôles technologiques

La présente section met en évidence certains aspects clés. On pourra les prendre en considération, selon le cas, pour les principales catégories de risque[5] technologique et pour mettre en place certains contrôles de base applicables lorsqu'un aspect est jugé comme étant à forte probabilité et à incidence élevée. La liste des contrôles dans la présente section n'est pas exhaustive. Les sociétés membres doivent concevoir et mettre en œuvre des contrôles personnalisés en tenant compte de leur modèle d'affaires unique, de leur stratégie et de leur propre évaluation des risques.

6.1 Information et gestion des données

Cet aspect concerne certains contrôles de base s'appliquant aux informations recueillies, créées, traitées ou stockées et éliminées. Les quatre piliers du risque technologique s'appliquent à l'élaboration de contrôles relatifs à la gestion des informations et des données, particulièrement des données déterminées comme étant essentielles et confidentielles.

Contexte	Contrôles
INVENTAIRE DES INFORMATIONS	
De quoi s'agit-il? *Relever toute interaction avec des données essentielles et confidentielles, et déterminer où résident ces données.* Pourquoi est-ce important?	➢ Cerner tous les points de contact au sein de la société avec les données, c.-à-d. où les informations sont recueillies, créées, traitées, utilisées ou stockées. ➢ Tenir et passer en revue un journal détaillant les différents types de données stockées (p. ex., emplacement des bases de données et des

[5] Consultez le Guide de pratiques exemplaires et le Guide de cybergouvernance de l'OCRCVM pour obtenir des conseils plus détaillés sur la gestion des risques de sécurité.

Contexte	Contrôles
• *Pour garantir qu'il n'y a pas de données confidentielles ou privées dont la sécurité et la protection sont négligées par inadvertance.* • *Pour assurer le respect de la législation sur la protection de la vie privée.*	serveurs, des centres de données en nuage, des dossiers partagés, des clés USB, des documents papier). ➢ Établir et consigner le processus de traitement des demandes de renseignements et des plaintes relatives à la protection de la vie privée. ➢ Veiller à ce que le traitement des informations confidentielles et privées soit conforme à l'ensemble de la réglementation en vigueur en matière de protection de la vie privée, ce qui peut inclure la transmission d'une notification claire aux clients et aux personnes sur l'utilisation, le traitement et le stockage de leurs informations personnelles, ainsi que l'obtention du consentement lorsque la loi l'exige[6].
GESTION DES ACCÈS[7]	
De quoi s'agit-il? *Restreindre l'accès à l'information sur la base du principe du moindre privilège, c.-à-d. que l'accès à la technologie et à l'information doit être limité à ce qui est nécessaire à la personne pour accomplir son travail.* Pourquoi est-ce important? • *Pour se protéger contre une violation des identifiants de connexion d'un utilisateur.* • *Pour limiter l'impact d'une violation, accidentelle ou intentionnelle, des identifiants de connexion d'un utilisateur.*	➢ Créer des politiques de hiérarchie des utilisateurs détaillant les exigences d'accès et les approbations requises. ➢ Contrôler l'accès des utilisateurs jouissant de droits élevés et inclure des alertes de surveillance lorsqu'un compte d'administrateur est ajouté ou supprimé. ➢ Accorder, supprimer ou modifier l'accès en temps utile dans le cadre du processus d'accueil et de départ de l'utilisateur. ➢ Mettre en œuvre des politiques strictes de gestion des mots de passe, notamment en ce qui concerne leur complexité, leur réutilisation et les

[6] Au Canada, la réglementation en matière de protection de la vie privée est régie par la *Loi sur la protection des renseignements personnels et les documents électroniques* (la LPRPDE), telle que modifiée par la *Loi sur la protection des renseignements personnels numériques.* S'ajoutent également au paysage législatif les lois provinciales sur la protection des renseignements personnels dans le secteur privé en Colombie-Britannique, en Alberta et au Québec.

[7] Ces contrôles sont liés à la gestion des appareils et à la gestion des systèmes et applications.

Contexte	Contrôles
	limites dans le nombre de tentatives de connexion. ➢ Examiner les droits d'accès à intervalles réguliers pour chaque dispositif, système ou application, y compris pour les comptes inactifs, en surveillant les tentatives d'accès anormales ou irrégulières, ainsi que les comptes désactivés. ➢ Vérifier l'authenticité des utilisateurs qui se connectent aux applications à intervalles réguliers. ➢ Imposer l'authentification à plusieurs facteurs, le verrouillage des écrans, la déconnexion temporisée et d'autres mesures d'authentification pour l'accès aux données confidentielles. ➢ Chiffrer les fichiers de données qui stockent les mots de passe.
PRÉVENTION DES PERTES DE DONNÉES	
De quoi s'agit-il? *Déterminer et protéger les informations essentielles et confidentielles.* Pourquoi est-ce important? • *Pour garantir que les données confidentielles et privées sont toujours traitées de manière sûre.* • *Pour aider les sociétés membres à sécuriser les données confidentielles et privées de la manière la plus efficace (c.-à-d. sur le plan des coûts, du temps et des ressources).* • *Pour assurer le respect de la législation sur la protection de la vie privée.* • *Pour limiter l'impact d'une violation des données.*	➢ Établir des politiques pour la reconnaissance et le classement des données essentielles et confidentielles (soit les informations permettant d'identifier une personne), ainsi que pour la sauvegarde, la conservation et la récupération des programmes et des données d'application. ➢ Suivre les mouvements de données essentielles et confidentielles à l'intérieur et à l'extérieur de la société. ➢ Créer et mettre en œuvre une politique de conservation des données. ➢ Former en permanence les utilisateurs pour qu'ils comprennent comment traiter les informations confidentielles en toute sécurité.

Contexte	Contrôles
INTÉGRITÉ DES DONNÉES	
De quoi s'agit-il? *Garantir l'exactitude et l'exhaustivité des informations produites.* Pourquoi est-ce important? • *Pour assurer la fiabilité des données nécessaires aux fonctions clés.* • *Pour garantir qu'une défectuosité technologique ou un extrant incorrect peut être détecté et corrigé.*	➢ Établir des procédures d'examen des rapports produits pour en garantir l'exactitude. ➢ Mettre en place des structures de responsabilité et de reddition de comptes afin de déterminer qui est responsable de l'exactitude et de l'exhaustivité des rapports lorsque d'autres sociétés ou fonctions s'appuient sur l'intégrité des rapports pour s'acquitter de leurs responsabilités[8].
SURVEILLANCE DES MENACES	
De quoi s'agit-il? *Surveiller les activités malveillantes et les menaces.* Pourquoi est-ce important? • *Pour détecter les tentatives extérieures d'accès non autorisé aux technologies ou données et protéger celles-ci.* • *Pour détecter les attaques d'initiés malveillants.* • *Pour permettre aux sociétés de réagir rapidement aux attaques et d'en limiter les dommages et l'impact.*	➢ Surveiller les opérations anormales, notamment les opérations inhabituelles des utilisateurs, le comportement des utilisateurs (p. ex., de gros volumes de téléchargement et de diffusion média en continu), l'activité du réseau et des systèmes (p. ex., volume élevé de trafic réseau, tentatives de connexion infructueuses, connexions après les heures de travail) et d'autres activités irrégulières. ➢ Établir et mettre en œuvre une politique de collecte, d'analyse, de suivi et d'examen des renseignements sur les événements de sécurité ainsi que des journaux d'audit. ➢ Maintenir un groupe ou une division en activité 24 heures sur 24, 7 jours sur 7 et qui sera chargé des services de sécurité.

[8] Les personnes inscrites auprès de l'OCRCVM qui ont des responsabilités réglementaires désignées, telles que les surveillants, les directeurs financiers, les chefs de la conformité, etc. doivent comprendre leur rôle dans la structure de responsabilité et de reddition de comptes de la société, pour s'assurer que les informations sur lesquelles ils se fondent sont exactes et complètes.

Contexte	Contrôles
	➢ Surveiller la situation sur le plan des menaces, notamment en s'abonnant à des services d'information à ce sujet.

6.2 Gestion des appareils

Cet aspect concerne certains contrôles de base relatifs à la gestion du matériel et des dispositifs utilisés pour mener les diverses activités et les opérations de la société membre. La sécurité, la durabilité et l'efficacité sont les principaux piliers du risque technologique à prendre en ligne de compte durant l'élaboration des contrôles liés à la gestion des appareils utilisés par la société membre.

Contexte	Contrôles
SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE	
De quoi s'agit-il? *Sécuriser physiquement les zones où se trouvent les actifs technologiques.* Pourquoi est-ce important? • *Pour protéger la technologie et le matériel physique contre les dommages accidentels, intentionnels ou environnementaux.*	➢ Mettre en place des contrôles d'accès physique, des technologies de surveillance et d'autres contrôles de sécurité pour prévenir et détecter les accès non autorisés aux emplacements sensibles (p. ex., les salles de serveurs). ➢ Protéger la salle de serveurs et le centre de données contre les menaces et les risques environnementaux (p. ex., incendies et dégâts d'eau). ➢ Exiger l'identification de tous les employés, entrepreneurs et visiteurs. ➢ Obtenir et examiner le rapport d'audit du fournisseur du centre de données (voir l'annexe C) et confirmer que des contrôles d'accès physique appropriés sont en place au centre de données.

