Ligne directrice

Titre	Gestion du risque lié aux technologies et du cyberrisque
Catégorie	Saines pratiques commerciales et financières
Date	31 juillet 2022
Secteur	Banques Succursales de banques étrangères Succursales de sociétés d'assurance étrangères Sociétés d'assurance vie et de secours mutuels Sociétés des assurances multirisques Sociétés de fiducie et de prêts
N°	B-13

Table des matières

A. Objet et portée

La présente ligne directrice établit les attentes du BSIF en matière de gestion du risque lié aux technologies et du cyberrisque. Elle s'applique à toutes les institutions financières fédérales (IFF), y compris les succursales de banques étrangères et les succursales de sociétés d'assurance étrangères, dans la mesure permise par les exigences applicables et les obligations légales concernant les activités qu'elles exercent au Canada [1] . Les attentes à l'égard des succursales sont énoncées dans la ligne directrice E 4, Entités étrangères exploitant une succursale au Canada Ces attentes visent à aider les IFF à être plus résilientes face au risque lié aux technologies et au cyberrisque.

Il n'y a pas d'approche universelle de gestion du risque lié aux technologies et du cyberrisque, compte tenu des risques et des vulnérabilités uniques qui varieront selon la taille de l'IFF, la nature, la portée et la complexité de ses activités et son profil de risque. La présente ligne directrice doit être lue et mise en œuvre dans une optique fondée sur le risque qui permet aux IFF d'être concurrentielles et de tirer pleinement parti de l'innovation numérique tout en assurant une saine gestion du risque lié aux technologies.

A.1 Définitions [2]

Le « risque lié aux technologies », qui englobe le « cyberrisque », s'entend du risque découlant de l'insuffisance, de la perturbation, de la destruction, des pannes et des dommages attribuables à un accès non autorisé, à des modifications ou à l'utilisation malveillante des actifs, des personnes ou des processus de technologie de l'information qui comblent et appuient les besoins opérationnels, pouvant entraîner des pertes financières ou porter atteinte à la réputation de l'institution.

Un « actif technologique » est un bien corporel (matériel, infrastructure, etc.) ou incorporel (logiciel, données, information, etc.) qui permet la prestation de services technologiques et qui doit être protégé.

Le terme « technologie » est utilisé au sens large dans la présente ligne directrice et englobe la « technologie de l'information » (TI). Le terme « cybersécurité », également utilisé au sens large, englobe quant à lui la « sécurité de l'information ».

A.2 Structure

La présente ligne directrice est organisée en trois domaines. Chacun d'eux énonce les principales composantes d'une saine gestion du risque lié aux technologies et du cyberrisque.

1. **Gouvernance et gestion du risque** – Énonce les attentes du BSIF au chapitre de la responsabilisation formelle, du leadership, de la structure organisationnelle et du cadre qui appuient la gestion du risque et la supervision de la technologie et de la cybersécurité.

2. **Activités et résilience technologiques** – Énonce les attentes du BSIF en matière de gestion et de supervision des risques liés à la conception, à la mise en œuvre et à la gestion des actifs et services technologiques, et à leur rétablissement.
3. **Cybersécurité** – Énonce les attentes du BSIF en matière de gestion et de supervision du cyberrisque.

A.3 Résultats

Chaque domaine est assorti d'un résultat que l'on souhaite voir les IFF obtenir en gérant les risques, contribuant ainsi au développement de leur résilience face au risque lié aux technologies et au cyberrisque.

1. La gouvernance du risque lié aux technologies et du cyberrisque repose sur des responsabilités et des structures claires ainsi que sur des stratégies et des cadres détaillés.
2. L'environnement technologique est stable, extensible et résilient, et il est tenu à jour et soutenu par des processus d'exploitation et de reprise technologiques robustes et durables.
3. La posture technologique est sûre et protège la confidentialité, l'intégrité et la disponibilité des actifs technologiques de l'IFF.

A.4 Consignes et renseignements connexes

Le risque lié aux technologies et le cyberrisque sont dynamiques et recoupent d'autres axes de risque. Il est donc conseillé aux IFF de lire la présente ligne directrice en parallèle avec d'autres consignes, outils et communications de surveillance du BSIF, ainsi qu'avec les consignes émises par d'autres instances et applicables au contexte opérationnel de l'IFF, dont les textes suivants :

- Ligne directrice Gouvernance d'entreprise du BSIF;
- Ligne directrice E-21, Gestion du risque opérationnel, du BSIF;
- Ligne directrice B-10, Impartition d'activités, de fonctions et de méthodes commerciales, du BSIF;
- Outil Autoévaluation en matière de cybersécurité du BSIF;
- Préavis Signalement des incidents liés à la technologie et à la cybersécurité, du BSIF;
- Alertes, renseignements et autres communications émis par le Centre canadien pour la cybersécurité;

- Cadres et normes reconnus pour les activités technologiques et la sécurité de l'information.

1. Gouvernance et gestion du risque

Résultat attendu : La gouvernance du risque lié aux technologies et du cyberrisque repose sur des responsabilités et des structures claires ainsi que sur des stratégies et des cadres détaillés.

1.1 Responsabilité et structure organisationnelle

Principe 1 : La haute direction doit confier la responsabilité de la gestion du risque lié aux technologies et du cyberrisque à des cadres supérieurs. Elle doit également veiller à ce qu'une structure organisationnelle appropriée et des ressources adéquates soient en place pour gérer le risque lié aux technologies et le cyberrisque à l'échelle de l'IFF.

1.1.1 La responsabilité de la haute direction est établie

Il incombe à la haute direction de diriger les activités de l'IFF liées aux technologies et à la cybersécurité et de confier clairement la responsabilité de la gouvernance du risque lié aux technologies et du cyberrisque à des cadres supérieurs. Les cadres en question peuvent comprendre le chef de la technologie de l'information, le dirigeant principal de la technologie (DPT), le dirigeant principal de l'information (DPI), le chef de la cybersécurité ou le dirigeant principal de la sécurité de l'information (DPSI). Ces postes doivent avoir une stature importante et une visibilité notable dans l'ensemble de l'institution.

