BANQUE DU CANADA
BANK OF CANADA

Cyberrésilience : attentes à l'égard des infrastructures de marchés financiers

Octobre 2021

Table des matières

Introduction 5

Objet 5

Démarche 6

Structure 6

Applicabilité des attentes 7

Gestion des cyberrisques résultant des interconnexions 8

1 Gouvernance 10

1.1 Préambule 10

1.2 Stratégie de cyberrésilience 10

1.3 Cadre de cyberrésilience 11

1.4 Rôles du conseil d'administration et de la direction générale 13

1.4.1 Responsabilités du conseil d'administration et de la direction générale 13

1.4.2 Culture 15

1.4.3 Compétences et responsabilités 15

2 Identification 16

2.1 Préambule 16

2.2 Identification et catégorisation 16

2.2.1 Identification des fonctions et processus opérationnels 16

2.2.2 Identification des actifs informationnels et accès connexe 16

2.2.3 Examen et mise à jour périodiques 18

2.3 Interconnexions 18

3 Protection 18

3.1 Préambule 18

3.2 Protection des processus et des actifs 19

3.2.1 Résilience dès la conception 19

3.2.2 Contrôles 20

3.2.3 Exemples de contrôles solides relatifs aux TIC 20

3.2.4 Protection par couches facilitant l'intervention et le rétablissement 25

3.3 Interconnexions 27

3.3.1 Risques liés aux interconnexions 27

3.4 Menaces internes 28

3.4.1 Analyse de la cybersécurité 28

3.4.2 Changements de la situation d'emploi 28

3.4.3 Contrôle de l'accès 29

3.5 Formation 32

3.5.1 Ensemble du personnel de l'IMF 32

3.5.2 Groupes à risque élevé 32

4 Détection 33

4.1 Préambule 33

4.2 Surveillance continue 33

4.3 Cadre de surveillance complet 34

4.4 Détection en couches 35

4.5 Intervention en cas d'incident 35

5 Intervention et rétablissement 36

5.1 Préambule 36

5.2 Intervention en cas d'incident, reprise des activités et rétablissement 36

5.2.1 Planification et préparation 36

5.2.2 Reprise des activités dans un délai de deux heures (objectif de temps de récupération) 37

5.2.3 Plans d'urgence 38

5.2.4 Intervention en cas d'incident et enquête 39

5.2.5 Capacité d'investigation numérique 39

5.3 Éléments liés à la conception 40

5.3.1 Conception et intégration opérationnelle 40

5.3.2 Intégrité des données 41

5.4 Interconnexions 42

5.4.1 Accords de partage de données 42

5.4.2 Contagion 42

5.4.3 Communication en cas de crise 43

5.4.4 Politique de divulgation responsable 43

6 Tests 43

6.1 Préambule 43

6.2 Programme exhaustif de tests 44

6.2.1 Méthodes, pratiques et outils 44

6.3 Coordination 47

7 Connaissance de la situation 48

7.1 Préambule 48

7.2 Renseignements sur les cybermenaces 48

7.3 Partage d'information 51

8 Apprentissage et évolution 52

8.1 Préambule 52

8.2 Apprentissage continu 52

8.2.1 Leçons tirées des cyberévénements 52

8.2.2 Acquisition de connaissances et de capacités 53

8.2.3 Capacité prédictive 53
8.3 Évaluation comparative de la cyberrésilience 53
8.3.1 Indicateurs 53
Annexe A: Glossaire 55

Introduction

Une cyberattaque contre le système financier pourrait provoquer un événement systémique qui aurait de graves répercussions sur la stabilité financière et sur la confiance globale dans le système financier. La stabilité financière est fortement tributaire du fonctionnement sûr et efficient des infrastructures de marchés financiers (IMF). En l'absence d'une gestion adéquate, les IMF peuvent être un vecteur de transmission des chocs au sein des marchés financiers nationaux et internationaux engendrant des répercussions économiques néfastes. Dans ce contexte, la cyberrésilience des IMF est une composante essentielle de la sécurité et de l'efficience du système financier.

En juin 2016, le Comité sur les paiements et les infrastructures de marché (CPIM) et l'Organisation internationale des commissions de valeurs (OICV) ont rédigé le document *Guidance on cyber resilience for financial market infrastructures* (le document d'orientation) en complément aux *Principes pour les infrastructures de marchés financiers* (PIMF) publiés par les deux organismes en avril 2012[1]. Le document d'orientation décrit plus en détail les dispositions et les mesures que les IMF devraient prendre pour accroître leur niveau de cyberrésilience. La Banque du Canada (la Banque) s'attend à ce que les IMF désignées respectent les dispositions du document d'orientation.

Comme l'environnement des cybermenaces est de plus en plus sophistiqué et complexe, et que la technologie progresse constamment, il devient nécessaire de s'adapter en améliorant et en renforçant les pratiques de cyberrésilience tout en tenant compte des évolutions pertinentes dans ce domaine. La Banque a rédigé le présent document comme un outil pour compléter le document d'orientation et communiquer clairement ses attentes en la matière aux organes de surveillance et aux IMF. Pour que ce document demeure pertinent au regard des évolutions futures, des sections supplémentaires portant sur des sujets précis pourront être ajoutées ultérieurement.

Objet

Le présent document intitulé *Cyberrésilience : attentes à l'égard des infrastructures de marchés financiers* complète le document d'orientation. Dans une optique de clarification et de transparence, il précise aux organes de surveillance et aux IMF comment appliquer le document d'orientation afin de continuellement améliorer la cyberrésilience des IMF. Par l'entremise du présent document, la Banque communiquera ses attentes de façon claire et uniforme à toutes les IMF désignées au pays, ce qui contribuera à la gestion adéquate des cyberrisques au sein du système financier canadien et fournira l'assurance du maintien de la stabilité financière.

[1] La Banque a adopté les PIMF comme ses normes de gestion des risques pour les systèmes de compensation et de règlement désignés (c.-à-d. les IMF).

Bien que le présent document s'adresse directement aux IMF, il importe que celles-ci communiquent activement avec leurs participants et les autres parties prenantes concernées pour favoriser la compréhension des objectifs de cyberrésilience, l'adhésion à ceux-ci ainsi que leur mise en œuvre. Étant donné les nombreuses interconnexions au sein du système financier, la cyberrésilience d'une IMF dépend en partie de celle des autres IMF, des prestataires de services et des participants.

Démarche

Des experts de la Banque ont procédé à un examen des principales normes internationales (p. ex., le cadre de cybersécurité et la série 800 des publications spéciales du National Institute of Standards and Technology [NIST], la norme ISO/IEC 27001/27002 et le référentiel COBIT 2019) afin d'identifier les domaines pertinents pour les IMF et conformes aux attentes énoncées dans le document d'orientation. La Banque s'est également inspirée d'autres orientations émises par les organismes de réglementation, notamment le document *Cyber resilience oversight expectations for financial market infrastructures* de la Banque centrale européenne et l'outil d'évaluation de la cybersécurité du Federal Financial Institutions Examination Council. En outre, les experts de la Banque ont examiné et évalué les évolutions récentes qui devraient être prises en compte pour concevoir un programme de cyberrésilience actuel et robuste. En se fondant sur leurs conclusions, la Banque a pu clarifier et détailler ses attentes à l'égard des IMF canadiennes. Lors de la rédaction du présent document, la Banque a sollicité les commentaires des IMF désignées.

Structure

Calquées sur les chapitres du document d'orientation, les sections du présent document décrivent cinq grands volets de la gestion des risques et trois éléments principaux qui devraient être couverts dans le cadre de cyberrésilience d'une IMF, respectivement : 1) gouvernance; 2) identification; 3) protection; 4) détection; 5) intervention et rétablissement; et 1) tests; 2) connaissance de la situation; 3) apprentissage et évolution. Chaque section débute par un préambule en italique qui en résume les principaux objectifs et qui est tiré du chapitre correspondant du document d'orientation.

Les sujets abordés dans chaque section sont répartis en sous-sections qui concordent en grande partie avec celles du document d'orientation. Toutefois, à la différence du document d'orientation, la numérotation dans le présent document commence après la section introductive. Chaque sous-section comporte un préambule tiré du document d'orientation ou rédigé par la Banque. Chaque sous-section comprend une liste numérotée d'attentes distinctes qui définissent les mesures concrètes que les IMF peuvent prendre pour mettre en œuvre les dispositions du document d'orientation. De plus, le glossaire du document d'orientation a été bonifié et modifié au besoin, notamment pour tenir compte du contexte canadien.

Applicabilité des attentes

La Banque s'attend à ce que toutes les IMF canadiennes désignées[2] respectent intégralement les dispositions du document d'orientation et tiennent compte des attentes exposées dans le présent document lors de la mise en œuvre de ces dispositions. Si une entité affiliée à une IMF élabore, met en place ou met en application le cadre de cybersécurité de l'IMF, il incombe à cette dernière et à son conseil d'administration de veiller à la bonne application des orientations. L'IMF doit s'assurer que les cyberrisques sont gérés efficacement, conjointement avec l'entité affiliée et conformément à sa stratégie et à ses objectifs de cyberrésilience. Les attentes énoncées dans le présent document s'appliquent donc à l'IMF (le système de compensation et de règlement et sa chambre de compensation) et à toute entité affiliée sur laquelle l'IMF s'appuie pour mettre en œuvre son cadre de cyberrésilience. L'IMF devrait s'aider du présent document pour respecter pleinement les attentes énoncées dans le document d'orientation et atteindre le niveau de cyberrésilience nécessaire au maintien de la stabilité financière.