Contexte	Contrôles
GESTION DES APPAREILS ET SERVEURS APPARTENANT À LA SOCIÉTÉ	
De quoi s'agit-il? *Gérer les risques associés aux actifs technologiques physiques.* Pourquoi est-ce important? • *Pour s'assurer qu'il n'y a pas de dispositifs non protégés ou non sécurisés, et donc vulnérables à un accès non autorisé.* • *Pour protéger et sécuriser tous les appareils contre les menaces externes pesant sur les données ou les applications qu'ils contiennent.* • *Pour protéger les informations confidentielles et privées sur tous les appareils contre les violations accidentelles résultant de la perte d'un appareil.* • *Pour s'assurer que l'appareil fonctionne efficacement et est compatible avec tous les systèmes et applications critiques.* • *Pour garantir la sauvegarde des informations essentielles sur l'appareil.*	➢ Tenir à jour une liste de tous les appareils qui précise l'emplacement, la date du dernier contrôle de maintenance et les personnes en possession des différents actifs. ➢ Établir des politiques pour l'utilisation acceptable des appareils – y compris des exigences pour arrêter ou verrouiller les appareils lorsqu'ils ne sont pas utilisés – et un plan de gestion des appareils mobiles. ➢ Établir des configurations de base pour le matériel qui ne peut être modifié qu'à l'aide d'une demande de changement en bonne et due forme. ➢ Empêcher les utilisateurs d'accéder à des sites et applications non sécurisés, et de désactiver les mécanismes de sécurité installés sur les appareils. ➢ Déployer des applications antimaliciel sur toutes les technologies (en particulier les appareils et les serveurs, ainsi que les systèmes et applications critiques pour les affaires de la société). ➢ Chiffrer les dispositifs qui recueillent, traitent, utilisent ou stockent des informations confidentielles. ➢ Mettre en place des outils pour effacer à distance les données de tous les appareils disparus ou volés. ➢ Établir et mettre en œuvre des politiques de fin de vie pour les dispositifs (c.-à-d. veiller à ce que les dispositifs obsolètes ou mis hors service soient nettoyés et éliminés de manière sûre). ➢ Élaborer et mettre en œuvre des politiques pour assurer la sauvegarde des serveurs et la disponibilité hors ligne.

Contexte	Contrôles
UTILISATION D'APPAREILS PERSONNELS	
De quoi s'agit-il? *Gérer les risques associés aux appareils personnels utilisés pour accéder à des informations essentielles et confidentielles, ainsi qu'à des systèmes et applications critiques.* Pourquoi est-ce important? • *Pour protéger et sécuriser tous les appareils personnels contre les menaces extérieures qui pèsent sur les données ou les applications de la société auxquelles ces appareils donnent accès.* • *Pour protéger les informations confidentielles et privées sur tous les appareils personnels contre les violations accidentelles résultant de la perte de ces appareils.* • *Pour garantir la sauvegarde des données et extrants commerciaux essentiels sur les appareils personnels.*	➢ Élaborer des politiques officielles sur l'utilisation des appareils personnels qui décrivent comment les utilisateurs peuvent utiliser leurs appareils personnels pour accéder aux systèmes et aux informations de la société. ➢ Tenir à jour une liste de tous les appareils personnels utilisés pour accéder aux informations de la société. ➢ Imposer l'accès aux données et applications confidentielles sur les appareils mobiles personnels au moyen d'un bac à sable ou d'un conteneur isolé et sécurisé. ➢ Mettre en place une capacité d'effacement à distance en cas de perte de l'appareil.
SÉCURITÉ DES RÉSEAUX	
De quoi s'agit-il? *Surveiller les réseaux internes et externes et les protéger contre les risques de sécurité.* Pourquoi est-ce important? • *Pour sécuriser tous les réseaux et les protéger contre les menaces extérieures qui pèsent sur les technologies et les informations qui s'y trouvent.*	➢ Bloquer automatiquement les tentatives d'accès aux réseaux internes par des appareils non enregistrés. ➢ Rechercher les dispositifs ou systèmes non autorisés sur le réseau. ➢ Installer des pare-feu pour mettre les connexions à l'abri des menaces extérieures. ➢ Établir des règles de détection qui limitent l'accès aux seuls sites de confiance et refusent les communications en provenance d'adresses IP malveillantes connues.

Contexte	Contrôles
• *Pour détecter les accès non autorisés aux réseaux par des intervenants externes ou internes.*	➢ Créer un accès aux réseaux pour les visiteurs ou les entrepreneurs temporaires avec restrictions d'accès.
PÉRIPHÉRIQUES DE STOCKAGE EXTERNES / SUPPORTS AMOVIBLES	
De quoi s'agit-il? *Gérer les risques associés aux périphériques de stockage externes et aux supports amovibles.* Pourquoi est-ce important? • *Pour sécuriser les données confidentielles et privées sur les dispositifs de stockage amovibles et les protéger contre la perte, le vol ou l'utilisation abusive.* • *Pour protéger les appareils et les réseaux contre toute infection par des logiciels malveillants au moyen de supports amovibles.*	➢ Chiffrer les dispositifs de stockage externes (p. ex., les disques durs externes et les clés USB). ➢ Verrouiller les ports des appareils appartenant à la société – limiter l'utilisation aux seuls appareils approuvés par la société. ➢ Limiter les actes des utilisateurs (p. ex., lecture seule, téléchargement seul, etc.) qui sont autorisés sur les appareils.

6.3 Gestion des systèmes et des applications

Cet aspect concerne certains contrôles de base visant l'ensemble des applications et logiciels utilisés dans diverses activités et opérations commerciales. La sécurité, l'intégrité, la durabilité et l'efficience sont les principaux piliers du risque technologique à prendre en compte durant l'élaboration des contrôles relatifs à la gestion des logiciels et des applications utilisés par la société.

Contexte	Contrôles
INVENTAIRE DES LOGICIELS	
De quoi s'agit-il? *Gérer les risques associés aux logiciels, aux systèmes et aux applications.*	➢ Tenir un inventaire des logiciels et des applications, le passer en revue au moins une fois par an et le mettre à jour si nécessaire. ➢ Établir un processus de demande/d'approbation pour l'acquisition et l'installation de logiciels.

Contexte	Contrôles
Pourquoi est-ce important? • *Pour garantir que tous les systèmes ou applications, ainsi que les données auxquelles les utilisateurs accèdent, sont protégés et sécurisés contre tout accès non autorisé ou téléchargement malveillant.* • *Pour s'assurer qu'il n'existe pas de systèmes ou d'applications non protégés ou non sécurisés, et donc vulnérables à un accès non autorisé.* • *Pour détecter et prévenir les modifications ou accès non autorisés (ou non planifiés) aux systèmes et applications qui pourraient entraîner des perturbations, des pertes ou des violations sur le plan commercial.*	➢ Détecter et bloquer les modifications ou installations non autorisées de logiciels. ➢ Établir des configurations de base pour les logiciels qui ne peuvent être mis à jour qu'à l'aide d'une demande de modification en bonne et dueforme.
GESTION DES CORRECTIFS ET DES VULNÉRABILITÉS	
De quoi s'agit-il? *Établir des pratiques en matière de correctifs et de vulnérabilités.* Pourquoi est-ce important? • *Pour veiller à ce que tous les systèmes ou applications, ainsi que les données auxquelles les utilisateurs accèdent, soient protégés contre les problèmes de sécurité et les vulnérabilités.* • *Pour garantir que tous les systèmes ou applications critiques continueront d'être opérationnels et soutenus par le développeur, afin d'être en mesure d'aborder et de corriger tout problème pouvant survenir.*	➢ Mettre en œuvre des solutions automatisées de gestion des correctifs et de mise à jour des logiciels. ➢ Tester les correctifs importants avant de les appliquer aux systèmes ou aux logiciels. ➢ Prioriser les correctifs manquants et en faire le suivi dans tous les environnements (y compris l'environnement de test et de production). ➢ Gérer les problèmes de fin de vie ou de fin de soutien (c.-à-d. prendre des mesures pour remplacer ou mettre à jour le produit avant l'expiration du soutien ou de la garantie).
SURVEILLANCE DU RENDEMENT ET DE L'INTÉGRITÉ DES EXTRANTS	

Contexte	Contrôles
De quoi s'agit-il? *Surveiller le fonctionnement et les extrants des systèmes et applications.* Pourquoi est-ce important? • *Pour veiller à ce que les systèmes et applications critiques continuent de fonctionner efficacement et de répondre aux besoins des utilisateurs.* • *Pour s'assurer que les systèmes et applications critiques produisent les résultats appropriés, selon les besoins.* • *Pour détecter les dysfonctionnements de système ou les extrants problématiques.* • *Pour veiller à ce que les systèmes et applications critiques continuent d'être utilisables en cas d'évolution des besoins des utilisateurs, des autres systèmes et applications connectés, et des exigences législatives ou réglementaires.* • *Pour s'assurer que les systèmes et applications critiques qui sont déployés représentent les solutions les plus efficaces et les plus efficientes disponibles.*	➢ Établir et surveiller les mesures de risque et de rendement pour les technologies et applications clés en fonction des besoins des responsables des activités et de la vision stratégique de la société membre. ➢ Examiner l'intégrité des informations générées pour s'assurer que le système produit des renseignements exacts et complets. ➢ Veiller à ce que les systèmes et la technologie utilisés pour la tenue des dossiers respectent toutes les exigences législatives et réglementaires applicables[9]. ➢ Veiller à ce que les activités de surveillance englobent toutes les technologies de communication utilisées[10]. ➢ Examiner les API et autres interfaces installés entre les différents systèmes et applications pour s'assurer de leur exhaustivité et de l'exactitude du traitement. ➢ Obtenir et examiner au moins une fois par an les rapports sur les contrôles organisationnels des sociétés de services (SOC 2) relatifs aux technologies et applications clés (voir l'annexe C pour une comparaison des différents rapports SOC).
CYCLE DE VIE DU DÉVELOPPEMENT DES LOGICIELS	
De quoi s'agit-il?	➢ Établir des normes et des pratiques de codage sûres pour les développeurs de logiciels en se basant sur les cadres du secteur.