1.1.2 Une structure, des ressources et une formation sont fournies

L'IFF doit :

- établir une structure organisationnelle de gestion du risque lié aux technologies et du cyberrisque à l'échelle de l'institution, avec des attributions claires, des ressources humaines et financières adéquates et une

expertise et une formation appropriées dans le domaine;

- intégrer dans les rangs de la haute direction des personnes ayant une compréhension suffisante du risque lié aux technologies et du cyberrisque;
- faire valoir une culture de sensibilisation au risque lié aux technologies et au cyberrisque dans l'ensemble de l'institution.

Veuillez consulter la ligne directrice Gouvernance d'entreprise du BSIF pour connaître les attentes du BSIF à l'égard des conseils d'administration des IFF en ce qui concerne la stratégie d'affaires, la propension à prendre des risques, les politiques opérationnelles et commerciales, ainsi que les politiques de gestion du risque et de gestion de crise.

1.2 Stratégie en matière de technologie et de cybersécurité

Principe 2 : L'IFF doit définir, documenter, approuver et mettre en œuvre un ou plusieurs plans stratégiques en matière de technologie et de cybersécurité. Le ou les plans doivent correspondre à la stratégie d'affaires et établir des buts et des objectifs mesurables qui évoluent en fonction des changements dans l'environnement technologique et cybernétique de l'IFF.

1.2.1 La stratégie est anticipatrice, complète et mesurable

Les plans stratégiques en matière de technologie et de cybersécurité de l'IFF doivent tenir compte des éléments suivants :

- prévoir les changements éventuels dans l'environnement technologique et cybernétique interne et externe de l'IFF;
- faire référence aux changements prévus dans l'environnement technologique de l'IFF;
- décrire clairement les facteurs, les possibilités, les vulnérabilités, les menaces et les mesures pour rendre compte des progrès réalisés par rapport aux objectifs stratégiques;
- inclure des indicateurs de risque qui sont définis, mesurés, suivis et faisant l'objet de rapports;
- expliquer comment les activités liées aux technologies et à la cybersécurité appuieront la stratégie d'affaires globale.

1.3 Cadre de gestion du risque lié aux technologies et du cyberrisque

Principe 3 : L'IFF doit établir un cadre de gestion du risque lié aux technologies et du cyberrisque. Le cadre doit établir la propension à prendre des risques liés aux technologies et des cyberrisques et définir les processus et exigences mis en place par l'IFF pour cerner, évaluer, gérer et surveiller les risques liés aux technologies et les cyberrisques, et en rendre compte.

1.3.1 Le cadre de gestion du risque concorde avec le cadre de gestion du risque d'entreprise et est en constante amélioration

L'IFF doit établir un cadre de gestion du risque lié aux technologies et du cyberrisque qui concorde avec son cadre de gestion du risque d'entreprise. L'IFF doit examiner et actualiser régulièrement son cadre de gestion du risque lié aux technologies et du cyberrisque pour y apporter des améliorations continues en fonction des résultats de la mise en œuvre et de la surveillance, et des autres leçons tirées (p. ex., les incidents antérieurs).

1.3.2 Le cadre de gestion du risque consigne les éléments clés

L'IFF doit tenir compte des éléments suivants de la gestion du risque au moment d'établir son cadre de gestion du risque lié aux technologies et du cyberrisque :

- la responsabilité à l'égard de la gestion du risque lié aux technologies et du cyberrisque, y compris des fonctions de supervision pertinentes;
- la propension à prendre des risques liés aux technologies et des cyberrisques et l'évaluation de ces risques (p. ex., limites, seuils et niveaux de tolérance);
- une taxonomie des risques liés aux technologies et des cyberrisques;
- les domaines de contrôle de la sécurité des technologies et de la cybersécurité;
- les politiques, normes et processus régissant le risque lié aux technologies et le cyberrisque, qui sont approuvés, examinés régulièrement et mis en œuvre uniformément à l'échelle de l'organisation;

- les processus de détermination, d'évaluation, de gestion et de suivi du risque lié aux technologies et du cyberrisque, et de production de rapports à cet égard, ainsi que les processus de gestion des exceptions;
- la gestion des risques singuliers posés par les menaces et technologies émergentes;
- la reddition de comptes auprès de la haute direction sur les indicateurs, les expositions et les tendances de la propension à prendre des risques liés aux technologies et des cyberrisques afin d'éclairer le profil de risque actuel et émergent de l'IFF.

Veuillez consulter la ligne directrice Gouvernance d'entreprise du BSIF pour connaître les attentes de ce dernier à l'égard des fonctions de supervision des IFF, notamment la gestion du risque, la conformité et l'audit interne.

2. Activités et résilience technologiques

Résultat attendu : L'environnement technologique est stable, extensible et résilient, et il est tenu à jour et soutenu par des processus d'exploitation et de reprise technologiques robustes et durables.

2.1 Architecture technologique

Principe 4 : L'IFF doit mettre en œuvre un cadre d'architecture technologique assorti de processus de soutien pour s'assurer que les solutions sont conçues conformément aux exigences opérationnelles, technologiques et liées à la sécurité.

2.1.1 Le cadre d'architecture permet de s'assurer que la technologie répond aux besoins opérationnels

L'IFF doit établir un cadre réunissant les principes nécessaires à la gouvernance, à la gestion, à l'évolution et à la mise en œuvre uniforme de l'architecture des TI à l'échelle de l'institution pour appuyer les objectifs et les exigences stratégiques de l'entreprise en matière de technologie, de sécurité et d'affaires.