Comme indiqué dans le document d'orientation, les composantes de l'environnement des technologies de l'information et des communications (TIC) d'une IMF et les entités qui font partie de son écosystème ne présentent pas la même criticité pour son fonctionnement. Les composantes de l'environnement des TIC de l'IMF peuvent aussi être exposées, à divers degrés, à différents types de cyberrisques[3]. Lors de l'application des dispositions du document d'orientation, une IMF se doit d'adopter une approche fondée sur les risques et de hiérarchiser ses mesures d'atténuation proportionnellement aux divers niveaux de cyberrisques auxquels elle est exposée. Le présent document ne se veut pas une liste de vérification ou d'exigences techniques. La Banque évaluera si l'IMF répond aux attentes exposées ci-après conformément à l'approche fondée sur les risques adoptée par l'IMF et au rôle de celle-ci dans le système financier canadien.

La conformité au document d'orientation n'est pas un effort ponctuel. Les IMF devraient s'efforcer d'élever continuellement leur niveau de cybermaturité, notamment en améliorant leurs capacités à reprendre leurs opérations essentielles et à se rétablir d'une cyberattaque réussie. Cette évolution et cette amélioration devraient être l'aboutissement de discussions menées entre l'IMF et la Banque pendant une période prolongée et dans la mesure de la criticité de l'IMF concernée.

---

[2] La *Loi sur la compensation et le règlement des paiements* confère à la Banque du Canada le pouvoir de désigner des systèmes de compensation et de règlement qui engendrent un risque systémique ou un risque pour le système de paiement.

[3] La section 1.3.6 du document d'orientation indique que les cyberrisques posés par les entités de l'écosystème de l'IMF – les participants, les IMF liées, les prestataires de services et les fournisseurs – varieront aussi et pas nécessairement en fonction du degré de pertinence de l'entité par rapport aux activités de l'IMF.

Le document d'orientation repose sur des principes étant donné que la nature dynamique des cybermenaces exige des méthodes d'atténuation en constante évolution. Les attentes à l'égard des IMF concernant la mise en œuvre des dispositions du document d'orientation sont précisées ici, mais la Banque accordera une certaine souplesse dans les méthodes choisies pour s'y conformer. Dans certains cas, le présent document utilise des exemples précis de mesures de cyberrésilience, notamment des contrôles liés aux TIC, pour illustrer et clarifier certains points. Cependant, ces exemples ne visent pas à imposer des exigences particulières ou à signifier l'aval de la Banque quant à l'utilisation de ces contrôles. Le choix et la mise en œuvre des mesures de cyberrésilience devraient être guidés par les évaluations des cyberrisques menées par l'IMF. En outre, en raison du rythme rapide des innovations dans le domaine des technologies de l'information et de l'évolution de l'ensemble des menaces, les pratiques de cyberrésilience peuvent changer au fil du temps.

Les IMF sont hétérogènes : elles diffèrent par leur taille, leurs structures organisationnelle et opérationnelle, leur modèle d'affaires et leur infrastructure. Par conséquent, il est possible qu'elles répondent aux attentes sous-jacentes en utilisant divers processus, technologies ou méthodologies.

Gestion des cyberrisques résultant des interconnexions

Ces dernières années, on observe une hausse des interconnexions entre les IMF et d'autres entités, telles que les participants, les IMF liées, les prestataires de services ainsi que les fournisseurs et leurs produits. Lorsque les IMF modernisent leurs principales fonctions, elles mettent souvent en œuvre des solutions de fournisseurs de services externes, comme des entreprises de technologie financière. Ces interconnexions offrent aux IMF de nombreux avantages (p. ex., innovation accrue, meilleur accès aux technologies de pointe, efficience opérationnelle, produits et services personnalisés, réductions des coûts), mais pourraient poser des défis accrus sur le plan de la gestion des cyberrisques.

Il importe que les IMF désignées gèrent les cyberrisques auxquels elles sont exposées du fait de leurs liens avec d'autres entités en identifiant, en évaluant et en mettant en œuvre de manière appropriée des mesures de protection visant à les atténuer. Chacune des sections du présent document (gouvernance, identification, protection, détection, intervention et rétablissement, tests, connaissance de la situation, apprentissage et évolution) fournit des indications précises quant à la façon dont les IMF désignées peuvent gérer ces risques. La Banque s'attend à ce que les IMF adoptent une approche fondée sur les risques pour mettre en œuvre ses indications sur la gestion des risques résultant des interconnexions.

Distinction entre « reprise des activités » et « rétablissement »

Dans les PIMF et le document d'orientation (ainsi que dans l'ensemble du secteur de la cybersécurité), les termes « reprise des activités » et « rétablissement » sont souvent utilisés, parfois de manière interchangeable. Cependant, il existe des différences subtiles entre les deux termes. La section 17.6 des PIMF stipule que le plan de continuité des opérations de l'IMF devrait prévoir « que des systèmes d'information (SI) essentiels puissent reprendre leur fonctionnement dans les deux heures qui suivent une perturbation ». La section 6.2.2 du document d'orientation évoque une reprise des activités dans un délai de deux heures en utilisant l'acronyme « RTO » (objectif de temps de récupération) qui désigne un rétablissement dans le milieu de la cybersécurité anglophone, ce qui peut être interprété différemment d'une reprise dans un délai de deux heures. Le terme « reprise des activités » se rapporte généralement à la reprise des processus opérationnels, tandis que celui de « rétablissement » désigne le fait de restaurer les systèmes TI et les données à un état de fonctionnement. Cette différence peut prêter à confusion. Dans le contexte d'une cyberattaque, il est raisonnable d'interpréter le concept d'objectif de temps de récupération de deux heures comme désignant le rétablissement des éléments ou des composantes des systèmes TI et des données nécessaires à l'IMF pour reprendre ses opérations essentielles. Il pourrait toutefois être risqué de tenter de rétablir l'intégralité du système en deux heures. Nous nous sommes efforcés de faire cette distinction entre « reprise des activités » et « rétablissement » dans les attentes énoncées tout au long du présent document.

1 Gouvernance

1.1 Préambule

Le terme « cybergouvernance » désigne les dispositions qu'une IMF a prises pour établir, mettre en œuvre et revoir son approche de la gestion des cyberrisques. Une cybergouvernance efficace présuppose un cadre de cyberrésilience clair et complet, qui favorise la sécurité et l'efficience des opérations de l'IMF, et qui contribue à l'atteinte des objectifs de stabilité financière. Ce cadre devrait être guidé par la stratégie de cyberrésilience de l'IMF et définir la manière dont ses objectifs connexes sont déterminés. Il devrait aussi décrire les exigences en matière de ressources humaines, de processus et de technologie pour assurer la gestion des cyberrisques et des communications rapides, en temps opportun, qui permettent à l'IMF de collaborer avec les parties prenantes concernées afin d'intervenir et de rétablir ses opérations de manière efficace en cas de cyberattaque. Le cadre doit reposer sur une définition claire des rôles et des responsabilités du conseil d'administration (ou son équivalent) et de la direction de l'IMF, auxquels il incombe de créer une culture reconnaissant que le personnel à tous les niveaux a une grande part de responsabilité dans la cyberrésilience de l'IMF.

Une solide cybergouvernance au sein de l'IMF est essentielle à la mise en place d'une approche systématique et proactive pour gérer les cybermenaces existantes et nouvelles auxquelles l'IMF est confrontée. La cybergouvernance appuie également les efforts visant à prendre en compte et à gérer de manière appropriée les cyberrisques à tous les niveaux de l'organisation, et à fournir les ressources et l'expertise nécessaires pour composer avec ces risques.

Cette section donne des orientations sur les éléments de base à inclure dans la stratégie et le cadre de cyberrésilience d'une IMF, et sur la manière dont les dispositions relatives à la gouvernance d'une IMF devraient soutenir cette stratégie et ce cadre.

1.2 Stratégie de cyberrésilience

La stratégie de cyberrésilience énonce les principes généraux et les plans à moyen terme de l'IMF pour atteindre son objectif de gestion des cyberrisques.

1. L'IMF devrait élaborer une stratégie de cyberrésilience, avec la participation de toutes les unités organisationnelles concernées. Cette stratégie devrait être arrimée aux stratégies d'entreprise et d'affaires de l'IMF ainsi qu'à ses autres stratégies pertinentes (p. ex., continuité des opérations et TI) et à ses priorités générales en matière d'intervention et de rétablissement.
2. L'IMF devrait s'assurer que sa stratégie de cyberrésilience couvre les aspects suivants :
    a. la vision et le mandat de l'IMF en matière de cyberrésilience;
    b. les buts, objectifs et résultats stratégiques visés par l'IMF sur le plan de la cyberrésilience;
    c. l'importance de la cyberrésilience pour l'IMF et ses principales parties prenantes internes et externes;

d. la tolérance aux cyberrisques de l'IMF pour qu'elle demeure en phase avec sa tolérance globale aux risques, ses objectifs opérationnels et sa stratégie d'entreprise;
e. les cyberrisques que les participants à l'IMF, d'autres IMF et des tiers font courir à l'IMF et que celle-ci leur fait courir;
f. des objectifs clairs et crédibles en matière de cybermaturité, revus périodiquement;
g. la gouvernance nécessaire à l'élaboration, au déploiement, à la gestion et à l'amélioration de la cyberrésilience;
h. la mise en œuvre, la gestion et le financement de la cyberrésilience, y compris le processus d'établissement du budget et les capacités organisationnelles;
i. l'intégration de la cyberrésilience dans toutes les activités de l'IMF, notamment les ressources humaines, les processus, les technologies et les nouveaux projets opérationnels.

3. Le conseil d'administration de l'IMF[4] devrait approuver la stratégie de cyberrésilience et veiller à ce qu'elle soit périodiquement revue et mise à jour en fonction de l'ensemble des menaces entourant l'IMF.