[9] Les règles de l'OCRCVM stipulent les exigences minimales en matière de livres et de registres, et de pistes d'audit, dont la plupart sont décrites dans la [Règle 3800 de l'OCRCVM]. Les sociétés membres doivent également s'assurer du respect du Règlement 23-101 et des [articles 7201 à 7205 des Règles de l'OCRCVM].

Contexte	Contrôles
Gérer les risques associés aux logiciels développés au sein de la société, à chaque étape du cycle de vie du développement. Pourquoi est-ce important? • *Pour protéger et détecter les modifications non autorisées, accidentelles ou imprévues de la programmation et du code.* • *Pour veiller à ce que toute modification apportée à la programmation et au code soit testée avant la mise en œuvre ou la mise en service, afin d'éviter tout conflit avec les applications ou les appareils connectés et de s'assurer que le résultat obtenu est correct.* • *Pour garantir que les systèmes et applications critiques continuent à produire les résultats voulus.* • *Pour veiller à ce que les systèmes et les applications soient modifiés en temps utile en cas de changements dans les besoins des utilisateurs, les configurations des autres systèmes et applications connectés, et les exigences législatives ou réglementaires.* • *Pour garantir que la solution développée continue d'être la plus efficace et la plus efficiente possible.*	➢ Effectuer des tests de sécurité durant toutes les phases de post-conception (avant la mise en œuvre ou l'installation) pour chaque application. ➢ Effectuer des examens indépendants du code. ➢ Mettre à jour les applications en fonction de l'expérience acquise, des innovations technologiques et des nouvelles menaces. ➢ Effectuer une analyse du code statique et remédier aux vulnérabilités relevées.

[10] L'OCRCVM a mis en place des règles concernant la surveillance et la conservation des communications avec les clients. Voir l'Avis de l'OCRCVM 11-0349 intitulé *Lignes directrices visant l'examen, la surveillance et la conservation des publicités, de la documentation commerciale et de la correspondance*, ainsi que le [paragraphe 1201(2) des Règles de l'OCRCVM et la Règle 3600 de l'OCRCVM].

6.4 Gestion des processus

Cet aspect concerne certains contrôles de base ciblant l'ensemble des processus, en particulier ceux qui ont un impact direct sur la sécurité, l'intégrité, la disponibilité et l'efficacité de la technologie.

Contexte	Contrôles
PROCESSUS OPÉRATIONNELS – DOCUMENTS ET ORGANIGRAMMES	
De quoi s'agit-il? *Comprendre et consigner la manière dont la technologie est intégrée aux différentes activités commerciales.* Pourquoi est-ce important? • *Pour déterminer s'il existe des processus manuels pouvant être automatisés de manière efficace et efficiente.* • *Pour veiller à ce que les processus nécessaires au bon fonctionnement des technologies critiques soient gérés, supervisés et étayés de manière appropriée.*	➢ Élaborer des organigrammes et des descriptions de processus pour comprendre comment la technologie est intégrée aux différentes activités commerciales. ➢ Déterminer et traiter séparément les aspects relevant de l'automatisation et des procédures manuelles.
SURVEILLANCE DE L'EFFICACITÉ DES PROCESSUS OPÉRATIONNELS	
De quoi s'agit-il? *Surveiller le rendement des processus opérationnels.* Pourquoi est-ce important? • *Pour veiller à ce que tous les processus et intrants nécessaires au fonctionnement des technologies critiques fonctionnent comme prévu.*	➢ Établir des mesures d'efficacité et d'efficience pour le rendement des fonctions et activités opérationnelles. ➢ Examiner à intervalles réguliers le rendement des fonctions par rapport aux mesures afin de déterminer si des changements doivent être apportés. ➢ Cerner les points faibles (p. ex., un taux d'échec plus élevé lorsque les procédures sont effectuées manuellement, les aspects où le risque de fraude est plus élevé, etc.)

Contexte	Contrôles
• *Pour garantir que les problèmes liés aux processus opérationnels peuvent être relevés afin d'être corrigés.* • *Pour veiller à ce que tous les processus clés soient supervisés et contrôlés de manière adéquate.*	➢ Examiner les organigrammes et les descriptions de processus à intervalles réguliers pour s'assurer qu'ils font l'objet d'un suivi, et évaluer les améliorations possibles. ➢ Consigner la solution de la direction pour traiter les problèmes.

6.5 Gestion du changement

Cet aspect englobe les contrôles relatifs aux changements apportés à la technologie et aux processus connexes une fois que ces derniers sont effectivement en place. Il s'agit d'un aspect souvent négligé, mais susceptible de causer des pertes importantes s'il n'est pas correctement géré. La mise en œuvre des changements apportés aux technologies ou aux fournisseurs d'importance doit prendre en considération les quatre piliers du risque technologique.

Contexte	Contrôles
POLITIQUES ET PROCÉDURES	
De quoi s'agit-il? *Maintenir un plan pour orienter la mise en œuvre des principaux changements apportés aux technologies ou aux fournisseurs essentiels.* Pourquoi est-ce important? • *Pour veiller à ce que l'adoption de technologies critiques nouvelles ou actualisées augmente l'efficacité et l'efficience.* • *Pour s'assurer que les changements et les mises en œuvre technologiques critiques sont opérationnalisés de manière transparente.* • *Pour réduire au minimum les perturbations, les retards, les coûts et les erreurs liés à la*	➢ Consigner et mettre en œuvre des processus de gestion du changement pour couvrir les facteurs clés que sont l'alignement stratégique, la gestion budgétaire, la gestion des risques, les calendriers établis, la communication, la gestion des parties intéressées et les changements culturels. ➢ Pour les conversions importantes de technologies ou de fournisseurs, établir un organigramme de l'ensemble des fonctions, processus, dispositifs, systèmes et applications de la société et veiller à ce que le plan tienne compte de tous les changements. ➢ Élaborer des mesures pour évaluer le succès et l'efficacité des changements proposés. ➢ Veiller à ce que du personnel expérimenté soit chargé de diriger et de suivre la gestion du changement, et d'améliorer continuellement le processus.

Contexte	Contrôles
mise en œuvre de changements importants dans les technologies critiques.	➢ Confier à des employés inscrits la responsabilité d'approuver les fonctions automatisées et d'en assurer le suivi continu.
CONVERSIONS DE SYSTÈMES DE LIVRES ET DE REGISTRES[11]	
De quoi s'agit-il? *Gérer les risques liés aux conversions ou aux mises en œuvre de systèmes et d'applications d'importance, lorsque de telles activités ont un impact sur les exigences réglementaires en matière de tenue de livres.* Pourquoi est-ce important? • *Pour assurer le respect des exigences réglementaires.* • *Pour prévenir la perte de données lors de la conversion.* • *Pour réduire au minimum les perturbations et les pertes.*	➢ Effectuer un audit avant la conversion/mise en œuvre pour évaluer l'état de préparation en ce qui concerne les fournisseurs, les fonctions commerciales, les systèmes et les applications essentiels, ainsi que les informations qui seront touchées. ➢ Veiller à ce que l'ensemble des documents, des accords de service et des politiques et procédures applicables soient mis à jour. ➢ Mettre à jour le plan de continuité des activités (PCA) afin d'y intégrer le nouveau système. ➢ Effectuer un audit après la conversion/mise en œuvre pour s'assurer que le système fonctionne comme prévu et que l'ensemble des données, systèmes de connexion et fonctions ont été correctement et complètement convertis et reproduits.

6.6 Gestion des fournisseurs

Cet aspect concerne certains contrôles de base relatifs à la gestion des fournisseurs critiques. Le recours à des fournisseurs externes pourrait ajouter un risque important à l'égard des quatre piliers du risque technologique[12].

[11] Telles sont les attentes de l'OCRCVM lorsque les sociétés membres procèdent à une conversion de leurs systèmes comptables d'importance. Les sociétés qui procèdent à une conversion majeure doivent signaler le changement proposé à l'OCRCVM, comme le précise l'Avis 10-0060 de l'OCRCVM intitulé *Déclaration des modifications de modèles d'entreprise* [paragraphe 2246(2) des Règles de l'OCRCVM].

[12] L'OCRCVM a publié l'Avis 14-0012 en 2014 pour fournir des directives sur les *ententes d'impartition*. Les principes abordés ici sont essentiellement les mêmes que ceux mentionnés dans l'Avis de l'OCRCVM.