2.1.2 L'architecture est complète

La portée des principes de l'architecture doit être complète (c.-à-d. qu'elle doit notamment tenir compte de l'infrastructure, des applications, des technologies émergentes et des données pertinentes). Suivant une approche fondée sur le risque, les systèmes et l'infrastructure connexe doivent être conçus et mis en œuvre pour assurer la disponibilité, l'extensibilité, la sécurité (« sécurité dès la conception ») et la résilience (« résilience dès la conception »), à la mesure des besoins opérationnels.

2.2 Gestion des actifs technologiques

Principe 5 : L'IFF doit tenir un inventaire à jour de tous les actifs technologiques à l'appui des processus ou fonctions opérationnels. Les processus de gestion des actifs de l'IFF doit traiter du classement des actifs pour faciliter le recensement et l'évaluation des risques, consigner les configurations pour assurer l'intégrité des actifs, prévoir l'aliénation sécurisée des actifs à la fin de leur cycle de vie et surveiller et gérer le caractère actuel des technologies.

2.2.1 Des normes de gestion des actifs technologiques sont établies

L'IFF doit établir des normes et des procédures pour gérer les actifs technologiques.

2.2.2 Un inventaire est tenu est à jour et les actifs sont catégorisés

L'IFF doit tenir à jour un système complet de gestion des actifs, ou inventaire, qui répertorie les actifs technologiques tout au long de leur cycle de vie. Selon la tolérance au risque de l'IFF, cet inventaire peut comprendre les actifs détenus ou loués par une IFF et les actifs de tiers utilisés pour stocker ou traiter des renseignements de l'IFF ou pour fournir des services opérationnels essentiels. Le système de gestion des actifs, ou inventaire, doit être appuyé par les éléments suivants :

- Des processus permettant de répertorier les actifs technologiques en fonction de leur criticité et/ou de leur classification. Ces processus doivent permettre de recenser les actifs technologiques essentiels qui ont une grande importance pour l'IFF, ou qui pourraient attirer des auteurs de menaces ou être la cible de

cyberattaques, et qui nécessitent donc des mesures de cyberprotection renforcées;

- Une documentation des interdépendances entre les actifs technologiques essentiels, s'il y a lieu, pour permettre la mise en place de processus appropriés de gestion des changements et de la configuration et pour aider à répondre aux incidents opérationnels et de sécurité, y compris les cyberattaques.

2.2.3 L'inventaire permet de répertorier et de gérer les configurations des actifs technologiques

L'inventaire des technologies doit également comprendre un système de consignation et de gestion des configurations des actifs pour accroître la visibilité et atténuer le risque de pannes technologiques et d'activités non autorisées. Des processus doivent être en place pour repérer, évaluer et corriger les écarts par rapport à la configuration de référence approuvée, et pour rendre compte des manquements.

2.2.4 Des normes d'aliénation sécurisée des actifs technologiques sont établies

L'IFF doit définir des normes et mettre en œuvre des processus pour assurer l'aliénation ou la destruction sécurisée des actifs technologiques.

2.2.5 Le caractère actuel des actifs technologiques est évalué et géré de manière assidue

L'IFF doit assidûment surveiller le caractère actuel des actifs logiciels et matériels utilisés dans l'environnement technologique à l'appui des processus opérationnels. Elle doit mettre en œuvre de façon anticipée des plans d'atténuation et de gestion du risque découlant d'actifs non corrigés, périmés ou non soutenus, et remplacer ou mettre à niveau les actifs avant que les activités de maintenance ne cessent.

2.3 Gestion de projets technologiques

Principe 6 : Des processus efficaces sont en place pour régir et gérer les projets technologiques, du début à la fin, afin de s'assurer que les résultats des projets sont conformes aux objectifs opérationnels et qu'ils sont atteints en tenant compte de la propension de l'IFF à prendre des risques.

2.3.1 Les projets technologiques sont régis par un cadre organisationnel

Les projets technologiques se distinguent souvent par leur ampleur, par les investissements requis et par leur importance dans la réalisation de la stratégie globale de l'IFF. Par conséquent, ils doivent être régis par un cadre organisationnel de gestion de projets qui prévoit des approches cohérentes et l'obtention de résultats de projet qui appuient la stratégie technologique de l'IFF. L'IFF doit évaluer et surveiller les résultats obtenus dans le cadre des différents projets et les risques connexes, et en rendre compte périodiquement.

2.4 Cycle de développement des systèmes

Principe 7 : L'IFF doit mettre en œuvre un cadre du cycle de développement des systèmes (CDS) pour assurer le développement, l'acquisition et l'entretien sécurisés de systèmes technologiques qui fonctionnent comme prévu à l'appui des objectifs opérationnels.

2.4.1 Le cadre du cycle de développement des systèmes guide le développement des systèmes et des logiciels

Le cadre du CDS doit décrire les processus et les mesures de contrôle à chaque étape du cycle afin de garantir la sécurité et la fonctionnalité des systèmes, tout en s'assurant que les systèmes et les logiciels fonctionnent comme prévu pour appuyer les objectifs opérationnels [3] . Le cadre du CDS peut comprendre les méthodes de développement de logiciels adoptées par l'IFF (p. ex., Agile, Waterfall).

2.4.2 Les exigences en matière de sécurité sont intégrées à toutes les étapes du cycle de développement des systèmes

Outre les processus et contrôles technologiques généraux, l'IFF doit établir des points de contrôle pour s'assurer que les exigences et les attentes en matière de sécurité sont intégrées à chaque étape du cycle. S'agissant des méthodes de développement de logiciels Agile, l'IFF doit continuer d'intégrer les principes du CDS et de sécurité dès la conception qui sont nécessaires tout au long de son processus Agile.

2.4.3 Les contrôles et exigences de sécurité sont intégrés aux activités technologiques et de développement

En intégrant les contrôles et les exigences de sécurité des applications dans le développement de logiciels et les activités technologiques, de nouveaux logiciels et services peuvent être livrés rapidement sans compromettre la sécurité des applications. Lorsque ces pratiques [4] sont utilisées, l'IFF doit s'assurer qu'elles sont conformes au cadre du CDS et aux politiques et normes applicables en matière de technologie et de cybersécurité.