1.3 Cadre de cyberrésilience

Le cadre de cyberrésilience désigne les politiques, normes techniques, procédures et contrôles instaurés par une IMF pour identifier les sources plausibles de cyberrisques auxquels elle est confrontée, les détecter, s'en protéger, intervenir et se rétablir par la suite.

4. L'IMF devrait disposer d'un cadre de cyberrésilience documenté qui expose clairement comment elle détermine ses objectifs de cyberrésilience[5] et sa tolérance au risque, ainsi que la manière dont elle identifie, atténue et gère efficacement ses cyberrisques pour contribuer à la réalisation de ses objectifs.

5. Le cadre de cyberrésilience de l'IMF devrait :

a. être approuvé par le conseil d'administration de l'IMF pour qu'il concorde bien avec la stratégie de cyberrésilience;

b. être conçu sur la base des principales normes, lignes directrices ou recommandations internationales, nationales et sectorielles (p. ex., la série ISO/IEC 27000, le cadre de cybersécurité et les publications spéciales du NIST) afin d'intégrer les solutions de cyberrésilience les plus efficaces;

---

[4] Si l'IMF appartient à un groupe d'entreprises, la stratégie de cyberrésilience peut être élaborée pour l'ensemble des entreprises. Dans ce cas, le conseil d'administration de l'IMF devrait veiller à ce que celle-ci soit consultée lors de l'élaboration de la stratégie de cyberrésilience globale pour que la stratégie reflète les objectifs de l'IMF dans ce domaine.

[5] Ces objectifs devraient viser à maintenir et à favoriser la capacité de l'IMF à anticiper les cyberattaques, à y résister, à les contenir et à se rétablir par la suite, afin de réduire la probabilité qu'une cyberattaque réussisse à perturber ses opérations ou les répercussions que celle-ci aurait sur l'ensemble du système financier (CPIM et OICV, *Guidance on cyber resilience for financial market infrastructures*, section 2.2.1).

c. définir clairement les rôles et les responsabilités, notamment la reddition de comptes en matière de prise de décision au sein de l'organisation, en ce qui a trait à l'identification, à l'atténuation et à la gestion des cyberrisques dans des conditions normales d'activité et dans des situations de crise ou d'urgence provoquées par un cyberincident;

d. intégrer systématiquement les exigences (c.-à-d. les politiques, les normes techniques et les contrôles) liées aux volets suivants : gouvernance, identification, protection, détection, intervention et rétablissement, tests, connaissance de la situation, apprentissage et évolution;

e. être cohérent avec le cadre de gestion des risques opérationnels et l'architecture d'entreprise de l'IMF;

f. inclure des exigences sur la promptitude et le moment des communications, et des mécanismes de coordination afin que l'IMF puisse collaborer avec les parties prenantes concernées pour intervenir et se rétablir de manière efficace en cas de cyberattaque;

g. tenir compte des cyberrisques que les participants à l'IMF, d'autres IMF, les fournisseurs et leurs produits, et les prestataires de services – entités dénommées collectivement « écosystème » de l'IMF – font courir à l'IMF et que celle-ci leur fait courir;

h. être revu et actualisé régulièrement.

6. L'IMF devrait évaluer et mesurer régulièrement l'adéquation, l'efficacité et le respect de son cadre de cyberrésilience (notamment en ce qui a trait aux contrôles de sécurité) au moyen de programmes et d'audits de conformité indépendants. Pour ce faire, l'IMF est invitée à utiliser des indicateurs et des modèles de maturité pertinents ainsi que les résultats de ses programmes de tests. Elle devrait périodiquement demander un audit externe.

7. L'IMF devrait revoir et actualiser périodiquement son cadre de cyberrésilience (notamment l'ensemble des politiques, normes techniques, procédures et contrôles), surtout si des modifications ont été apportées à sa stratégie ou à ses objectifs de cyberrésilience. Elle devrait élaborer une méthodologie pour mener à bien cet examen en prenant en compte, entre autres, les facteurs suivants :

   a. les cybermenaces actuelles et leur évolution (p. ex., les menaces liées à la chaîne d'approvisionnement, à l'utilisation des services infonuagiques, aux médias sociaux, aux applications mobiles et à l'Internet des objets);

   b. les renseignements sur les cybermenaces, notamment les auteurs de menace et les nouvelles tactiques, techniques et procédures susceptibles de toucher spécifiquement l'IMF;

c. les résultats des évaluations des risques liés aux fonctions essentielles, aux rôles clés, aux processus, aux actifs informationnels, aux fournisseurs de services externes et aux interconnexions de l'IMF;

d. les cyberincidents qui ont touché l'IMF directement ou l'une des entités de son écosystème;

e. les leçons tirées de la certification, des audits ou d'autres formes d'assurance ainsi que des tests appliqués au cadre de cyberrésilience;

f. les résultats de l'IMF au regard des indicateurs pertinents;

g. les évolutions commerciales et les objectifs stratégiques futurs.

8. L'IMF devrait suivre en permanence l'évolution de ses capacités de cyberrésilience, en comparant son état actuel à un état futur défini (c.-à-d. un niveau de maturité cible). Elle peut s'appuyer sur un modèle de maturité pour documenter les progrès réalisés.

9. L'IMF devrait avoir un plan pour atteindre son niveau de maturité cible, soit une véritable feuille de route décrivant l'allocation des ressources et la marche à suivre pour parvenir à ce niveau cible.

1.4 Rôles du conseil d'administration et de la direction générale

1.4.1 Responsabilités du conseil d'administration et de la direction générale

10. Le conseil d'administration de l'IMF est ultimement responsable de l'efficacité de la gestion des cyberrisques[6,7]. Il devrait clairement définir les rôles et responsabilités en matière de gestion des cyberrisques, établir la tolérance aux cyberrisques et la stratégie de cyberrésilience de l'IMF, et approuver le cadre de cyberrésilience.

11. Le conseil d'administration et la direction générale devraient mettre en place un processus garantissant une identification et une gestion en continu des cyberrisques. Toutes les unités organisationnelles devraient participer à la décision d'accepter, d'atténuer ou d'éviter ces risques, conformément aux objectifs de fiabilité opérationnelle de l'IMF.

12. L'IMF devrait concevoir des indicateurs de risque pertinents dégageant les tendances et les constantes, qui seront utilisés par la direction générale et le conseil d'administration

---

[6] Conformément à la section 3.2.8 des PIMF, le conseil d'administration de l'IMF doit surveiller la supervision exercée par la direction générale lors de la mise en œuvre du cadre de cyberrésilience et veiller à ce que l'IMF réponde aux attentes énoncées dans le document d'orientation et le présent document. Cette attente s'applique également lorsque l'IMF fait partie d'un groupe d'entreprises dans lequel la stratégie et le cadre de cyberrésilience sont établis pour l'ensemble des entreprises.

[7] L'IMF peut envisager de s'appuyer sur l'un de ses comités, comme son comité de gestion des risques, pour aider le conseil d'administration à s'acquitter de ses responsabilités relativement à la gestion des cyberrisques et de la résilience.

pour prendre des décisions fondées sur le risque et faire état des progrès accomplis dans la mise en œuvre de son cadre de cyberrésilience.

13. Le conseil d'administration et la direction générale devraient veiller à ce que les cyberrisques auxquels est exposée l'IMF[8] et la gestion de ces risques soient régulièrement examinés lors des réunions du conseil.

14. La direction générale devrait superviser de près la mise en œuvre du cadre de cyberrésilience par l'IMF, ainsi que les politiques, les normes techniques, les procédures et les contrôles connexes. Cette supervision consiste notamment à :

    a. établir l'ordre de priorité des livrables liés à la cyberrésilience et de l'allocation des ressources en fonction des résultats des évaluations de la cyberrésilience, des principaux indicateurs de rendement et de risque, de l'ensemble des objectifs opérationnels et des progrès réalisés au regard de la maturité cible;

    b. effectuer régulièrement des autoévaluations de la cyberrésilience afin d'évaluer le niveau de cybermaturité de l'IMF;

    c. passer en revue l'autoévaluation ainsi que les leçons tirées des résultats des tests, et prendre les décisions qui s'imposent pour améliorer l'efficacité des activités liées à la cybersécurité;

    d. veiller à ce que le personnel chargé de mettre en œuvre le cadre de cyberrésilience de l'IMF ait les compétences, les connaissances, l'expérience et les ressources adéquates, qu'il soit suffisamment informé et qu'il dispose des pouvoirs requis pour prendre des décisions rapidement, en temps opportun;

    e. réexaminer en permanence les aptitudes, les compétences et les besoins de formation de sorte que l'IMF ait l'ensemble des compétences requises à mesure que les technologies et les risques évoluent.

15. La direction générale devrait veiller à ce que tous les employés comprennent leur rôle dans l'atténuation des cyberrisques et aient accès à un niveau adéquat de formation.

16. Le conseil d'administration et la direction générale devraient élaborer, au besoin, des plans de relève pour le personnel à haut risque (p. ex., cadres supérieurs, administrateurs de systèmes, développeurs de logiciels et opérateurs de systèmes essentiels). De plus, ils devraient définir des critères de recrutement (compétences, connaissances, expérience, etc.) pour les postes clés dans le domaine de la cybersécurité, conformément aux plans de relève établis.

[8] Les rapports au conseil d'administration peuvent comprendre une évaluation de la cyberrésilience comparativement au dernier rapport, des renseignements sur les projets de cyberrésilience, les cyberincidents et les résultats des tests d'intrusion et de ceux menés par l'équipe rouge.

17. La direction générale devrait contribuer et participer aux exercices sectoriels visant à tester et à renforcer la cyberrésilience de l'écosystème de l'IMF.