Contexte	Contrôles
DILIGENCE RAISONNABLE À L'ÉGARD DES FOURNISSEURS	
De quoi s'agit-il? *Valider et approuver les fournisseurs essentiels.* Pourquoi est-ce important? • *Pour s'assurer que le fournisseur jouit d'une bonne réputation et qu'il sera en mesure de fournir les technologies ou services critiques de la manière requise, en temps voulu.* • *Pour s'assurer que le fournisseur est en mesure de respecter les normes de rendement de la société.* • *Pour s'assurer que le fournisseur est en mesure de respecter les normes de sécurité de la société.* • *Pour garantir que le fournisseur sera apte à réagir aux problèmes et fera preuve de souplesse face aux changements dans les besoins des utilisateurs – comme dans les exigences législatives ou réglementaires.* • *Pour s'assurer que le fournisseur peut offrir ses produits ou services de manière efficace et efficiente.*	➢ Élaborer des politiques et des procédures relatives à la gestion des risques associés aux fournisseurs et du rendement de ces derniers, ce qui englobe l'analyse de rentabilité, la recherche de fournisseurs, l'évaluation des risques, l'examen juridique et la conclusion d'un contrat. ➢ Procéder à un examen continu de tous les fournisseurs et de leurs services et examiner les informations, les systèmes et les processus concernés. ➢ Affecter un cadre de la société à la gestion des relations et des accords avec les fournisseurs critiques. ➢ Évaluer les fournisseurs et les risques potentiels qu'ils posent sur le plan de l'information et de la sécurité avant de conclure un contrat (p. ex., évaluer la situation en matière de cybersécurité, mener des évaluations indépendantes de celle-ci, évaluer le risque lié au recours à des sous-traitants, etc.). ➢ Obtenir des preuves de certifications, des rapports d'audit, des témoignages de clients, des rapports de conformité des principaux organismes de réglementation, ainsi que des états financiers vérifiés, et effectuer d'autres vérifications d'antécédents pour s'assurer que le fournisseur est digne de confiance et viable.
INTÉGRATION DES FOURNISSEURS	
De quoi s'agit-il?	➢ Obtenir un accord signé[13] qui mentionne et explique, entre autres, les éléments suivants :

[13] Pour les fournisseurs de services nuagiques, se reporter à la norme internationale *ISO/IEC 19086-1 : Informatique en nuage – Cadre de travail de l'accord du niveau de service*, qui fournit des conseils sur l'établissement d'un contrat de niveau de service.

Contexte	Contrôles
Établir les étapes du processus d'intégration des nouveaux fournisseurs approuvés. Pourquoi est-ce important? • *Pour assurer une communication claire et la consignation des droits et des responsabilités.* • *Pour protéger la société contre les coûts et les risques liés aux fournisseurs.* • *Pour garantir que les fournisseurs n'ont accès qu'aux systèmes, applications et données dont ils ont besoin.*	○ les rôles et les responsabilités; ○ la propriété de l'information et de la technologie; ○ les normes de rendement et de sécurité, y compris l'obtention de rapports d'audit/SOC exempts d'exceptions importantes, et les conséquences de toute violation; ○ les clauses d'indemnité ou d'approbation préalable des sous-traitants d'importance; ○ les clauses de notification des changements importants chez le fournisseur qui auraient un impact sur la société; ○ les clauses de résiliation, y compris les délais et les responsabilités en matière de conservation et de destruction des informations confidentielles et exclusives; ○ le dédommagement; ○ les clauses de non-divulgation. ➢ Créer une liste de contrôle pour l'intégration des fournisseurs qui contient tous les aspects de la gestion des relations. ➢ Schématiser et déterminer toutes les informations et technologies auxquelles les fournisseurs auront accès. ➢ Communiquer les mesures et les normes que le fournisseur doit respecter et le processus de transmission des violations importantes aux échelons supérieurs.

Contexte	Contrôles
SURVEILLANCE DU RENDEMENT DES FOURNISSEURS ET DES RISQUES QU'ILS PRÉSENTENT	
De quoi s'agit-il? *Surveiller le rendement du fournisseur et de ses services.* Pourquoi est-ce important? • *Pour garantir que le fournisseur peut continuer à fournir des technologies ou des services critiques de manière efficace et efficiente, de la manière requise et en temps voulu.* • *Pour faire en sorte que le fournisseur respecte les normes de rendement de la société (c.-à-d. que la société sera en mesure de détecter et de corriger tout problème de rendement).* • *Pour s'assurer que le fournisseur respecte les normes de sécurité de la société (c.-à-d. que la société sera capable de détecter tout problème ou toute menace à sa sécurité et de se protéger contre ces problèmes et menaces).* • *Pour s'assurer que le fournisseur réagit aux problèmes qui lui sont signalés.* • *Pour veiller à ce que les risques pour la société que posent les changements de fournisseurs, de technologies ou de processus soient relevés et atténués.*	➢ Examiner régulièrement le rendement des fournisseurs, conformément aux mesures établies. ➢ Examiner régulièrement les contrôles de sécurité des fournisseurs, notamment en obtenant des attestations relatives à l'utilisation des données confidentielles et exclusives de la société. ➢ Évaluer les fournisseurs sur la base de la rétroaction du personnel chargé de la fonction commerciale, des communiqués de presse, des innovations technologiques, des informations financières et des changements dans le secteur ou la réglementation. ➢ Obtenir et examiner un rapport de type 2 sur le contrôle des sociétés de services (SOC 2) au moins une fois par an (voir l'annexe C pour une comparaison des différents rapports SOC) et évaluer le risque et le plan d'action relatifs aux exceptions importantes. ➢ Entretenir des contacts réguliers avec les fournisseurs essentiels pour discuter de toute violation des normes de rendement ou de sécurité, et découvrir si des changements envisagés pourraient avoir un impact sur la société ou le fournisseur. ➢ Signaler par voie hiérarchique les problèmes d'importance relevés dans le cadre de la surveillance du fournisseur, de son rendement ou de la sécurité.
INTÉGRATION DES FOURNISSEURS DANS LE PLAN DE CONTINUITÉ DES ACTIVITÉS (PCA)	
De quoi s'agit-il? *Tenir à jour des plans de sauvegarde concernant les fournisseurs critiques.*	➢ Mettre en œuvre un plan de sauvegarde à l'échelle de la société concernant tous les fournisseurs essentiels. ➢ Planifier et tester une stratégie de remplacement avec d'autres fournisseurs ou un processus de

Contexte	Contrôles
Pourquoi est-ce important? • *Pour réduire au minimum les perturbations et les coûts si un fournisseur critique devenait incapable de fournir la technologie ou les services de la manière requise et en temps voulu.*	contournement en cas d'incapacité soudaine ou inattendue d'un fournisseur de fournir les services. ➢ Obtenir et examiner le PCA du fournisseur pour s'assurer qu'il dispose lui aussi de plans de sauvegarde pour continuer à assurer la prestation des services en cas d'incidents ou de sinistres.
FIN DE LA RELATION AVEC UN FOURNISSEUR	
De quoi s'agit-il? *Établir les étapes du processus de modification ou de cessation des relations avec des fournisseurs.* Pourquoi est-ce important? • *Pour garantir que la société est protégée contre les problèmes de sécurité survenant chez le fournisseur après que la relation a pris fin.*	➢ Mettre en œuvre des contrôles pour éliminer les données et supprimer l'accès une fois qu'un contrat avec un fournisseur est résilié ou a pris fin. ➢ Obtenir du fournisseur l'attestation qu'il élimine – lui, ainsi que ses sous-traitants – toutes les informations de la société en sa possession.

6.7 Continuité des activités, intervention en cas d'incident et reprise après sinistre

Cet aspect concerne certains contrôles de base visant à garantir la disponibilité et la durabilité des technologies et des informations critiques. Ces contrôles visent notamment à s'assurer qu'il existe un plan pratique et réalisable permettant de réagir aux incidents et de reprendre les activités normales. Il s'agit notamment de veiller à ce que les fonctions commerciales reposant sur des technologies essentielles et critiques, de même que les processus connexes, puissent être maintenues si la technologie devenait inopérante pendant des périodes courtes ou prolongées.

Contexte	Contrôles
PLANIFICATION DE LA CONTINUITÉ DES ACTIVITÉS ET DE LA REPRISE APRÈS SINISTRE[14]	
De quoi s'agit-il? *Maintenir un PCA pour pouvoir faire face aux défaillances ou aux interruptions des technologies critiques.* Pourquoi est-ce important? • *Pour réduire au minimum les perturbations et les coûts si une technologie critique n'est pas disponible de la manière requise et en temps voulu.*	➢ Élaborer un plan de continuité des activités (PCA) pour faire face aux risques technologiques; ce PCA doit indiquer : les fonctions, la technologie et l'information clés de la société; le personnel responsable; la durée maximum prévue des pannes; le plan et les délais d'intervention; les événements à même de déclencher l'exécution du plan. ➢ Veiller à ce que les personnes responsables de l'utilisation et du soutien des technologies critiques soient intégrées au PCA et que du personnel remplaçant soit désigné, toutes ces personnes devant connaître les principaux aspects du PCA. ➢ Déterminer la capacité de la société à gérer un nombre accru d'ouvertures de comptes de clients et d'activités de négociation, ainsi que son aptitude à planifier la résilience opérationnelle. ➢ Tenir à jour le répertoire des employés et des personnes-ressources clés. ➢ Examiner et réviser le PCA au moins une fois par an. ➢ Évaluer le budget annuel pour se concentrer sur les risques émergents associés au secteur et à ses activités commerciales.
PLANIFICATION DE L'INTERVENTION EN CAS D'INCIDENT[15]	
De quoi s'agit-il?	➢ Élaborer un plan d'intervention en cas d'incident de sécurité abordant la manière de traiter une violation des données ou une cyberattaque indépendamment du processus lié au PCA.

[14] Les [articles 4711 à 4714 des Règles de l'OCRCVM] exige que les sociétés membres établissent un plan de continuité des activités (PCA) et qu'elles le testent fréquemment.

[15] Consultez le document Gestion des cyberincidents – Guide de planification de l'OCRCVM pour obtenir des conseils détaillés.