2.4.4 Les risques associés aux systèmes et aux logiciels acquis sont évalués

Pour les logiciels et les systèmes acquis, l'IFF doit s'assurer que les évaluations du risque lié à la sécurité sont effectuées et que la mise en œuvre des systèmes est assujettie aux exigences de contrôle qu'impose son cadre du CDS.

2.4.5 Les principes de programmation assurent un code sûr et stable

L'IFF doit définir et mettre en œuvre des principes de programmation et des pratiques exemplaires (p. ex., programmation sécurisée, utilisation de codes de tiers et de codes sources ouverts, référentiels et outils de programmation, etc.).

2.5 Gestion des changements et des versions

Principe 8 : L'IFF doit établir et mettre en œuvre un processus de gestion des changements technologiques et élaborer la documentation connexe pour s'assurer que les changements apportés aux actifs technologiques sont effectués d'une manière contrôlée qui réduit au maximum la perturbation de l'environnement de production.

2.5.1 Les changements apportés aux actifs technologiques sont effectués de manière contrôlée

L'IFF doit veiller à ce que les changements apportés aux actifs technologiques dans l'environnement de production soient documentés, évalués, mis à l'essai, approuvés, mis en œuvre et vérifiés de manière contrôlée. La norme de gestion des changements et des versions doit décrire les principaux contrôles requis tout au long du processus de

gestion des changements. La norme doit également définir les changements urgents et les exigences de contrôle pour s'assurer que ces changements sont mis en œuvre de manière contrôlée et assortis de mesures de protection adéquates.

2.5.2 Contrôle de la séparation des tâches contre les changements non autorisés

La séparation des tâches est une mesure de contrôle clé utilisée pour protéger les actifs contre les changements non autorisés. L'IFF doit séparer les tâches dans le cadre du processus de gestion des changements pour s'assurer qu'une même personne ne peut pas élaborer, autoriser, exécuter et déplacer des codes ou des versions entre les environnements technologiques de production et ceux hors production.

2.5.3 Les changements apportés aux actifs technologiques sont traçables

Des contrôles doivent être mis en œuvre pour assurer la traçabilité et l'intégrité du changement enregistré ainsi que de l'actif modifié (p. ex., code, versions) à chaque étape du processus de gestion des changements.

2.6 Gestion des correctifs

Principe 9 : L'IFF doit mettre en œuvre des processus de gestion des correctifs pour assurer l'application contrôlée et rapide des correctifs à l'échelle de son environnement technologique afin de corriger les vulnérabilités et les défauts.

2.6.1 Les correctifs sont appliqués rapidement et de manière contrôlée

Le processus de gestion des correctifs doit définir clairement les attributions de tous les intervenants. L'application des correctifs doit respecter les processus existants de gestion des changements de l'IFF, y compris les processus de gestion des changements urgents. Tous les correctifs doivent être mis à l'essai avant leur mise en production.

2.7 Gestion des incidents et des problèmes

Principe 10 : L'IFF doit détecter, consigner, gérer, résoudre, suivre et signaler les incidents technologiques de manière efficace et réduire au maximum leurs répercussions.

2.7.1 Les incidents sont gérés de manière à réduire au maximum les répercussions sur les systèmes touchés et les processus opérationnels

L'IFF doit définir des normes et mettre en œuvre des processus de gestion des incidents et des problèmes. Des normes doivent prévoir une structure de gouvernance appropriée qui permet de détecter et de signaler rapidement les incidents, de restaurer et/ou de rétablir un système touché, ainsi que d'enquêter sur les causes profondes des incidents et de les résoudre.

2.7.2 Le processus de gestion des incidents est clair, réactif et fondé sur le risque

L'IFF doit mettre en œuvre des processus et des procédures de gestion des incidents technologiques qui peuvent s'articuler autour des éléments suivants :

- définir et documenter les attributions des intervenants internes et externes pour leur permettre de répondre efficacement aux incidents;
- établir des indicateurs avancés ou des déclencheurs de perturbation des systèmes (c.-à-d. des mesures de détection) qui reposent sur des activités continues d'évaluation des menaces et de surveillance du risque;
- recenser et classer les incidents en fonction de leur priorité, qui dépend de leurs répercussions sur les services opérationnels;
- élaborer et mettre en œuvre des procédures d'intervention en cas d'incident qui atténuent les répercussions des incidents, y compris des mesures de communication interne et externe qui comportent des déclencheurs et des processus de signalement aux échelons supérieurs et de notification;
- effectuer des mises à l'essai et des exercices périodiques à l'aide de scénarios plausibles afin de cerner et de combler les lacunes dans les mesures et les capacités d'intervention en cas d'incident;

- effectuer des exercices et des mises à l'essai périodiques de son processus de gestion des incidents, de ses guides et de ses autres outils d'intervention (p. ex., coordination et communication) pour valider et maintenir leur efficacité;
- établir et mettre à l'essai périodiquement des processus de gestion des incidents avec des fournisseurs tiers.

2.7.3 Des processus sont établis pour enquêter sur les problèmes, les résoudre et en tirer des leçons

L'IFF doit élaborer des processus de gestion des problèmes qui prévoient la détection, la catégorisation, l'enquête et la résolution des causes soupçonnées d'incidents. Les processus doivent comprendre des examens postérieurs à l'incident de même que des diagnostics des causes profondes et des répercussions, et permettre de déterminer des tendances des incidents. Les processus de contrôle connexes sont fonction des activités de gestion des problèmes et des constatations qui en découlent, l'objectif étant d'améliorer de façon continuelle les processus et les procédures de gestion des incidents, y compris la gestion des changements et des versions.

2.8 Évaluation et suivi des services technologiques

Principe 11 : L'IFF doit élaborer des normes de service et de capacité ainsi que des processus pour suivre la gestion opérationnelle de la technologie, afin de s'assurer que les besoins opérationnels sont satisfaits.