1.4.2 Culture

18. Le conseil d'administration et la direction générale devraient entretenir un niveau élevé de sensibilisation et d'adhésion à la cyberrésilience, et prêcher par l'exemple en favorisant une culture qui reconnaît que les employés de tous les niveaux ont une grande part de responsabilité dans la cyberrésilience de l'IMF.

19. La direction générale de l'IMF devrait veiller à continuellement propager sa culture de sensibilisation aux cyberrisques dans toute l'organisation. Les programmes de formation devraient être actualisés régulièrement pour tenir compte de l'évolution de l'ensemble des menaces dans l'écosystème de l'IMF.

20. L'IMF devrait établir des politiques énonçant les conséquences pour les employés et les contractuels qui ne respectent pas les politiques de cybersécurité. Ces politiques devraient être claires et adaptées au risque et au contexte d'une situation donnée.

1.4.3 Compétences et responsabilités

21. Pour s'acquitter de leurs responsabilités liées à la stratégie et au cadre de cyberrésilience, le conseil d'administration et la direction générale de l'IMF devraient être composés de membres dotés du juste équilibre de compétences, de connaissances et d'expérience pour comprendre et gérer les cyberrisques auxquels l'IMF est confrontée. Le conseil d'administration devrait être suffisamment informé et pouvoir remettre en question de façon crédible les recommandations et les décisions des membres désignés de la direction générale. Pour atteindre cet objectif, l'IMF devrait :

    a. nommer une personne ayant des compétences en cybersécurité au sein du conseil d'administration;

    b. veiller à ce que les membres du conseil d'administration et la direction générale comprennent leurs rôles et responsabilités en matière de cyberrésilience (notamment leur rôle dans la gestion des cyberrisques) et reçoivent une formation, au besoin.

22. Le conseil d'administration et la direction générale devraient nommer un cadre supérieur, par exemple un chef de la sécurité de l'information, qui sera responsable de l'application du cadre de cyberrésilience au sein de l'organisation et en rendra compte.

23. L'IMF devrait veiller à ce que ce cadre supérieur :

    a. dispose de l'autorité adéquate et d'un accès à des ressources suffisantes (humaines et technologiques);

    b. ait accès au conseil d'administration;

    c. jouisse d'une indépendance d'action par rapport aux autres opérations TI;

d. possède les connaissances et l'expertise requises pour planifier et mettre en œuvre les initiatives de cyberrésilience de l'IMF de manière compétente.

2 Identification

2.1 Préambule

Puisque la défaillance opérationnelle d'une IMF peut porter atteinte à la stabilité financière, les IMF doivent absolument déterminer, par ordre de priorité, les opérations et les actifs informationnels connexes à protéger contre toute compromission. Une IMF se doit de connaître sa situation interne et ses dépendances externes pour pouvoir intervenir avec efficacité en cas d'éventuelles cybermenaces. Pour ce faire, elle doit connaître ses actifs informationnels et comprendre ses processus, ses procédures, ses systèmes et tous ses liens d'interdépendance pour renforcer sa cyberrésilience globale.

Cette section décrit comment une IMF devrait identifier et catégoriser les processus opérationnels, les actifs informationnels et les liens d'interdépendance externes, et procéder à des évaluations des risques.

2.2 Identification et catégorisation

Il importe que l'IMF comprenne quels sont les fonctions opérationnelles et processus connexes essentiels à ses activités principales et qu'elle identifie les actifs informationnels qui soutiennent ces fonctions et processus. Des évaluations des risques devraient être menées pour définir les priorités sur le plan de la cyberrésilience.

2.2.1 Identification des fonctions et processus opérationnels

1. Une IMF devrait avoir un processus permettant d'identifier et de documenter ses fonctions opérationnelles, ses processus connexes et ses liens d'interdépendance (internes et externes), notamment les processus qui dépendent de fournisseurs de services externes. Elle devrait effectuer une analyse des répercussions sur les opérations afin de quantifier l'incidence des perturbations sur ses opérations essentielles. Les fonctions et processus opérationnels identifiés devraient être classés selon leur criticité et associés aux objectifs de fiabilité opérationnelle de l'IMF. L'IMF devrait se servir de cette information pour établir ses priorités en matière de mécanismes de protection, de détection, d'intervention et de rétablissement.

2.2.2 Identification des actifs informationnels et accès connexe

2. L'IMF devrait identifier les actifs informationnels [9] qui appuient ses processus opérationnels. Elle devrait :

[9] Selon le document d'orientation, les actifs informationnels sont des éléments de données, des appareils ou

a. établir une norme pour catégoriser l'information et les systèmes d'information selon le niveau de préoccupation de l'IMF par rapport à la confidentialité, à l'intégrité et à la disponibilité;

b. identifier ses actifs informationnels et les configurations des systèmes, et tenir à jour un registre central qui lui permet de connaître en tout temps les actifs informationnels qui appuient ses fonctions et ses processus opérationnels;

c. élaborer et tenir à jour un diagramme du réseau actuel illustrant :

   i. les ressources du réseau (y compris les adresses IP et les sous-réseaux);

   ii. les composantes interreliées;

   iii. les liens vers des services internes et externes (y compris les liens avec d'autres parties prenantes, des services Internet, des services infonuagiques et tout autre système de tiers).

3. L'IMF devrait adopter et appliquer un processus d'évaluation des cyberrisques et tenir un registre servant à consigner et à surveiller les risques. Ce processus devrait indiquer les conditions dans lesquelles les évaluations doivent être effectuées ou mises à jour (p. ex., développement et modernisation de systèmes, nouvelles menaces, et vulnérabilités repérées dans les systèmes ou l'infrastructure de l'IMF). Le registre devrait identifier et classer les risques selon leur criticité.

4. L'IMF devrait effectuer des évaluations des risques associés à ses actifs informationnels, et en consigner les résultats, conformément à son processus d'évaluation des cyberrisques.

5. Après avoir terminé ou mis à jour une évaluation des risques, l'IMF devrait consulter et actualiser son registre des risques en fonction des résultats. Ceux-ci devraient guider le choix des contrôles de sécurité et leur mise en œuvre, et permettre de les classer par ordre de priorité d'après les risques auxquels l'IMF est exposée.

6. L'IMF devrait tenir un dépôt central des comptes individuels et des comptes associés aux systèmes, ainsi que des droits d'accès. Ce dépôt devrait :

   a. indiquer les droits d'accès aux actifs informationnels et aux systèmes connexes;

   b. contenir des renseignements pertinents pour aider l'IMF à identifier les activités anormales[10];

   c. être protégé contre les accès et les modifications non autorisés.

---

d'autres composantes de l'environnement qui appuient les activités liées à l'information. Ils comprennent les données, le matériel et les logiciels, et ne se limitent pas uniquement à ceux qui appartiennent à l'IMF. Ils englobent aussi ceux qui sont loués et ceux qui sont utilisés par des fournisseurs de services.

[10] Les activités anormales sont des activités qui sortent du cadre des comportements attendus.

2.2.3 Examen et mise à jour périodiques

7. L'IMF devrait intégrer ses efforts d'identification aux autres processus pertinents – comme les processus d'acquisition et de gestion des changements – pour faciliter l'examen périodique de la liste de ses fonctions et processus opérationnels essentiels, des identifiants individuels et des systèmes, et de ses actifs informationnels de sorte que ces renseignements demeurent à jour, exacts et complets.

2.3 Interconnexions

L'identification des processus opérationnels essentiels de l'IMF et des actifs informationnels qui les appuient devrait aussi englober les entités de l'écosystème de cette dernière. Les systèmes et processus de l'IMF ont des interconnexions, directes ou indirectes, avec les systèmes et processus de ces entités. La cyberrésilience de ces entités pourrait donc avoir une incidence notable sur les cyberrisques auxquels est exposée l'IMF, surtout parce que l'ampleur des risques qu'elles représentent n'est pas nécessairement proportionnelle à la criticité de leur relation professionnelle avec l'IMF.

8. L'IMF devrait identifier les cyberrisques que les entités de son écosystème lui font courir, ou qu'elle fait courir à ces entités, et prendre les dispositions nécessaires avec celles-ci au besoin. Par exemple, elles peuvent déterminer ensemble les vulnérabilités et les menaces qu'elles ont en commun et prendre les mesures appropriées pour atténuer ces risques, en vue d'améliorer la résilience globale de l'écosystème.

9. Pour identifier et évaluer les risques que comportent pour elle les interconnexions entre les participants, l'IMF devrait tenir compte d'un grand éventail de vecteurs de menace et de risque qui pourraient entraîner la compromission de ses principales fonctions opérationnelles. Elle devrait entre autres déterminer la probabilité qu'une menace survienne et, le cas échéant, en évaluer l'incidence, et analyser les risques qu'elle court. Elle devrait aussi évaluer les risques pour son écosystème qui pourraient découler des interconnexions entre les participants.

10. Pour identifier et évaluer les risques que comportent les interconnexions avec des fournisseurs externes, l'IMF doit bien connaître les services et les processus de ces derniers, notamment les détails relatifs aux services qu'ils lui procurent et à leur façon de procéder. Elle pourrait devoir compter sur diverses sources pour recueillir ces renseignements (p. ex., information accessible au public, autoévaluations et évaluations indépendantes) qui lui permettront de comprendre, d'identifier et d'évaluer les risques.

3 Protection

3.1 Préambule

La cyberrésilience repose sur des contrôles de sécurité, des systèmes et des processus efficaces qui protègent la confidentialité, l'intégrité et la disponibilité des actifs et services de l'IMF. Ces mesures

devraient être proportionnelles à l'ensemble des menaces qui pèsent sur l'IMF et au rôle de celle-ci dans le système financier, et être conformes à la tolérance au risque de l'IMF.