Contexte	Contrôles
Tenir à jour un plan d'intervention en cas d'incident pour faire face aux événements à risque pour la sécurité. Pourquoi est-ce important? • *Pour garantir que la société peut réagir rapidement lorsqu'un incident de sécurité est détecté, afin de limiter la portée d'une attaque et de réduire au minimum les pertes.*	➢ Engager et retenir les services d'une équipe d'experts en matière d'intervention, formée d'un accompagnateur spécialisé dans les violations de sécurité, d'un conseiller juridique, d'enquêteurs informatiques, de représentants des compagnies d'assurance et de consultants en communication de crise, et chargée de se pencher sur la question d'éventuels incidents avant qu'ils ne se produisent. ➢ Mettre en place une équipe interne d'intervention (comprenant des représentants des services juridiques, des communications de l'entreprise et des ressources humaines). ➢ Élaborer un plan de communication pour signaler les incidents de sécurité au public et aux médias, à la direction de la société, aux parties intéressées concernées, aux organismes de réglementation[16], aux commissaires à la protection de la vie privée ainsi qu'aux employés. ➢ Effectuer une analyse des causes principales des incidents importants et effectuer une enquête informatique une fois l'incident maîtrisé.
ESSAI ET MISE EN ŒUVRE DES AMÉLIORATIONS	
De quoi s'agit-il? *Mettre à l'essai le PCA et les plans d'intervention en cas d'incident.* Pourquoi est-ce important? • *Pour veiller à ce que le PCA et les plans d'intervention en cas d'incident soient pratiques et facilement opérationnels s'ils devaient être soudainement déclenchés.*	➢ Mettre à l'essai le PCA et le plan d'intervention en cas d'incident à intervalles réguliers, pour s'assurer qu'ils sont à jour et efficaces. ➢ Effectuer des exercices de simulation et des simulations de crise pour valider les plans et s'assurer que les lacunes éventuelles sont comblées. ➢ Mettre à jour le PCA et les plans d'intervention en fonction des enseignements tirés des essais.

[16] La Règle 3100 des courtiers membres [article 3703 des Règles de l'OCRCVM] exige que les incidents de cybersécurité qui respectent les critères stipulés fassent l'objet d'un signalement.

Contexte	Contrôles
• *Pour veiller à ce que tout problème ou toute lacune dans le PCA et les plans d'intervention soit cerné et corrigé.*	➢ Accroître la capacité à gérer un nombre accru d'ouvertures de comptes de clients et d'activités de négociation en tenant compte des besoins.

6.8 Gestion des ressources humaines

Cet aspect concerne certains contrôles de base relatifs aux ressources humaines qui permettent de garantir que les risques de sécurité sont gérés et que les personnes clés nécessaires au développement ou à la maintenance de la technologie critique sont embauchées et maintenues en poste. Il s'agit notamment de veiller à ce que ces personnes clés puissent être remplacées en cas de besoin, qu'elles fassent l'objet d'une formation croisée et qu'elles bénéficient du soutien requis.

Contexte	Contrôles
GESTION DES RESSOURCES HUMAINES	
De quoi s'agit-il? *Gérer les risques technologiques et de sécurité associés aux employés, aux entrepreneurs et aux fournisseurs.* Pourquoi est-ce important? • *Pour réduire au minimum les chances que des utilisateurs autorisés ayant accès à des technologies critiques et à des informations confidentielles soient la cause d'un incident ou d'une faille de sécurité.* • *Pour veiller à ce que la société soit informée des attaques ou des violations dès qu'elles se produisent, afin qu'elle puisse prendre rapidement des mesures pour y réagir, en limiter la portée et réduire les pertes au minimum.* • *Pour veiller à ce que les sociétés puissent prévenir les menaces provenant des utilisateurs autorisés.*	➢ Mettre en place des procédures de sécurité en bonne et due forme pour l'intégration des employés, des entrepreneurs et des fournisseurs et pour la fin de la relation avec ces employés, entrepreneurs et fournisseurs. ➢ Procéder à des vérifications d'antécédents et à un contrôle des risques de sécurité pour les nouveaux employés, entrepreneurs et fournisseurs. ➢ Définir des procédures disciplinaires en cas de non-respect des politiques de sécurité. ➢ Établir et mettre en œuvre un programme visant à détecter et à gérer les menaces d'initiés. ➢ Organiser une formation de sensibilisation à la cybersécurité pour l'ensemble du personnel lors de l'embauche et au moins une fois par an; cette formation devrait porter sur la manière de traiter les données confidentielles – y compris les informations personnelles – et de détecter les menaces (par exemple, les courriels d'hameçonnage).

Contexte	Contrôles
• *Pour garantir que les sociétés peuvent détecter les attaques en provenance d'utilisateurs autorisés.*	➢ Établir et communiquer la procédure à suivre par les employés, les entrepreneurs et les fournisseurs pour signaler les problèmes de sécurité et les problèmes potentiels. ➢ Inclure dans le code de conduite une section relative aux informations confidentielles et la faire signer annuellement par les employés, les entrepreneurs et les fournisseurs.
ATTRACTION ET MAINTIEN EN POSTE DES EMPLOYÉS TALENTUEUX	
De quoi s'agit-il? *Tenir à jour un plan pour embaucher et retenir les personnes clés nécessaires à la gestion des technologies critiques.* Pourquoi est-ce important? • *Pour réduire au minimum les perturbations et les coûts liés à l'indisponibilité des employés clés chargés de gérer les technologies critiques.* • *Pour s'assurer que les sociétés peuvent exécuter leur plan technologique stratégique et réaliser leurs objectifs.*	➢ Déterminer le plan stratégique des ressources humaines concernant la technologie et assurer le recrutement et l'orientation des talents dans toute l'organisation. ➢ Déterminer les rôles essentiels et les employés clés en matière de technologie et élaborer une stratégie pour retenir ou attirer les talents pouvant assumer ces rôles. ➢ Assurer la formation croisée des employés clés nécessaires à la gestion, au développement et à l'utilisation des technologies critiques, et désigner les remplaçants de ces employés.

7. Registre des risques

Les sociétés membres devraient envisager de consigner tous les travaux effectués sur les risques et les contrôles connexes dans un registre des risques.

Vous trouverez ci-dessous un exemple de ce à quoi peut ressembler ce registre :

			Principes *(cochez tous les éléments qui s'appliquent)*				Probabilité *(cochez un élément)*					Incidence *(cochez un élément)*					
Fonction commerciale	**Nom de la technologie**	**Événements à risque**	**C**	**I**	**D**	**E**	**TF**	**PÉ**	**M**	**É**	**TÉ**	**I**	**Min**	**Mod**	**Maj**	**I**	**Contrôles d'atténuation**

La mise en place du registre des risques n'est pas un exercice ponctuel. Les politiques et procédures de gestion des risques de la société doivent en effet tenir compte des aspects suivants :

- Le registre des risques sera passé en revue au moins une fois par an par le personnel concerné.
- Les événements à risque désignés comme ayant une incidence élevée ou une forte probabilité seront examinés plus fréquemment afin que les contrôles en place soient toujours suffisants et efficaces pour gérer le risque.
- Certains éléments déclencheurs clés nécessitent une mise à jour ou une révision du registre des risques. Par exemple :
    - lors de l'acquisition de technologies ou de changements touchant les fournisseurs (passation de contrat, embauche, gestion);
    - lorsque les circonstances dans le secteur ou la société augmentent l'incidence des événements à risque ou la probabilité qu'ils se produisent;
    - lors de la mise en œuvre d'un changement de processus opérationnel;
    - lorsqu'il y a changement de fournisseur de services de TI.

8. Importance de la gouvernance

La gestion efficace du risque technologique nécessite la participation des personnes chargées de la gouvernance et de la surveillance de la stratégie au sein de la société membre.

Comme il a été mentionné précédemment, le risque technologique ne relève pas seulement des employés responsables des TI, de la gestion des risques ou de la conformité. Une gestion efficace du risque technologique nécessite en effet la collaboration du personnel des divers secteurs d'activité, depuis la base jusqu'au sommet, ce qui inclut le conseil d'administration et la haute direction de la société.

Le conseil d'administration est responsable de la gouvernance de la société. Alors que la haute direction se charge d'élaborer une stratégie technologique de base et un cadre de gestion des risques, le conseil d'administration assume la responsabilité de superviser la haute direction et de remettre en question ses propositions stratégiques et plans de mise en œuvre[17].

Les responsabilités du conseil d'administration et de la haute direction en matière de technologie sont essentiellement à deux volets :

1. Élaboration et supervision du plan technologique stratégique;
2. Surveillance de la gestion des risques technologiques.

[17] Dans la plupart des PME membres de l'OCRCVM, le conseil d'administration est aussi formé de membres de la haute direction.

8.1 Élaboration et supervision du plan stratégique sur la technologie de la société

Dans un secteur où la technologie est de plus en plus ancrée dans l'entreprise, le conseil d'administration et la haute direction doivent se pencher non seulement sur leur degré de dépendance à l'égard de la technologie, mais aussi sur leur vision à long terme en ce qui concerne l'adoption ou le développement de la technologie, l'automatisation et l'innovation. Ils doivent par conséquent déterminer quelle forme la dépendance doit prendre.

Par exemple, le conseil d'administration et la haute direction devraient prendre en considération :

- le fait que la société doit être innovatrice en technologie financière ou, dans le cas contraire, jusqu'à quel stade du processus d'adoption de la technologie elle doit s'engager, et dans quels fonctions ou secteurs commerciaux. Il faut savoir, par exemple, si le développement technologique fait partie des compétences essentielles de la société dans toutes ses fonctions commerciales ou s'il convient plutôt de faire appel à d'autres fournisseurs;
- les technologies émergentes et leur potentiel de perturbation pour la société et le secteur;
- le fait que la société dispose ou non des ressources nécessaires pour réaliser son plan technologique stratégique;
- le fait qu'il faut intégrer ou non leur vision de la technologie et de l'innovation dans le marketing et les affaires publiques;
- l'examen des projets technologiques en cours pour s'assurer qu'ils sont mis en œuvre dans les délais et dans les limites du budget, et qu'ils sont conformes à la stratégie globale de la société.