2.8.1 Le rendement des services technologiques est évalué, suivi et examiné régulièrement aux fins d'amélioration

L'IFF doit établir des normes de gestion des services technologiques assorties d'indicateurs de rendement et/ou de cibles de service définis qui peuvent servir à évaluer et à suivre la prestation des services technologiques. Les processus doivent également prévoir la mise en place de correctifs lorsque les cibles ne sont pas atteintes.

2.8.2 Le rendement et la capacité de l'infrastructure technologique sont suffisants

L'IFF doit définir des exigences en matière de rendement et de capacité, accompagnées de seuils d'utilisation de l'infrastructure. Ces exigences doivent faire l'objet d'un suivi continu par rapport à des seuils définis pour s'assurer que le rendement et la capacité technologiques répondent aux besoins opérationnels actuels et futurs.

2.9 Reprise après sinistre

Principe 12 : L'IFF doit établir et tenir à jour un programme organisationnel de reprise après sinistre (PORAS) pour renforcer sa capacité à fournir des services technologiques en cas de perturbation tout en respectant sa tolérance au risque.

2.9.1 Un programme de reprise après sinistre est établi

L'IFF doit élaborer, mettre en œuvre et tenir à jour un PORAS qui énonce l'approche qu'elle adopte pour rétablir les services technologiques en cas de perturbation. L'IFF doit arrimer le programme de reprise après sinistre à son programme de gestion de la continuité des activités. Le PORAS doit établir :

- la reddition de comptes et la responsabilité à l'égard de la disponibilité et du rétablissement des services technologiques, y compris les mesures de reprise;
- un processus de détermination et d'analyse des services technologiques et des principales dépendances nécessaires pour fonctionner dans le respect de la tolérance au risque de l'IFF;
- les plans, les procédures et/ou les capacités de rétablissement des services technologiques à un niveau acceptable, et dans un délai acceptable, selon la définition et les priorités établies par l'IFF;
- une politique ou une norme définissant les mesures de contrôle à appliquer aux processus de sauvegarde et de récupération des données, les exigences en matière de stockage des données et les tests à effectuer périodiquement.

2.9.2 Les principales dépendances sont gérées par l'IFF

L'IFF doit gérer les principales dépendances requises pour appuyer le PORAS, notamment :

- les exigences en matière de sécurité de l'information afférentes aux données et à leur stockage (p. ex., le chiffrement);
- l'emplacement des centres d'actifs technologiques, des sites de sauvegarde et des fournisseurs de services, et la proximité des centres de données principaux et d'autres emplacements d'actifs technologiques

essentiels.

Principe 13 : L'IFF doit mettre à l'essai des scénarios sur les capacités de reprise après sinistre pour confirmer que ses services technologiques fonctionnent comme prévu en période de perturbation.

2.9.3 Les scénarios de reprise après sinistre sont testés

Pour promouvoir l'apprentissage, l'amélioration continue et la résilience technologique, l'IFF doit valider régulièrement ses stratégies, plans et/ou capacités de reprise après sinistre, en fonction de scénarios graves mais plausibles, et à ce qu'elle en rende compte. Ces scénarios doivent être prospectifs et couvrir, le cas échéant :

- les risques ou menaces nouveaux et émergents;
- les changements importants apportés aux technologies ou aux objectifs opérationnels;
- les situations qui peuvent entraîner une panne prolongée;
- l'historique des incidents et les complexités ou faiblesses technologiques connues.

Les scénarios de reprise après sinistre de l'IFF doivent vérifier :

- les capacités et les processus de sauvegarde et de reprise de l'IFF afin de valider les stratégies, les plans et les mesures de résilience et de confirmer la capacité de l'organisation à satisfaire aux exigences prédéfinies;
- les technologies essentielles de tiers et les points d'intégration avec dépendances en amont et en aval, y compris la technologie sur place et hors des locaux.

3. Cybersécurité

Résultat attendu : Une posture technologique sûre qui préserve la confidentialité, l'intégrité et la disponibilité des actifs technologiques de l'IFF.

3.0 La confidentialité, l'intégrité et la disponibilité des actifs technologiques sont protégées

L'IFF doit, de façon anticipée, déterminer et détecter les cybermenaces, les cyberévénements et les cyberincidents externes et internes, se protéger à leur encontre et y réagir et s'en remettre afin de préserver la confidentialité, l'intégrité et la disponibilité de ses actifs technologiques.

3.1 Identifier

Principe 14 : L'IFF doit disposer d'une gamme de pratiques, de capacités, de processus et d'outils pour identifier et évaluer les faiblesses en matière de cybersécurité qui pourraient être exploitées par les auteurs de menaces externes et internes.

3.1.1 Les risques liés à la sécurité sont recensés

L'IFF doit recenser les cybermenaces actuelles ou émergentes de façon anticipée en les évaluant afin de déterminer les menaces et les risques liés à la sécurité. Cela comprend la mise en œuvre d'évaluations, de processus et d'outils axés sur les menaces et les risques liés à la sécurité de l'information et à la cybersécurité pour assurer des mesures de contrôle aux différents niveaux de défense.

3.1.2 Les menaces font l'objet d'évaluations et de mises à l'essai fondées sur le renseignement

L'IFF doit adopter une approche fondée sur le risque pour évaluer les menaces et effectuer des mises à l'essai. L'IFF doit définir des déclencheurs et des fréquences minimales pour les évaluations des menaces fondées sur le renseignement afin de mettre à l'essai les processus et contrôles de cybersécurité. En outre, l'IFF doit régulièrement effectuer des mises à l'essai et des exercices pour cerner les vulnérabilités ou les lacunes de contrôle de ses programmes de cybersécurité (p. ex., tests d'intrusion et méthode de l'équipe rouge) au moyen d'une approche fondée sur le renseignement. La portée et les répercussions potentielles de ces mises à l'essai doivent être clairement définies par l'IFF, et des contrôles efficaces d'atténuation du risque doivent être appliqués tout au long de l'évaluation pour gérer les risques inhérents connexes.