La présente section indique comment l'IMF devrait s'y prendre pour mettre en œuvre des mesures de protection appropriées et efficaces qui concordent avec les pratiques exemplaires de cyberrésilience et de cybersécurité, dans le but de prévenir ou de limiter l'incidence d'un cyberévénement potentiel.

3.2 Protection des processus et des actifs

Pour protéger ses processus et ses actifs, l'IMF doit adopter une approche de résilience dès la conception, établir de solides contrôles des TIC et avoir recours à une défense par couches.

3.2.1 Résilience dès la conception

L'IMF devrait tenir compte de la cyberrésilience dès les premières étapes de la conception et du développement des systèmes, et pendant toute leur durée de vie. Elle pourra ainsi minimiser les vulnérabilités des logiciels et du matériel et veiller à ce que les contrôles de sécurité appropriés soient intégrés aux systèmes et aux processus dès leur mise en œuvre. Si les systèmes ou l'une de leurs composantes ont été acquis auprès d'un fournisseur externe, ou s'ils sont exploités par un fournisseur externe, l'IMF devrait s'assurer que les contrôles de sécurité appropriés ont été appliqués.

1. L'IMF devrait :

    a. adopter une méthode de développement de systèmes fondée sur une approche de résilience dès la conception pour l'élaboration, l'établissement, l'acquisition ou la modification de ses systèmes, processus et produits. À chaque étape du développement, elle devrait gérer ses cyberrisques et intégrer la résilience selon les résultats de l'analyse des risques;

    b. établir et communiquer des principes relatifs à l'ingénierie des systèmes sécurisés, et veiller à ce que des processus et procédures soient établis, consignés, actualisés et appliqués aux efforts de mise en œuvre des systèmes d'information;

    c. lorsqu'elle conçoit, développe ou fait l'acquisition des systèmes et des processus, définir les exigences en matière de sécurité et les exigences relatives aux systèmes et processus pour identifier les contrôles nécessaires à la protection de ses systèmes, processus et données;

    d. séparer[11] les environnements de test, de développement et de production afin de réduire les risques opérationnels. Chaque environnement devrait être dûment sécurisé, conformément aux normes de sécurité de l'IMF;

[11] Physiquement ou logiquement

e. dans la mesure du possible, veiller à ce que l'environnement de test soit très semblable à l'environnement de production, surtout en ce qui a trait aux logiciels, aux configurations du réseau et au matériel à l'appui des systèmes essentiels;

f. examiner et tester rigoureusement les applications, les systèmes et les réseaux essentiels pour vérifier leur conformité à ses normes de sécurité et veiller à ce qu'il n'y ait pas d'incidences néfastes sur les opérations ou la sécurité organisationnelles. Par exemple, ces tests peuvent porter sur les éléments suivants : sécurité fonctionnelle des systèmes et logiciels essentiels (pour s'assurer qu'ils fonctionnent bien); frontières; robustesse et tolérance aux pannes; performance et chargement; flux de données; cas d'utilisation. Les tests de sécurité devraient être intégrés aux tests d'acceptation des nouveaux systèmes, des mises à jour et des nouvelles versions;

g. limiter le plus possible la surface d'attaque, par exemple en désactivant les fonctions ou les services inutiles ou inutilisés, et en bloquant les comportements des logiciels qui sont habituellement exploités par les pirates ou les maliciels;

h. veiller à ce que les modifications apportées aux systèmes pendant leur cycle de vie fassent l'objet de processus et de procédures de contrôle officiels.

3.2.2 Contrôles

2. L'IMF devrait établir des politiques et des procédures soutenant la mise en place d'un ensemble complet et approprié de contrôles de protection lui permettant d'atteindre les objectifs de cyberrésilience nécessaires au bon déroulement de ses opérations, à la protection de ses actifs et au respect de ses exigences opérationnelles. Quand elle choisit ses contrôles relatifs aux TIC, l'IMF devrait suivre les pratiques exemplaires de cyberrésilience, comme les normes NIST et ISO. Le présent document ne vise pas à remplacer les normes existantes de l'IMF.

3. L'IMF devrait mettre en place ces contrôles après avoir déterminé ses fonctions essentielles, rôles clés, processus, actifs informationnels, fournisseurs externes et interconnexions, conformément à l'évaluation des risques effectuée à la phase d'identification.

Même si le présent document n'est pas axé sur les contrôles relatifs aux TIC, les sous-sections suivantes indiquent un certain nombre de contrôles importants dont l'IMF devrait tenir compte. L'ensemble de contrôles qu'elle choisit de mettre en place repose sur des facteurs qui lui sont propres.

3.2.3 Exemples de contrôles solides relatifs aux TIC

3.2.3.1 Protection des renseignements : contrôles de protection des données et des renseignements

4. Pour assurer la confidentialité, l'intégrité et la disponibilité de ses données et renseignements stockés et utilisés, l'IMF devrait mettre en place de solides contrôles de protection, notamment :

    a. des mécanismes de protection contre les maliciels (balayage, blocage ou mise en quarantaine aux points d'entrée et de sortie du réseau, aux passerelles de messagerie électronique, aux serveurs et aux systèmes d'extrémité). L'IMF devrait mettre à jour ses mécanismes de protection contre les codes malveillants chaque fois qu'une nouvelle version est offerte. Elle devrait faire les mises à jour en respectant ses politiques et procédures de gestion de la configuration et des changements. La protection devrait comprendre la détection et l'atténuation des tentatives d'hameçonnage. Le personnel de l'IMF devrait savoir comment utiliser efficacement les antimaliciels et connaître les menaces d'hameçonnage;

    b. des outils de vérification de l'intégrité[12] pour détecter les changements non autorisés apportés au fichier d'entrée essentiel provenant de sources internes et externes (p. ex., des entités participantes);

    c. des mécanismes de chiffrement des données conformes aux processus de l'IMF pour l'évaluation de la criticité, de la sensibilité et des risques;

    d. des mécanismes de chiffrement conformes aux normes et aux processus reconnus et couvrant des aspects tels que les algorithmes, les longueurs de clé, la création de clés et la gestion de clés;

    e. la protection physique du matériel servant à la création, au stockage et à l'archivage de clés;

    f. le balayage régulier de l'environnement de production pour identifier des vulnérabilités potentielles et des possibilités de mettre à jour les anciennes technologies. Des contrôles et d'autres couches de défense devraient être mis en place et testés pour s'assurer qu'ils protègent les systèmes vulnérables ou non pris en charge;

    g. des vérifications de la validité de toutes les données entrées dans les applications, particulièrement les applications Web. Ces vérifications devraient porter sur la validité de la syntaxe; les types, les longueurs et les plages de données; les valeurs acceptables;

    h. la prévention de la divulgation, de la modification, de la suppression ou de la destruction non autorisée des données stockées sur un support;

[12] Par exemple, des empreintes ou des signatures numériques

i. la destruction sécurisée des supports quand ils ne sont plus utilisés, en suivant des procédures officielles;

j. lors du transport d'un support, la protection des renseignements stockés contre toute consultation non autorisée, utilisation malveillante ou corruption;

k. l'assurance que toutes les données sensibles et tous les logiciels sous licence ont été effacés de manière sécurisée avant la destruction ou la réutilisation des appareils ou des supports;

l. l'établissement et l'application de politiques pour le rangement du bureau (documents imprimés) et le verrouillage de l'écran (installations de traitement de l'information). Les supports amovibles devraient être entreposés conformément à la politique organisationnelle.

3.2.3.2 Protection des renseignements : contrôles de sécurité des communications et du réseau

5. L'IMF devrait mettre en place de solides contrôles de sécurité des communications et du réseau, notamment :

a. des protocoles réseau sécurisés et des mécanismes de chiffrement [13], avec évaluation des risques à l'appui, pour protéger la confidentialité et l'intégrité des renseignements échangés sur son réseau et au-delà de celui-ci (p. ex., connexions à distance et interconnexions avec des tiers);

b. un vaste éventail de technologies et d'outils pour détecter et bloquer les tentatives d'attaque ou d'intrusion (ou les attaques ou intrusions réelles), y compris celles qui proviennent de connexions de tiers autorisés (p. ex., les réseaux des participants). L'IMF peut utiliser des systèmes de détection ou de prévention des intrusions, des solutions de sécurité des terminaux [14] ou toute autre solution pertinente [15], particulièrement sur des appareils et dans des environnements servant à accéder à distance au réseau de l'IMF;

c. des contrôles qui gèrent les appareils non contrôlés ou qui les empêchent de se connecter au réseau interne logique de l'IMF (y compris à distance), ce qui permet de limiter l'accès au réseau aux appareils autorisés et de protéger les sessions de l'écoute électronique, du déni de service, de la mystification, etc. L'infrastructure réseau de l'IMF devrait être balayée régulièrement pour y détecter les appareils et les points d'accès non autorisés;

d. la protection des systèmes d'information essentiels contre les attaques par déni de service, y compris les attaques majeures par déni de service distribué, pour

[13] Par exemple, le protocole de sécurité de la couche de transport, le protocole de sécurité IP ou d'autres réseaux virtuels privés

[14] Par exemple, un logiciel antivirus, un coupe-feu, ou un système de détection ou de prévention des intrusions au niveau de l'hôte

[15] Par exemple, une passerelle d'accès ou un serveur intermédiaire

empêcher la perturbation de ses services essentiels. L'IMF peut avoir recours à diverses technologies, comme des dispositifs de protection périphérique, des services infonuagiques offerts par des tiers pour la protection contre les attaques par déni de service distribué, et une capacité et une bande passante accrues ou d'urgence pour réduire les risques d'attaque par déni de service;

e. l'assurance que la protection s'applique à toute la surface d'attaque de l'IMF, et que l'infrastructure connexe ou élargie[16] qui peut servir de vecteur d'attaque pour accéder à l'infrastructure essentielle est aussi officiellement autorisée, surveillée et contrôlée.