8.2 Surveillance de la gestion du risque technologique

Le conseil d'administration et la haute direction devraient veiller à ce que les événements à haut risque soient correctement déterminés et gérés[18].

Par exemple, en ce qui concerne le risque technologique, le conseil d'administration et la haute direction devraient envisager de faire ce qui suit :

- examiner le registre des risques pour s'assurer que les événements à haut risque ont été déterminés et sont gérés de manière adéquate;
- examiner les politiques et les procédures pour s'assurer que la gestion du risque technologique est intégrée et incorporée dans tous les aspects pertinents des activités commerciales;

[18] L'article 1502 des Règles de l'OCRCVM, qui sera en vigueur à partir du 31 décembre 2021, prévoit que les sociétés membres de l'OCRCVM doivent attribuer la responsabilité de chaque catégorie de risque importante à un membre de la haute direction qualifié. Si le risque technologique est considéré comme une catégorie de risque importante pour la société, le respect de cette règle devra être pris en considération.

- établir des structures de responsabilité et de reddition de comptes pour superviser la gestion du risque technologique;
- approuver des seuils de tolérance et d'appétit pour le risque pour les incidents technologiques et de sécurité, et effectuer le suivi des dépassements majeurs de tels seuils;
- élaborer des mesures de rendement pour juger du succès ou de l'efficacité des contrôles de gestion du risque;
- exiger de voir les résultats des audits ou des exercices de simulation qui testent et valident les contrôles, tant à l'interne que chez les fournisseurs externes.

Le risque technologique devenant omniprésent, les membres du conseil d'administration et de la haute direction responsables de la gouvernance doivent s'efforcer de comprendre l'environnement technologique dans lequel la société membre évolue. Pour les petites entreprises, cette tâche peut se révéler difficile; elles pourraient alors envisager, par exemple :

- de recruter des spécialistes et des consultants experts en technologie et en gestion des risques chargés de conseiller le conseil d'administration et la haute direction;
- de former et de sensibiliser les membres du conseil d'administration et de la haute direction sur les technologies, les innovations et les risques pertinents;
- d'intégrer de nouveaux membres au conseil d'administration et de recruter de hauts dirigeants qui ont une expérience pertinente en matière de gestion du risque technologique.

Le conseil d'administration et la haute direction doivent être engagés et contribuer à la détermination du plan technologique stratégique et à la gestion des risques de la société afin d'assurer le succès à long terme de celle-ci.

9. Conclusion

Compte tenu de la dépendance croissante à l'égard de la technologie et de l'automatisation, les sociétés membres de l'OCRCVM sont encouragées à se pencher plus attentivement sur la gestion des risques associés à cette dépendance. Une gestion efficace du risque technologique est possible si certains principes de base sont respectés.

Les sociétés qui ne disposent pas aujourd'hui d'un cadre en bonne et due forme pour gérer le risque technologique devraient envisager de prendre des mesures en faisant appel à des consultants en gestion des risques en général – et en gestion du risque technologique en particulier. Ceux-ci pourront alors concevoir et mettre en œuvre un cadre personnalisé unique qui tient compte du modèle d'affaires et des parties intéressées en cause. La société membre pourra ainsi mieux gérer le risque associé à l'utilisation de la technologie.

10. Annexes

A. Guides et références

Normes mondiales

- ISO 27000
- NIST
- COBIT

Publications

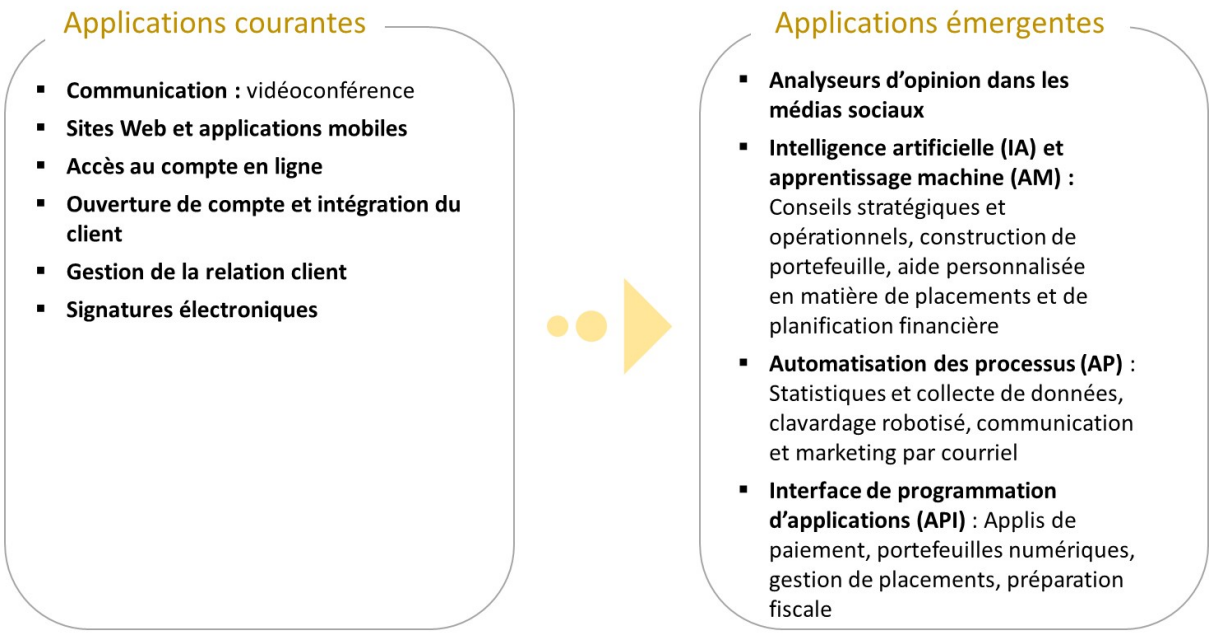
- Guide de pratiques exemplaires en matière de cybersécurité, Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), 2015
- Gestion des cyberincidents – Guide de planification, Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), 2015
- Renforcer la résilience du secteur financier dans un monde numérique, Bureau du surintendant des institutions financières, septembre 2020
- Forging New Pathways: The next evolution of innovation in Financial Services, Forum économique mondial, septembre 2020 (en anglais seulement)
- Transfert transfrontalier des données personnelles, Commissariat à la protection de la vie privée du Canada, janvier 2009
- Guide de cybergouvernance de l'OCRCVM, Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), janvier 2020
- ISO/IEC 19086-1 : Informatique en nuage – Cadre de travail de l'accord du niveau de service, Organisation internationale de normalisation/ISO (en anglais seulement)
- La protection de la vie privée et l'externalisation pour les entreprises, Commissariat à la protection de la vie privée du Canada, janvier 2014
- Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité, Commissariat à la protection de la vie privée du Canada, octobre 2018

B. Applications de la technologie par les sociétés membres de l'OCRCVM

Service à la clientèle et expérience

Au cours des dernières années, les sociétés membres de l'OCRCVM ont considérablement augmenté leurs investissements dans les technologies visant à améliorer le service à la clientèle et l'expérience des clients. Certaines des applications les plus largement utilisées sont liées aux communications virtuelles (p. ex., outils de vidéoconférence) et à la collecte sécurisée d'informations auprès du client. La signature électronique est un autre secteur de l'automatisation qui devient de plus en plus la règle plutôt que l'exception : son adoption s'est accélérée en raison des circonstances découlant de la pandémie.

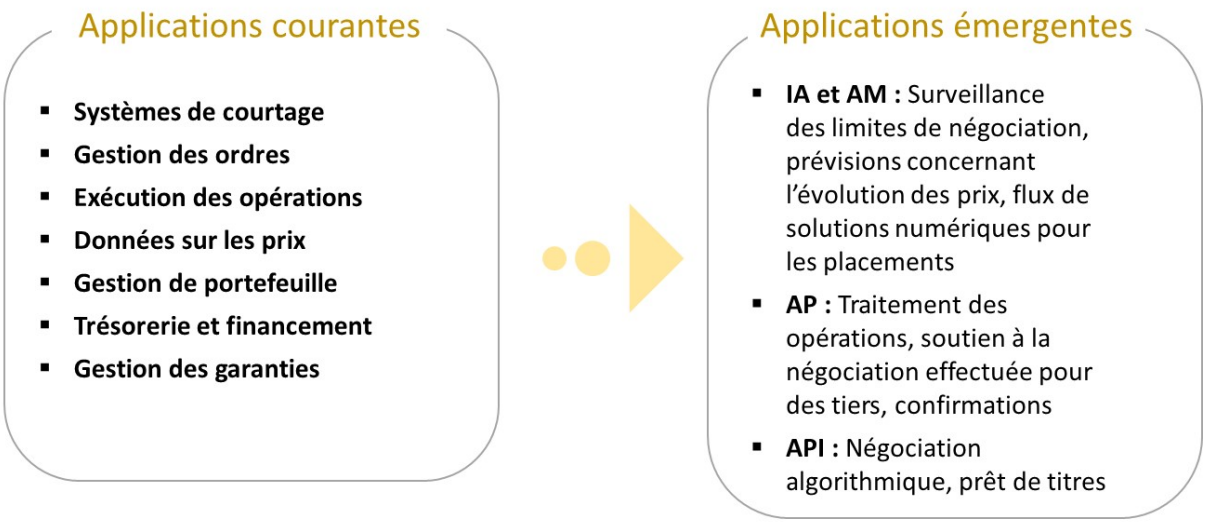
Aussi, plusieurs sociétés membres de l'OCRCVM en sont à divers stades du déploiement des technologies en ce qui concerne l'ouverture de comptes clients et le processus d'intégration. De même, les sites Web et les applications mobiles offrant aux clients un accès en ligne aux renseignements sur leur compte et d'autres systèmes de gestion de la relation client sont également des services où les technologies sont largement utilisées. Il convient de noter que ces observations ne s'appliquent pas aux sociétés offrant à leurs clients des services de négociation en ligne (soit les sociétés offrant des services d'exécution d'ordres sans conseils et des robots-conseillers), les technologies soutenant l'interface de négociation des clients et les applications correspondantes faisant partie intégrante du modèle d'affaires de ces sociétés.