3.1.3 Les vulnérabilités sont recensées, évaluées et classées

L'IFF doit établir des processus pour effectuer des évaluations régulières de la vulnérabilité de ses actifs technologiques, y compris, sans s'y limiter, les dispositifs, systèmes et applications réseau. Les processus doivent préciser la fréquence à laquelle les analyses et les évaluations de la vulnérabilité sont effectuées. L'IFF doit évaluer et classer les cybervulnérabilités et les cybermenaces pertinentes selon la gravité de la menace et de l'exposition des actifs technologiques au risque à l'aide d'une méthode normalisée d'évaluation du risque. Ce faisant, l'IFF doit tenir compte de l'impact cumulatif potentiel des vulnérabilités, quel que soit le niveau de risque, qui pourraient présenter un risque élevé une fois combinées.

3.1.4 Les données sont recensées, classifiées et protégées

L'IFF doit veiller à ce que des contrôles adéquats soient en place pour recenser, classifier et protéger les données structurées et non structurées, en fonction de leur niveau de confidentialité. L'IFF doit mettre en œuvre un processus pour effectuer des analyses de reconnaissance périodiques afin de détecter les changements et les écarts par rapport aux normes et aux contrôles établis et protéger ainsi les données contre un accès non autorisé.

3.1.5 La connaissance situationnelle et le partage d'informations sont assurés en continu

L'IFF doit continuellement assurer une connaissance situationnelle du contexte externe des cybermenaces et de son propre environnement de menaces en ce qui concerne ses actifs technologiques. Il peut s'agir de participer à des forums sectoriels de renseignements sur les menaces et de partage d'informations ou de s'abonner à des sources d'information sur les menaces fiables et pertinentes. Dans la mesure du possible, l'IFF est invitée à assurer un échange rapide de renseignements sur les menaces pour faciliter la prévention des cyberattaques, contribuant ainsi à sa propre cyberrésilience et à celle du secteur financier en général.

3.1.6 Des exercices de modélisation des menaces et des chasses aux menaces sont effectués

Dans la mesure du possible, l'IFF doit tenir à jour des modèles de cybermenaces pour repérer les menaces à la cybersécurité qui touchent directement ses actifs et ses services technologiques. Les menaces doivent être évaluées régulièrement afin d'améliorer le programme de cybersécurité, les capacités et les contrôles nécessaires

pour atténuer les menaces actuelles et émergentes. L'IFF doit utiliser des techniques manuelles pour repérer et isoler de façon anticipée les menaces qui ne sont pas détectées par les outils automatisés (p. ex., chasse aux menaces).

3.1.7 La sensibilisation à la cybersécurité est encouragée et mise à l'essai

L'IFF doit permettre à ses employés, à ses clients et à ses tiers de signaler les cyberactivités suspectes et les y encourager, en reconnaissant le rôle que chacun peut jouer dans la prévention des cyberattaques. L'IFF doit sensibiliser les employés, les clients et les tiers concernés sur les scénarios de cyberattaque qui les ciblent directement. En outre, l'IFF doit régulièrement évaluer les connaissances des cybermenaces de ses employés et l'efficacité des processus et outils de signalement.

3.1.8 Le profil de cyberrisque fait l'objet d'un suivi et de rapports

L'IFF doit tenir à jour un profil de cyberrisque complet pour faciliter la supervision et la prise de décisions dans les meilleurs délais, et elle doit en rendre compte. Le profil doit s'appuyer sur les sources, processus, outils et capacités internes et externes existants de recensement et d'évaluation du risque. L'IFF doit également veiller à ce que des processus et des outils soient en place pour évaluer, surveiller et regrouper les risques résiduels.

3.2 Protéger

Principe 15 : L'IFF doit concevoir, mettre en œuvre et tenir à jour des mesures et des contrôles de cybersécurité multicouches et préventifs pour protéger ses actifs technologiques.

3.2.1 Des pratiques de type « sécurité dès la conception » sont adoptées

L'IFF doit adopter des pratiques de type « sécurité dès la conception » pour protéger ses actifs technologiques. Les contrôles de défense de la sécurité sont censés être préventifs, dans la mesure du possible, et l'IFF doit examiner régulièrement les cas d'utilisation des contrôles de sécurité en vue de recourir davantage à des contrôles préventifs plutôt qu'à des contrôles de détection. Les contrôles de sécurité normalisés doivent être appliqués de bout en bout, dès la conception, aux applications, aux micro-services et aux interfaces de programmation élaborées par l'IFF.

3.2.2 Des technologies cryptographiques solides et sécurisées sont utilisées

L'IFF doit mettre en œuvre et maintenir de solides technologies cryptographiques pour protéger l'authenticité, la confidentialité et l'intégrité de ses actifs technologiques. Cela comprend des contrôles pour la protection des clés de chiffrement contre tout accès, utilisation et divulgation non autorisés tout au long du cycle de vie de gestion des clés cryptographiques. L'IFF doit évaluer régulièrement sa norme et ses technologies de cryptographie pour s'assurer qu'elles demeurent efficaces contre les menaces actuelles et émergentes.

3.2.3 Des contrôles et des fonctionnalités améliorés sont appliqués pour protéger les actifs technologiques essentiels et externes

L'IFF doit disposer de contrôles et de fonctionnalités renforcés pour contenir rapidement les menaces à la cybersécurité, défendre ses actifs technologiques essentiels et demeurer résiliente contre les cyberattaques. À cette fin, elle peut envisager les éléments suivants :

- déterminer les contrôles de cybersécurité requis pour protéger ses actifs technologiques essentiels;
- concevoir des contrôles d'applications pour contenir et limiter les répercussions d'une cyberattaque;
- mettre en œuvre, surveiller et examiner les normes de sécurité appropriées, les configurations de référence et les exigences de renforcement de la sécurité;
- déployer des couches supplémentaires de contrôles de sécurité, de façon appropriée, pour se défendre contre les cyberattaques (p. ex., attaques volumétriques, réseau faible/lent et attaques logiques d'applications).