3.2.3.3 Gestion de la configuration et des changements

6. L'IMF devrait avoir des politiques, des processus et des procédures pour la gestion de la configuration et des changements. Le processus de gestion de la configuration et des changements devrait reposer sur des normes et des pratiques exemplaires bien établies et reconnues dans le domaine (p. ex., ITIL). L'IMF pourrait mettre en place les mesures suivantes :

   a. former un comité consultatif sur les changements composé des principales parties prenantes (p. ex., les responsables de la gestion des opérations et des TI) pour approuver les changements et les classer par ordre de priorité après avoir tenu compte de leur incidence sur la sécurité et la stabilité de l'environnement de production;

   b. surveiller les changements à apporter à l'organisation, aux processus opérationnels, aux installations de traitement de l'information et aux systèmes qui ont une incidence sur la cybersécurité afin de s'assurer qu'ils font l'objet de contrôles;

   c. tester, valider et consigner les changements à apporter aux systèmes d'information avant de les mettre en œuvre dans l'environnement de production (p. ex., faire des tests d'intégration, de régression et d'acceptation par les utilisateurs). Les changements à apporter aux systèmes d'information comprennent entre autres la modification des composantes matérielles, logicielles ou micrologicielles et des paramètres de système et de sécurité;

   d. mettre en œuvre des mécanismes automatisés pour empêcher l'installation sur les systèmes d'information des changements et des correctifs qui n'ont pas été préapprouvés;

[16] Par exemple, l'utilisation de services de voix sur IP, de vidéoconférence et de collaboration ainsi que d'appareils, de téléphones intelligents et d'applications

e. établir des paramètres de système et de sécurité de base[17] pour les systèmes d'information et les composantes (y compris les appareils utilisés pour accéder à son réseau à distance) qui :

   i. sont consignés, officiellement examinés et régulièrement mis à jour pour les adapter à l'évolution de l'ensemble des menaces;

   ii. emploient des mécanismes automatisés (p. ex., des outils de gestion des stocks de matériel et de logiciels, de la configuration et du réseau) pour veiller à ce que la base de référence soit à jour, complète, exacte et accessible;

   iii. permettent la consignation des incidents de sécurité;

   iv. sont configurés de manière à exploiter les capacités essentielles seulement et à désactiver ou désinstaller les fonctions et les services inutiles;

f. maintenir un contrôle sur les types de logiciels installés en déterminant les actions permises et interdites concernant l'installation des logiciels. Pour les systèmes essentiels, l'IMF devrait avoir recours aux capacités d'établissement d'une liste blanche des logiciels configurée selon un modèle consistant à tout interdire ou à permettre à titre exceptionnel;

g. mettre en place les procédures nécessaires pour que les changements soient mis en œuvre adéquatement et efficacement[18];

h. analyser en amont les incidences que pourrait avoir la mise en œuvre des changements proposés aux systèmes sur la sécurité;

i. veiller à ce que seules les personnes autorisées et qualifiées puissent apporter des changements aux systèmes d'information, y compris des mises à jour et des ajustements;

j. veiller à ce que des processus pour planifier la mise en œuvre des changements soient établis, et communiquer au préalable avec les personnes visées et les consulter au besoin;

k. établir des processus pour identifier, évaluer et approuver les changements véritablement urgents, c'est-à-dire qui exigent une intervention immédiate. Des examens devraient être effectués après la mise en œuvre pour confirmer que les procédures d'urgence ont bien été suivies et pour définir l'incidence des changements;

l. avoir les processus et procédures nécessaires pour retourner en arrière rapidement quand les changements ou les correctifs échouent. Tout changement apporté à

---

[17] Selon NIST 800-53 R.4, la configuration de base est un « ensemble documenté de spécifications pour un système d'information, ou élément de configuration dans un système, qui a été officiellement revu et approuvé à un moment donné, et qui ne peut être modifié qu'en suivant des procédures de contrôle des modifications ».

[18] Par exemple, des examens de code et des tests unitaires

l'environnement de production doit être accompagné d'un plan de rechange, s'il y a lieu.

3.2.3.4 Paramètres de sécurité correspondant au niveau de protection

7. L'IMF devrait configurer les systèmes et les appareils de TIC avec des paramètres de sécurité qui correspondent au niveau de protection attendu. Voici quelques exemples de contrôles qui permettraient d'atteindre cet objectif :

   a. établissement et consignation de normes relatives à la configuration des paramètres de sécurité de base pour faciliter l'application uniforme de ces derniers aux systèmes d'exploitation, aux bases de données, aux dispositifs réseau et aux appareils mobiles de l'entreprise dans l'environnement de TIC. Ces normes devraient prescrire les contrôles, les paramètres, les fonctions et les spécifications techniques de sécurité TI requis pour atteindre les objectifs de cybersécurité visant à protéger les actifs informationnels et les solutions technologiques de l'IMF;

   b. intégration des normes lors de la planification, de la conception, de l'élaboration et de la maintenance de systèmes ou de solutions;

   c. contrôles fréquents de l'application des normes pour rectifier rapidement les cas de non-conformité;

   d. mise en place d'un processus officiel fondé sur les risques pour le traitement et l'approbation des exceptions associées aux cas où des solutions ne peuvent être rendues conformes aux normes;

   e. examen périodique des normes de configuration de base et mises à jour au besoin.

3.2.4 Protection par couches facilitant l'intervention et le rétablissement

8. Les contrôles de protection de l'IMF devraient permettre la surveillance et la détection des activités anormales. L'IMF devrait :

   a. définir et consigner le profil de base des activités de ses systèmes, proportionnellement aux risques, pour faciliter la détection des écarts par rapport à celui-ci (p. ex., les activités anormales et les événements). Ce profil devrait tenir compte des activités techniques liées aux systèmes (comme les schémas de trafic réseau normal, l'utilisation des comptes et les règles d'accès) et des activités opérationnelles des systèmes (comme la fréquence, la taille, le moment et le volume normaux ou attendus des transactions des participants);

   b. développer les capacités appropriées (personnes, processus, technologies, etc.) pour surveiller et détecter les activités et événements anormaux, en définissant des critères, des paramètres et des déclencheurs adéquats pour générer des alertes. Par exemple, l'IMF peut intégrer à la logique applicative des systèmes ou des

applications une fonction permettant de détecter les transactions [19] ou les comportements[20] inhabituels, ou mettre en place des processus d'analyse avancée des données qui permettront de cerner les tendances et l'aviseront si des événements inhabituels se produisent;

c. utiliser des analyses de journaux corrélées, des alertes et des flux de trafic pour prendre des mesures adéquates en amont en vue d'améliorer ses capacités de cyberrésilience.

9. Afin de contenir les activités anormales, l'IMF devrait développer les capacités appropriées, si possible, pour bloquer les activités suspectes au niveau de l'application ou du réseau.

10. Pour séparer les systèmes et les données ayant divers degrés de criticité, l'IMF devrait :

a. établir une frontière sécurisée qui protège son infrastructure réseau [21]. Cette frontière devrait identifier les zones fiables ou non fiables, selon le profil de cyberrisque et la criticité des actifs informationnels qui s'y trouvent. Des droits d'accès appropriés devraient être établis à l'intérieur de chaque zone de sécurité et entre les zones, selon le principe du droit d'accès minimal. Un modèle de trafic consistant à tout interdire ou à permettre à titre exceptionnel devrait être utilisé entre les zones, si possible;

b. gérer et contrôler les réseaux pour protéger l'information des systèmes et des applications;

c. utiliser un réseau logique distinct et dédié pour l'administration des systèmes d'information[22];

d. concevoir son infrastructure de connexions réseau de manière à pouvoir instantanément segmenter ou couper ces connexions pour prévenir la contagion ou le mouvement latéral découlant des cyberattaques. L'IMF devrait également s'assurer que les procédures appropriées sont en place afin d'isoler ou de bloquer (promptement et en temps opportun) ses connexions à des tiers en cas de cyberattaque ou de risque de contagion;

e. mettre en œuvre des mécanismes automatisés qui peuvent isoler les actifs informationnels touchés en cas d'événement défavorable.

---

[19] Par exemple, des transactions qui sont anormalement grosses ou petites, fréquentes ou peu fréquentes, ou dans le mauvais ordre

[20] Par exemple, des activités effectuées par des personnes inhabituelles, à des moments inhabituels ou à partir d'endroits inhabituels

[21] Par exemple, en utilisant des outils tels qu'un routeur, un coupe-feu, un système de détection ou de prévention des intrusions, un réseau privé virtuel, une zone démilitarisée ou des serveurs mandataires

[22] Par exemple, un segment de réseau local virtuel et un sous-réseau IP

3.3 Interconnexions

La gestion de la sécurité des tiers permet d'assurer la protection des actifs de l'IMF qui sont accessibles aux participants, aux IMF liées, aux fournisseurs de produits et services, ou aux autres entités de l'écosystème de l'IMF, tout en maintenant le niveau de sécurité de l'information et de prestation de services convenu dans les ententes afin de réduire au minimum les perturbations pour l'IMF.

3.3.1 Risques liés aux interconnexions

11. Étant donné son importance systémique et sa position unique au sein du système financier, l'IMF devrait mettre en place des mesures de protection visant à atténuer les risques découlant des entités de son écosystème. Les contrôles appropriés pour chaque entité dépendent des résultats de l'évaluation des risques effectuée à la phase d'identification, y compris les risques associés à l'entité connectée et au type de relation qu'entretient l'IMF avec cette dernière.