Activités de négociation

La fonction de négociation des sociétés de l'OCRCVM, qui comprend le processus de compensation et de règlement, repose en grande partie sur l'automatisation et toute une série de technologies faisant partie intégrante des activités principales.

Un système de courtage englobant la tenue de dossiers liés aux comptes, aux opérations et aux informations sur les actifs constitue le système technologique de base utilisé par les sociétés membres de l'OCRCVM. De la même façon, les sociétés membres utilisent la technologie dans un certain nombre d'autres domaines, notamment pour la gestion des ordres, l'exécution des opérations, les données sur les prix, la gestion de portefeuille, les opérations de financement, la gestion des garanties, etc.

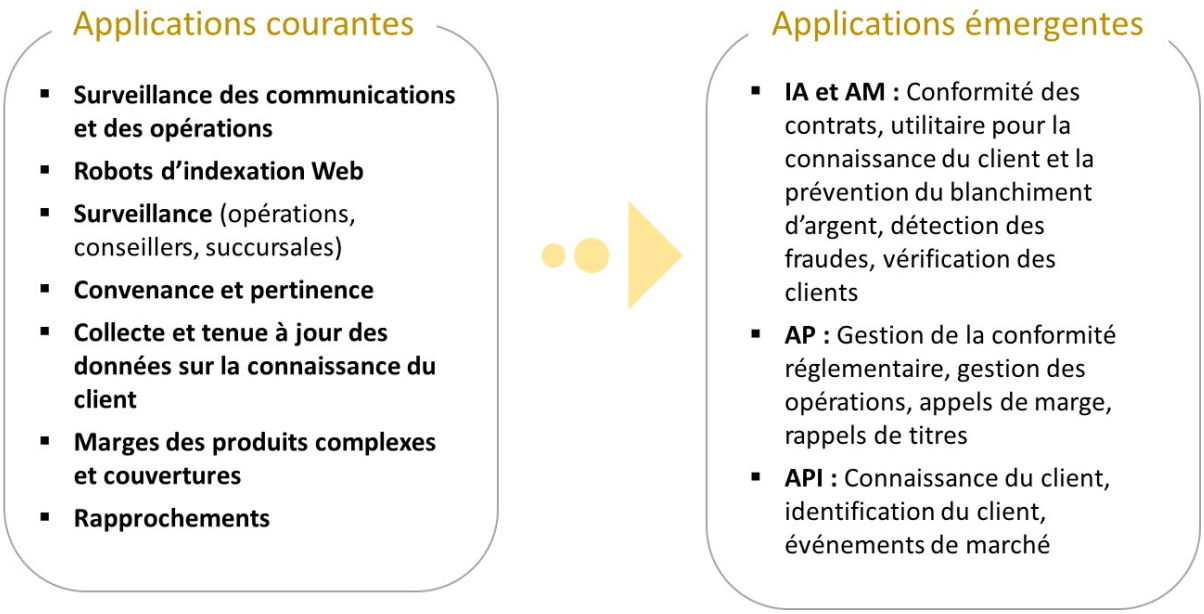


Conformité

La fonction de conformité des sociétés membres de l'OCRCVM s'appuie de plus en plus sur diverses technologies, que les sociétés utilisent pour les aider à s'acquitter de leurs responsabilités réglementaires. Ces technologies sont généralement appelées « technologies réglementaires » (ou *RegTech*).

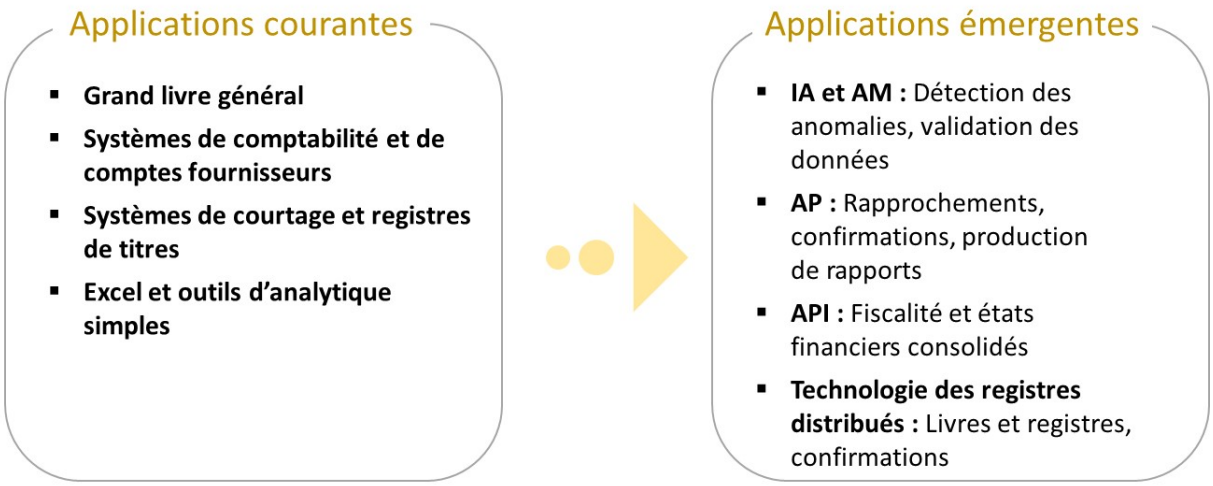
Du point de vue de leur conduite, les sociétés membres de l'OCRCVM ont généralement recours à la technologie pour appuyer la fonction de conformité avec les obligations de surveillance (des opérations, des personnes, des établissements, etc.), et assurer la convenance et le caractère approprié des opérations des clients, la collecte adéquate de l'information et le respect des exigences touchant la connaissance du client, ainsi que la production d'informations destinées à la clientèle telles que les relevés de compte.

Enfin, du point de vue de la surveillance prudentielle, les sociétés membres de l'OCRCVM s'appuient sur la technologie pour assurer le respect des exigences en matière de capital et de liquidité et pour protéger les actifs.



Finances et production de rapports

Depuis plusieurs années, les sociétés membres de l'OCRCVM se tournent vers la technologie pour faciliter les fonctions liées aux finances et à la production de rapports. Elles utilisent divers systèmes, tels que les systèmes de comptabilité générale et de courtage, ainsi que des feuilles de calcul Excel et d'autres outils d'analyse simples pour combiner les renseignements provenant des différents systèmes afin de générer des rapports complets.

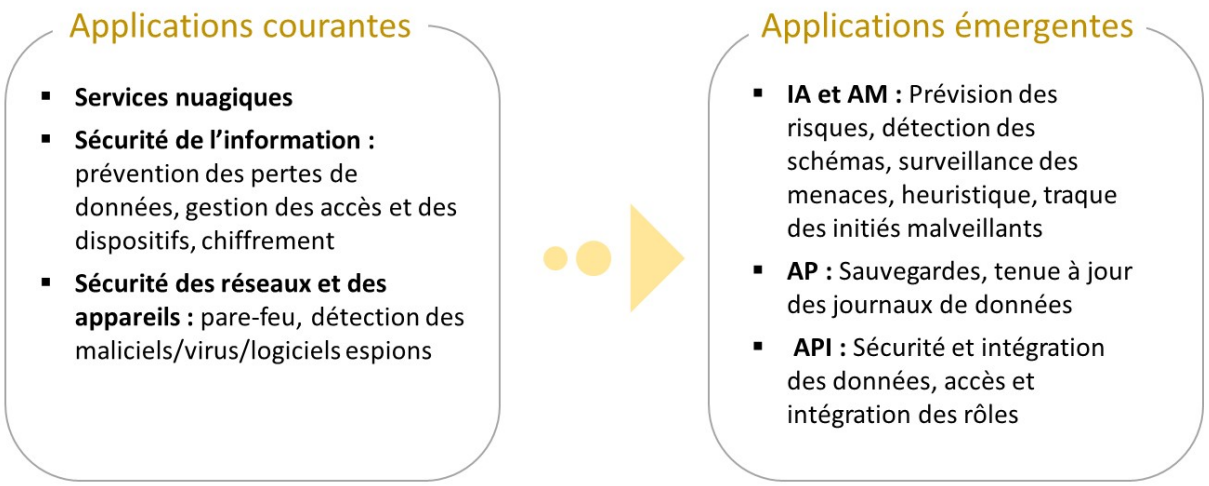


Technologies de l'information, sécurité et gestion

Au cours des dernières années, les sociétés membres de l'OCRCVM ont mis en place des technologies pour faire face aux risques liés à l'explosion des cyberattaques, à l'essor des mégadonnées et à l'augmentation du nombre d'exigences réglementaires touchant la protection de la vie privée.