3.2.4 Les contrôles de cybersécurité sont stratifiés

L'IFF doit mettre en œuvre et maintenir plusieurs niveaux de contrôles de cybersécurité et se défendre contre les menaces à chaque étape du cycle de vie des attaques (p. ex., depuis la reconnaissance et l'accès initial jusqu'à l'exécution des objectifs). L'IFF doit également faire preuve de résilience face aux cybermenaces actuelles et émergentes en maintenant des contrôles et des outils de défense. Pour ce faire, elle doit notamment s'assurer de l'efficacité opérationnelle continue des contrôles en réduisant au maximum les faux positifs. Dans la mesure du

possible, l'IFF doit :

- protéger tous ses réseaux, y compris ses services externes, contre les menaces en réduisant au maximum sa surface d'attaque;
- définir les zones de réseau logique autorisées et appliquer des contrôles pour séparer et limiter ou bloquer l'accès et le trafic à destination et en provenance des zones de réseau;
- tirer parti d'une combinaison de listes d'acceptation et de refus, y compris la vérification de l'intégrité des fichiers (p. ex., hachage/signature de fichier) et les indicateurs de compromission, en plus des capacités avancées de protection fondées sur le comportement qui sont continuellement mises à jour;
- appliquer des contrôles et des dispositifs de défense visant la prévention et la détection des intrusions dans le périmètre de son réseau, en plus des mécanismes de contrôle des pertes de données, des programmes malveillants et des virus.

3.2.5 Des contrôles de sécurité pour protéger les données et en prévenir la perte sont mis en œuvre

À partir d'une classification claire de ses données, l'IFF doit concevoir et mettre en œuvre des contrôles fondés sur le risque pour protéger ses données tout au long de leur cycle de vie, ce qui comprend des dispositifs et des contrôles de prévention de la perte de données et des contrôles pour les données au repos, les données en transit et les données utilisées.

3.2.6 Les vulnérabilités de sécurité sont corrigées

Pour s'assurer que les vulnérabilités de sécurité sont bien gérées, l'IFF doit :

- maintenir les capacités pour assurer l'application rapide de correctifs fondés sur le risque aux vulnérabilités des logiciels des fournisseurs et des applications internes qui tiennent compte de la gravité de la menace et de la vulnérabilité des systèmes exposés;
- appliquer les correctifs le plus tôt possible, en fonction des risques et des échéanciers définis;
- mettre en œuvre des contrôles compensatoires au besoin pour atténuer suffisamment le risque lorsqu'aucune mesure de correction n'est disponible (p. ex., attaques du jour zéro);

- surveiller régulièrement l'état des correctifs et la correction des vulnérabilités par rapport aux échéanciers définis, y compris tout arriéré et toute exception, et en rendre compte.

3.2.7 Des contrôles de gestion de l'identité et de l'accès sont mis en œuvre

L'IFF doit mettre en œuvre des contrôles de l'identité et de l'accès fondés sur le risque, y compris l'authentification multifactorielle (AMF) [5] et la gestion de l'accès privilégié. Dans la mesure du possible, l'IFF doit :

- appliquer les principes du droit d'accès minimal, établir régulièrement une attestation d'accès et veiller à l'utilisation de mots de passe complexes difficiles à deviner pour authentifier l'accès des employés, des clients et des tiers aux actifs technologiques;
- mettre en œuvre l'AMF pour les canaux externes et comptes privilégiés (p. ex., clients, employés et tiers);
- gérer les justificatifs d'identité des comptes privilégiés au moyen d'une chambre forte sécurisée;
- assurer l'enregistrement et le suivi des activités du compte dans le cadre du suivi continu de la sécurité;
- assurer l'authentification, la gestion et le suivi sécurisés des comptes des systèmes et des services pour détecter toute utilisation non autorisée;
- mener la vérification appropriée des antécédents, dans la mesure du possible, des personnes qui ont accès aux systèmes ou aux données de l'IFF, en fonction de la criticité et de la classification des actifs technologiques.

3.2.8 Les configurations de sécurité de base sont appliquées et les écarts sont gérés

L'IFF doit mettre en œuvre des configurations de base approuvées fondées sur le risque pour les actifs technologiques et les outils de défense de sécurité, y compris ceux fournis par des tiers. Dans la mesure du possible, les configurations de sécurité de base pour différents niveaux de défense doivent viser la désactivation des paramètres et de l'accès par défaut. L'IFF doit définir et mettre en œuvre des processus pour gérer les écarts de configuration.

3.2.9 Des capacités d'analyse et de mise à l'essai des applications sont utilisées

Dans la mesure du possible, l'IFF doit utiliser des capacités d'analyse et de mises à l'essai statiques ou dynamiques pour s'assurer que les vulnérabilités des systèmes et applications nouveaux ou modifiés sont évaluées avant leur mise en production. Des contrôles de sécurité doivent également être mis en œuvre pour maintenir la sécurité lorsque les pratiques de développement et d'exploitation sont combinées par un pipeline de développement continu et automatisé (voir le paragraphe 2.4.2).

3.2.10 Des contrôles et des processus d'accès physique sont appliqués

L'IFF doit définir et mettre en œuvre des contrôles et des processus de gestion de l'accès physique pour protéger l'infrastructure réseau et les autres actifs technologiques contre l'accès non autorisé et les dangers environnementaux.

3.3 Détecter

Principe 16 : L'IFF conçoit, met en œuvre et maintient des capacités continues de détection de sécurité pour permettre le suivi, le signalement et la réalisation d'enquêtes criminalistiques.