3.3.1.1 Conditions de participation

12. Au besoin, l'IMF devrait préciser des conditions de participation pour s'assurer d'atteindre ses objectifs de cyberrésilience. Par exemple, elle devrait imposer des conditions dans les domaines suivants[23] :

    a. restrictions relatives aux connexions;

    b. contrôle des accès et gestion des comptes privilégiés;

    c. identification et gestion de l'authentification;

    d. confidentialité et protection de l'intégrité par chiffrement;

    e. gestion des vulnérabilités et des correctifs;

    f. gestion de la détection et des interventions;

    g. sensibilisation et formation en matière de sécurité.

13. L'IMF devrait obtenir l'assurance de la part de ses participants que ceux-ci répondent à ses exigences en matière de cyberrésilience. Pour ce faire, elle peut leur demander d'effectuer régulièrement des autoévaluations ou de fournir des attestations externes de leur résilience.

3.3.1.2 Cyberrésilience des tiers

14. L'IMF devrait obtenir l'assurance de la part de ses fournisseurs de produits et services, comme les fournisseurs de services de TIC (collectivement appelés « les tiers »), qu'ils répondent à ses exigences en matière de cyberrésilience. Lorsqu'elle négocie ou renouvelle ses contrats avec des tiers, l'IMF devrait veiller à ce que les clauses à l'appui de

[23] Les IMF qui fournissent des services de compensation et de règlement des paiements devraient inclure des exigences en vue de réduire le risque de fraude dans les paiements de gros lié à la sécurité des terminaux, conformément à la stratégie publiée en mai 2018 par le Comité sur les paiements et les infrastructures de marché.

ses objectifs de cyberrésilience fassent l'objet d'un consensus et soient mises par écrit. Les contrats devraient notamment couvrir les points suivants :

a. validation des capacités en matière de sécurité. L'IMF devrait demander à un tiers de fournir une évaluation ou une confirmation de ses capacités en matière de sécurité. Par exemple, elle peut demander une autoévaluation (basée sur l'annexe F des PIMF ou un questionnaire qu'elle a elle-même conçu, notamment) ou une évaluation effectuée par un tiers, comme une attestation, une accréditation ou un audit externe;

b. exigences relatives à la sécurité de l'information, pour atténuer les risques associés à l'accès des tiers aux actifs informationnels de l'IMF[24];

c. exigences de confidentialité et de non-divulgation;

d. risques liés à la sécurité de l'information et associés aux services et aux chaînes d'approvisionnement de produits de TIC;

e. avis relatifs aux changements apportés aux niveaux de service ou aux fonctions de sécurité.

15. L'IMF devrait réévaluer les risques au besoin, lorsqu'elle est informée de l'apport de changements aux niveaux de service ou aux fonctions de sécurité de tiers.

3.4 Menaces internes

Les menaces internes émanent de toute personne qui connaît l'infrastructure et l'information de l'organisation, ou qui y a accès, et qui l'utilise, de façon volontaire ou non, à des fins malveillantes. Elles peuvent exposer à des risques les employés, les clients, les actifs, la réputation et les intérêts de l'IMF[25].

3.4.1 Analyse de la cybersécurité

16. L'IMF devrait mettre en place des mesures pour détecter et analyser les comportements anormaux chez les personnes qui ont accès à ses systèmes. Elle devrait employer des techniques d'identification et de prévention des pertes de données pour se protéger contre le retrait de données confidentielles de son réseau.

3.4.2 Changements de la situation d'emploi

17. L'IMF devrait mener des enquêtes de sécurité sur les nouveaux employés et vérifier leurs antécédents pour éviter les menaces internes. Elle devrait aussi périodiquement effectuer des vérifications semblables pour l'ensemble des membres de son personnel, tout au long de leur emploi, selon leur accès aux systèmes essentiels. De plus, elle devrait établir des

[24] Les actifs informationnels comprennent les actifs qui sont la propriété directe de l'IMF et ceux sur lesquelles elle compte pour mener ses opérations essentielles, sans toutefois en être propriétaire.

[25] Source : Centre canadien pour la cybersécurité (2020), *Comment protéger votre organisation contre les menaces internes*, ITSAP.10.003

processus et des contrôles pour atténuer les risques liés à la cessation d'emploi ou aux changements de responsabilités des employés.

18. L'IMF devrait intégrer la cybersécurité à chaque étape de la durée de l'emploi, en précisant les mesures de sécurité à prendre à l'accueil des nouveaux employés, tout au long de leur emploi et à la cessation de celui-ci. Par exemple, elle devrait :

    a. effectuer des enquêtes de sécurité et des vérifications des antécédents pour tous les candidats (employés ou contractuels), selon leurs fonctions éventuelles et la criticité des actifs et de l'information auxquels ils pourraient avoir accès dans le cadre de leur travail. Les ententes conclues avec les employés et les contractuels devraient indiquer leurs responsabilités, et celles de leur organisation, à l'égard de la sécurité de l'information;

    b. veiller à ce que les employés et les contractuels actuels se conforment aux politiques, aux procédures et aux contrôles établis;

    c. quand un employé change de responsabilités, veiller à ce que tous les droits d'accès liés à son poste précédent et non nécessaires à ses nouvelles fonctions lui soient retirés en temps opportun. Les employés occupant un poste sensible (notamment ceux qui passent à un poste nécessitant un accès privilégié à des systèmes essentiels ou qui deviennent du personnel à risque élevé) devraient faire l'objet d'une vérification au préalable;

    d. établir des procédures pour retirer rapidement, en temps opportun, les droits d'accès aux actifs informationnels pour les employés qui quittent l'organisation. À la cessation de leur emploi, les membres du personnel devraient retourner tous les actifs appartenant à l'IMF, y compris les documents importants[26].

19. Tous les employés, contractuels et partenaires externes devraient porter bien en vue une pièce d'identité et informer immédiatement le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés ou une personne ne portant pas de pièce d'identité visible.

20. L'IMF devrait veiller à ce que l'accès aux zones sécurisées ou aux installations de traitement de l'information confidentielle, y compris pour le personnel de soutien externe, soit accordé au besoin seulement. Cet accès devrait être autorisé et surveillé.

3.4.3 Contrôle de l'accès

3.4.3.1 Accès logique

21. L'IMF devrait s'assurer de ce qui suit :

    a. L'identité de chaque utilisateur a été vérifiée avant l'autorisation et la création d'un compte. Si les utilisateurs font partie d'une entité participante externe, l'IMF veille

[26] Par exemple, l'équipement, les logiciels, le matériel d'authentification ainsi que les documents et la correspondance contenant des processus opérationnels, des procédures techniques et des coordonnées

à ce que cette entité effectue la vérification de l'identité, laquelle doit être définie comme une exigence dans le contrat du participant.

b. Tous les utilisateurs[27] ont été identifiés et authentifiés de façon distincte de sorte que les actions et les activités puissent être attribuées à chacun individuellement.

c. Les authentifiants[28] sont adaptés à l'usage auquel ils sont destinés, c'est-à-dire que leur niveau de sûreté est proportionnel à la criticité du système d'information, du processus d'application ou du rôle de l'utilisateur. L'authentification multifacteur est utilisée pour les systèmes, rôles et processus les plus critiques. En ce qui concerne l'authentification par mot de passe, l'IMF voit à l'établissement et au respect des exigences relatives aux mots de passe[29].

d. L'accès de l'utilisateur aux ressources est déterminé et administré selon un modèle formel[30] appliquant une politique de contrôle de l'accès[31]. Le modèle choisi donne l'assurance que l'accès aux ressources est accordé uniquement aux personnes autorisées. La politique sur le contrôle de l'accès prévoit des mesures visant à retirer aux personnes qui n'ont plus d'autorisation les droits d'accès aux ressources.

e. Le principe de séparation des tâches vise les processus d'application et les transactions exposés à un risque de fraude ou d'utilisation malveillante[32]. Selon ce principe, personne ne peut accomplir seul l'ensemble des étapes de ces processus ou transactions.

f. Des processus sont établis pour gérer la création, la modification ou le retrait de comptes d'utilisateur et de droits d'accès. Ces interventions sont soumises à l'approbation du personnel compétent. Elles sont également enregistrées aux fins d'examen périodique.

g. Le nombre limite de tentatives de connexion infructueuses est fixé et respecté. Les mesures à prendre en cas de dépassement du nombre maximal de tentatives sont également précisées[33].

h. Le répertoire de tous les comptes d'utilisateur et de systèmes (notamment, des comptes privilégiés et des comptes d'accès à distance) et des droits d'accès y afférents est tenu à jour.

---

[27] Y compris les utilisateurs internes (p. ex., employés et contractuels) et externes (p. ex., participants à l'IMF)

[28] Par exemple, mots de passe, jetons, données biométriques, certificats d'infrastructure à clé publique ou cartes-clés

[29] Par exemple, le niveau de complexité minimal du mot de passe (longueur, type de caractères, etc.), sa durée et les règles relatives à sa réutilisation

[30] Par exemple, un contrôle de l'accès basé sur les rôles, sur des règles ou sur les attributs

[31] La politique peut être intégrée aux mécanismes de contrôle de l'accès et appliquée techniquement, ou elle peut prendre la forme d'une brève description (par écrit) et appliquée à l'aide de procédures manuelles (p. ex., ajout d'utilisateurs à des groupes dans un modèle de contrôle de l'accès basé sur les rôles).