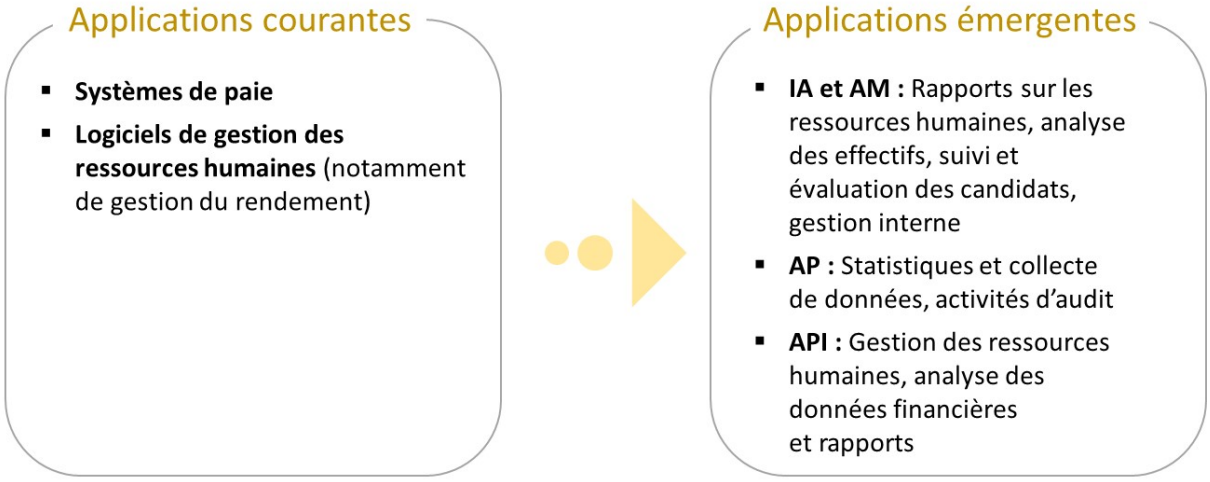
L'adoption des services nuagiques est l'un des domaines où la technologie connaît le plus d'effervescence.

Les sociétés utilisent également la technologie pour les aider à gérer les risques liés à la sécurité de l'information, par exemple pour la prévention des pertes de données, la gestion des accès, la gestion des actifs et la surveillance des activités anormales – sans oublier la protection des systèmes et des données, notamment par l'utilisation du chiffrement, des pare-feu, des antimaliciels, etc.

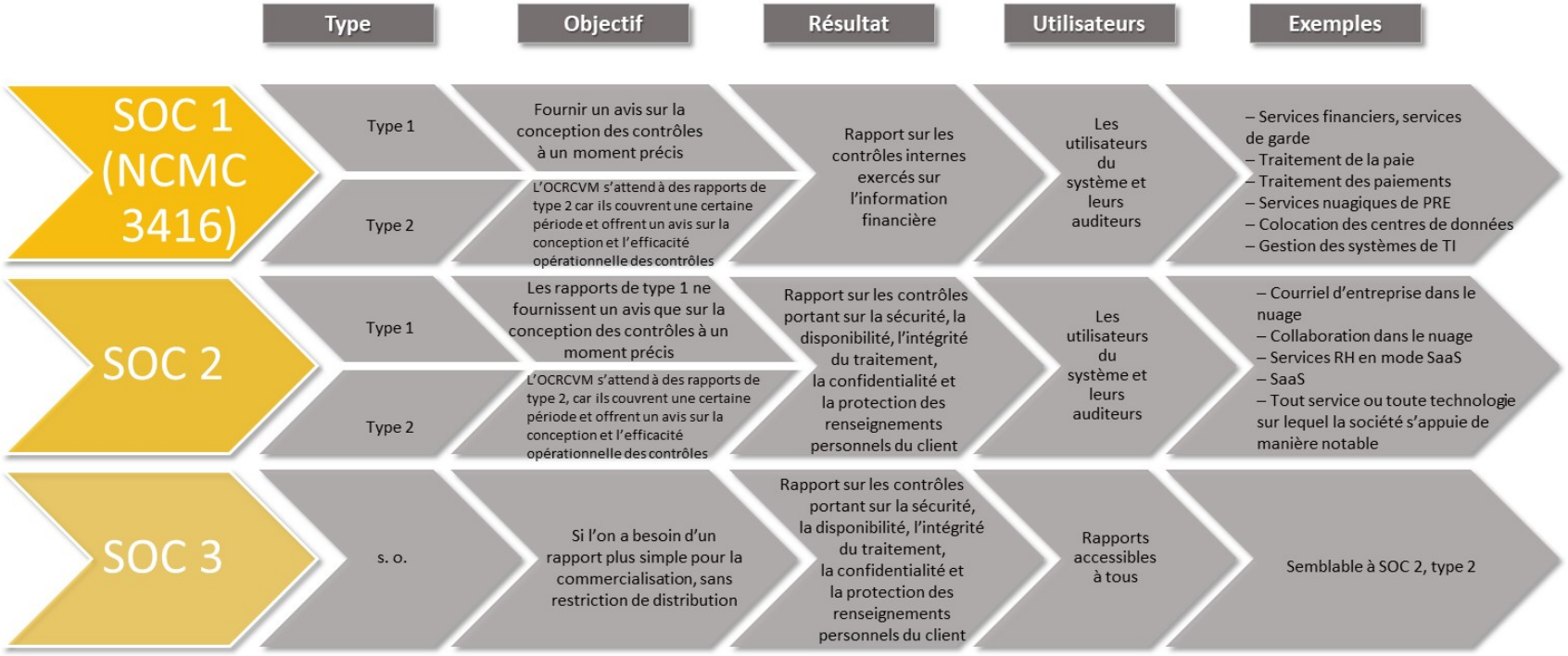


Ressources humaines et fonctions administratives, juridiques et autres

Les sociétés membres de l'OCRCVM s'appuient sur diverses technologies et applications pour gérer leurs ressources humaines et leurs fonctions administratives. La plupart utilisent une technologie quelconque pour stocker les informations relatives aux ressources humaines, notamment les renseignements personnels et les informations sur la paie, la gestion du rendement, l'embauche, etc. La prévalence de la technologie dépend de la taille et de l'étendue des activités de la société. Par exemple, les services de paie sont généralement fournis à l'interne si la société est relativement grande, ou sous-traités à un fournisseur dans le cas d'une entreprise plus petite.



C. Rapports SOC – Graphique comparatif



D. Glossaire

Appétit pour le risque

Risque total qu'une entreprise peut tolérer.

Automatisation des processus (AP)

L'automatisation des processus désigne la démarche consistant à affecter à la robotique des tâches manuelles et répétitives plutôt qu'aux humains afin de rationaliser les flux de travail dans les institutions financières.

Étiquette blanche/solutions externes

Par « étiquette blanche », on entend le fait qu'un produit ou un service créé par une société (le producteur) est ensuite renommé et vendu par une autre société (le distributeur).

Hébergement sur place

Le terme « hébergement sur place » signifie qu'une société conserve toute son infrastructure informatique dans ses propres locaux; l'infrastructure est gérée soit par la société, soit par un tiers.

Infrastructure en tant que service (IaaS)

L'IaaS permet de mettre virtuellement en place des serveurs, des réseaux, des capacités de stockage et des logiciels systèmes afin d'augmenter ou de remplacer les centres de données ou les ordinateurs mis en réseau individuellement.

Intelligence artificielle (IA) et apprentissage machine (AM)

On entend par IA l'application d'outils de calcul pour traiter des tâches nécessitant traditionnellement l'intelligence humaine.

L'AM est un sous-ensemble de l'IA; il renvoie à une technologie capable d'autoapprentissage et d'autoamélioration. L'AM peut ainsi constituer des modèles prédictifs à partir d'exemples, de données et d'expériences plutôt que de simplement suivre des règles préprogrammées.

Interfaces de programmation d'applications (interfaces API)

Une API est un ensemble de fonctions qui permet à différentes applications d'interagir entre elles et d'accéder à des données comme à d'autres systèmes d'exploitation.

Logiciel en tant que service (SaaS)

Le SaaS fournit toutes les fonctions d'une application traditionnelle, mais au lieu d'utiliser les ressources informatiques locales, les données circulent sur Internet par l'entremise du navigateur Web.

Norme canadienne de missions de certification (NCMC 3416)

La Norme canadienne de missions de certification (NCMC 3416) porte sur l'établissement de rapports sur les contrôles d'une société de services lorsque ces contrôles sont susceptibles d'être pertinents pour le contrôle interne qu'exercent les entités utilisatrices sur l'information financière (Manuel de l'ICCA).

Plateforme en tant que service (PaaS)

La PaaS fournit des serveurs virtuels où les applications existantes peuvent être exécutées, ou de nouvelles développées, sans qu'il soit nécessaire de maintenir des systèmes d'exploitation locaux, du matériel de serveur, une infrastructure, etc.

Rapports de contrôle des sociétés de services (SOC)

Les rapports de conformité SOC couvrent les activités d'une société de services. Voir l'annexe C pour un graphique comparatif des différents rapports.

SSAE 18 (anciennement SSAE 16)

Les rapports d'audit SSAE 18 fournissent à la direction une évaluation indépendante du caractère adéquat des procédures de contrôle et une « assurance raisonnable » quant à l'efficacité de l'environnement de contrôle du traitement, lorsque cet aspect a une incidence sur le contrôle interne qu'exercent les entités utilisatrices sur l'information financière. (Source : Deloitte)

Technologie des registres distribués (TRD)

La TRD désigne un ensemble concerté de registres dupliqués, qui sont partagés numériquement à l'échelle de plusieurs emplacements.

Tolérance au risque

Niveau de risque individuel qu'une entreprise peut tolérer, c'est-à-dire par service, activité ou fonction.