3.3.1 Une journalisation de sécurité continue et centralisée est assurée à l'appui des enquêtes

L'IFF doit veiller à une journalisation de sécurité continue des actifs technologiques et des différentes couches d'outils de défense. Les outils centraux permettant de regrouper, de corréler et de gérer les journaux des événements liés à la sécurité devraient permettre un accès rapide aux journaux durant une enquête sur un cyberévénement. Pour tout cyberincident ou cybermenace important, l'enquête criminalistique de l'IFF ne doit pas être limitée ou retardée par des journaux désagrégés, inaccessibles, ou incomplets (c'est-à-dire des événements de sécurité critiques manquants ou non répertoriés). L'IFF doit instaurer des périodes minimales de conservation des journaux de sécurité et tenir à jour des journaux des cyberévénements pour faciliter une enquête criminalistique approfondie et sans entrave sur ces événements.

3.3.2 Les activités malveillantes et non autorisées sont détectées

L'IFF doit maintenir des capacités de gestion de l'information et des événements liés à la sécurité pour assurer la détection et le signalement continus des activités malveillantes et non autorisées des utilisateurs et des systèmes. Dans la mesure du possible, des méthodes élaborées de détection et de prévention fondées sur le comportement doivent être utilisées pour détecter les anomalies de comportement des utilisateurs et des entités et les menaces externes et internes émergentes. Afin de poursuivre l'amélioration de ses outils de suivi, l'IFF doit se fier aux plus récents renseignements sur les menaces et indicateurs de compromission.

3.3.3 Les alertes de cybersécurité font l'objet d'un triage

L'IFF doit définir les attributions pour permettre le triage des alertes de cybersécurité à risque élevé afin de contenir et d'atténuer rapidement les cybermenaces importantes avant qu'elles ne donnent lieu à un incident de sécurité important ou à une perturbation opérationnelle.

3.4 Répondre, rétablir et apprendre

Principe 17 : L'IFF doit répondre aux cyberincidents ayant une incidence sur ses actifs technologiques, y compris les incidents provenant de tiers fournisseurs, les contenir, s'en remettre et en tirer des enseignements.

3.4.1 Les capacités d'intervention en cas d'incident sont intégrées et harmonisées

Le deuxième domaine (activités et résilience technologiques) énonce les attentes fondamentales à l'égard des capacités de gestion des incidents et des problèmes de l'IFF. L'IFF doit assurer la concordance de ses protocoles de cybersécurité, de technologie, de gestion de crises et de communication. Ces protocoles doivent comprendre toutes les étapes du signalement rapide aux échelons supérieurs et la coordination des intervenants (internes et externes) à la suite d'un cyberévénement ou cyberincident majeur.

3.4.2 La taxonomie des cyberincidents est définie

L'IFF doit clairement définir et adopter une taxonomie des cyberincidents qui permet de classer les cyberincidents et les incidents de sécurité de l'information selon des critères précis, comme la gravité, la catégorie, le type et la cause profonde. Elle doit être conçue pour aider l'IFF à répondre aux cyberincidents, à les gérer et à en rendre compte.

3.4.3 Le processus et les outils de gestion des cyberincidents sont tenus à jour

L'IFF doit tenir à jour un processus et des guides de gestion des cyberincidents pour en assurer la gestion rapide et efficace.

3.4.4 Des capacités d'intervention, de confinement et de rétablissement rapides sont établies

L'IFF doit mettre sur pied une équipe d'intervention en cas de cyberincident dotée en permanence d'outils et de capacités pour répondre rapidement aux cyberévénements et cyberincidents qui pourraient avoir une incidence importante sur ses actifs technologiques, ses clients et d'autres intervenants, pour les contenir et pour pouvoir s'en remettre.

3.4.5 Des enquêtes criminalistiques et des analyses des causes profondes sont menées au besoin

L'IFF doit mener une enquête criminalistique à la suite d'un incident qui a pu exposer ses actifs technologiques à un risque important. Après un incident très grave, l'IFF doit effectuer une évaluation détaillée des répercussions directes et indirectes (financières et/ou non financières) et une analyse des causes profondes pour déterminer les mesures correctives à prendre, s'attaquer à la cause profonde et donner suite aux leçons tirées. L'analyse des causes profondes doit évaluer les menaces, les faiblesses et les vulnérabilités des personnes, des processus, de la technologie et des données.

Notes de bas de page

1 Les « succursales de banques étrangères » sont des banques étrangères autorisées à exercer leurs activités au Canada par l'exploitation de succursales en vertu de la partie XII.1 de la *Loi sur les banques*. Les « succursales de sociétés d'assurance étrangères » sont des entités étrangères qui sont autorisées à garantir au Canada des risques par l'exploitation de succursales en vertu de la partie XIII de la *Loi sur les sociétés d'assurances*.

2 Les définitions utilisées dans la ligne directrice B-13 sont fondées sur celles d'organismes de normalisation reconnus. Les IFF peuvent donc recourir aux définitions établies par ces organismes pour les termes techniques employés dans la ligne directrice.

3 Le cadre du cycle de développement des systèmes (CDS) est le processus global de développement, de mise en œuvre et de retrait des systèmes d'information au moyen d'un processus en plusieurs étapes allant du lancement à l'aliénation, en passant par l'analyse, la conception, la mise en œuvre et l'entretien (NIST Special Publication 800-100). Les méthodes de développement de logiciels (p. ex., Agile, Waterfall) sont axées sur une composante particulière du développement de systèmes, tandis que le CDS est un processus plus global pour le cycle de vie de bout en bout d'un système.

4 Ces pratiques sont communément appelées « DevSecOps » (développement, sécurité, opérations).

5 L'AMF utilise des facteurs d'authentification indépendants qui comprennent généralement un élément que l'utilisateur a) **connaît**, comme un mot de passe ou un NIP; b) **possède**, comme un dispositif ou un jeton d'identification cryptographique; et/ou c) **est**, comme ses caractéristiques biométriques ou son comportement.