[32] Par exemple, les gros volumes de transactions et les transactions de grande valeur

[33] Blocage temporaire, blocage jusqu'à ce qu'un administrateur active la connexion, etc.

i. Des mécanismes automatisés sont mis en place pour prendre en charge la gestion des comptes d'accès au système d'information. Il peut s'agir de contrôles de sécurité intégrés au système, permettant de désactiver et de supprimer automatiquement les comptes inactifs, les comptes temporaires et les comptes d'urgence après une période prédéterminée, ou encore d'outils servant à la gestion de l'identité et de l'accès, par exemple.

j. Le personnel concerné est automatiquement avisé lorsqu'un utilisateur se voit accorder un accès privilégié.

k. Des procédures particulières sont mises en place pour accorder un accès privilégié aux personnes qui en ont besoin pour accomplir leur travail ou au cas par cas.

l. Des mécanismes automatisés sont employés pour créer et modifier des comptes ainsi que pour assurer le suivi continu et la vérification des opérations d'activation, de désactivation et de suppression afin que le personnel concerné soit informé quand un comportement potentiellement malveillant ou une activité suspecte est détecté. Les mécanismes d'authentification de l'IMF respectent les pratiques exemplaires du secteur et les normes pertinentes[34].

3.4.3.2 Accès physique

22. L'IMF devrait s'assurer de ce qui suit :

a. Des périmètres de sécurité sont définis et utilisés pour protéger les sites qui renferment des informations sensibles ou essentielles et les installations de traitement de l'information.

b. Les zones sécurisées sont protégées par des mécanismes appropriés de contrôle d'entrée de façon à permettre l'accès au personnel autorisé seulement.

c. Le matériel informatique essentiel est placé en lieu sûr et protégé afin de réduire l'exposition aux menaces et risques environnementaux et la possibilité que des personnes non autorisées y aient accès. La protection physique du matériel informatique essentiel est assurée notamment par les dispositifs suivants : alimentation et éclairage de secours, systèmes d'extinction d'incendie ainsi que mécanismes de contrôle de la température et de l'humidité et de protection contre les dommages causés par l'eau. Les points d'accès sans fil et les câbles d'alimentation et de télécommunication pour les systèmes essentiels sont à l'abri de l'altération et des dommages.

d. Le matériel est entretenu adéquatement pour assurer son accessibilité et le maintien de son intégrité.

[34] Par exemple, NIST 800-53 et ISO 27001/27002

3.5 Formation

23. Tous les employés (y compris les membres de la direction générale et du conseil d'administration) et les contractuels devraient être tenus d'assurer la sécurité de l'information conformément aux politiques de cyberrésilience, aux normes techniques et aux procédures établies par l'IMF.

3.5.1 Ensemble du personnel de l'IMF

24. L'IMF devrait :

    a. veiller à ce que tout le personnel – permanent et temporaire – reçoive une formation lui permettant d'acquérir et de maintenir une connaissance adéquate des méthodes de détection et d'atténuation des cyberrisques ainsi que des compétences en la matière (p. ex., formation sur le harponnage);

    b. former le personnel sur le signalement d'activités inhabituelles ou d'incidents (p. ex., tentatives d'hameçonnage, demandes d'informations sensibles ou de mots de passe, demandes provenant de sources inconnues);

    c. s'assurer que ses employés comprennent bien les cyberrisques auxquels ils sont exposés dans le cadre de leur travail ainsi que leur rôle et leurs responsabilités en ce qui a trait à la protection des actifs de l'IMF, notamment les systèmes essentiels;

    d. intégrer une formation sur la cybersécurité à son programme d'accueil des nouvelles recrues;

    e. fournir une formation appropriée à ses employés appelés à exploiter de nouveaux systèmes ou applications avant que ceux-ci soient mis en service;

    f. s'assurer que son personnel est au courant des procédures opérationnelles standard;

    g. évaluer l'efficacité de sa formation pour déterminer si les connaissances qui y sont transmises ont des effets positifs sur le comportement, et modifier la formation au besoin[35].

3.5.2 Groupes à risque élevé

25. L'IMF devrait identifier les employés et les contractuels qui font partie des groupes à risque élevé, comme ceux qui bénéficient de droits d'accès privilégié aux systèmes ou qui occupent des fonctions névralgiques, et leur donner une formation ciblée sur la sécurité de l'information.

[35] Par exemple, tentatives de piratage psychologique ou d'hameçonnage

4 Détection

4.1 Préambule

Afin d'assurer une bonne cyberrésilience, l'IMF doit être en mesure de reconnaître les signes d'un cyberincident potentiel ou de détecter les brèches commises. La détection précoce permet à l'IMF de se préparer pour mettre en place des mesures appropriées afin de faire obstacle aux brèches éventuelles, et également de colmater de manière proactive les brèches perpétrées. Dans ce dernier cas, un endiguement précoce pourrait réduire l'incidence de l'attaque – par exemple, en empêchant un intrus d'accéder à des données confidentielles ou de les exfiltrer. Compte tenu de la nature furtive et très élaborée des cyberattaques ainsi que des nombreux points d'entrée par lesquels il peut y avoir compromission, l'IMF devrait veiller à maintenir les capacités nécessaires pour assurer une surveillance étroite et repérer les activités anormales.

La présente section décrit les mesures de protection et les capacités que devrait avoir l'IMF pour détecter les activités anormales, les cyberévénements et les cyberincidents.

4.2 Surveillance continue

La surveillance continue englobe les technologies, les processus et procédures, les environnements d'exploitation et les personnes nécessaires pour surveiller et détecter les activités et événements anormaux en temps réel (ou quasi réel).

1. L'IMF devrait mettre en place des mesures de surveillance continue par rapport au profil de base des activités de ses systèmes qui a été abordé à la sous-section 3.2.4.

2. L'IMF devrait :

    a. concevoir et mettre en œuvre des mécanismes de détection automatisés (p. ex., un système de gestion des informations et événements de sécurité) qui mettent en corrélation les alertes de ses réseaux et systèmes avec toute activité anormale dans ses unités organisationnelles;

    b. être en mesure de surveiller :

        i. l'activité utilisateur, les exceptions et les événements de cybersécurité;

        ii. les connexions réseau, les fournisseurs de services externes, les dispositifs et les logiciels;

    c. assurer une surveillance et un contrôle continus du trafic réseau, y compris les connexions à distance ainsi que la configuration des points terminaux et l'activité à ces points, afin d'identifier rapidement et en temps opportun les vulnérabilités potentielles ou les événements anormaux;

    d. comparer le trafic réseau et la configuration des points terminaux avec le trafic attendu;

e. définir les seuils d'alerte pour ses systèmes de surveillance et de détection afin de déclencheret de faciliter le processus d'intervention en cas d'incident;

f. veiller à ce que ses capacités de détection, le profil de base des activités de ses systèmes ainsi que les critères, paramètres et déclencheurs soient revus, testés et actualisés régulièrement de façon appropriée et ordonnée, avec les autorisations requises;

g. surveiller en continu les liens entre ses actifs informationnels pendant tout leur cycle de vie, et recueillir, stocker et analyser ces données pour faciliter les interventions en cas d'incident et les investigations numériques.

4.3 Cadre de surveillance complet

Le cadre de surveillance requis est à la fois vaste et approfondi. Il englobe les fonctions opérationnelles, les transactions et les processus d'applications, les dispositifs de systèmes et de réseau, ainsi que les communications. Il tient compte des activités et menaces à l'interne, de même que des menaces provenant de l'extérieur.

3. L'IMF devrait :

a. recueillir des données sur les tendances et comportements (utilisation du réseau, heures de travail, appareils connus, etc.), et les surveiller et les analyser. Cette démarche aide une IMF à identifier les activités anormales, et à évaluer la mise en œuvre de nouvelles solutions (analyse de données, apprentissage automatique, intelligence artificielle, etc.) et de nouveaux contrôles à l'appui de la détection des menaces internes et des mesures prises pour intervenir en temps réel;

b. voir à ce que ses capacités de détection reçoivent l'information pertinente sur les menaces et les vulnérabilités – une information pouvant être recueillie auprès de différentes sources et de divers fournisseurs;

c. mettre en œuvre un mécanisme perfectionné de détection afin d'identifier les menaces connues et d'accroître la probabilité de repérer celles qui visent à exploiter des vulnérabilités inconnues jusque-là (jour zéro) ou qui s'appuient sur des méthodes, techniques et chaînes d'attaque inédites;

d. s'assurer de bien comprendre les menaces d'utilisation malveillante provenant de sources internes et de tiers de confiance et de modéliser ces menaces, ainsi que de disposer des capacités nécessaires pour détecter ces menaces au sein des applications, des bases de données, des systèmes et des réseaux;

e. avoir en place des processus pour surveiller les activités qui ne respectent pas sa politique de sécurité et qui pourraient entraîner une perte de confidentialité ou d'intégrité, ou encore le vol ou la destruction de données.

4.4 Détection en couches

Il faut être en mesure de détecter les intrusions dès le début pour rapidement les endiguer et assurer un rétablissement.

4. L'IMF devrait mettre en œuvre des capacités de détection en instaurant des contrôles de détection en couches s'appliquant aux personnes, aux processus et aux technologies[36]. Chaque couche devrait servir de filet de sécurité aux couches antérieures pour leur permettre de détecter une attaque et de retarder et entraver la progression de son auteur dans une chaîne ou séquence d'attaques. De bonnes capacités de détection des intrusions pourraient aider l'IMF à identifier les failles de ses mesures de protection et à les corriger rapidement, le cas échéant.

5. L'IMF devrait explorer constamment de nouvelles technologies et techniques pour contrer les mouvements latéraux. Ces technologies et techniques devraient déclencher des alertes et informer l'IMF d'éventuelles activités malveillantes.

4.5 Intervention en cas d'incident

Les capacités de surveillance et de détection de l'IMF devraient faciliter son processus d'intervention en cas d'incident ainsi qu'appuyer la collecte d'information pour les investigations numériques.

6. Les capacités de surveillance et de détection de l'IMF devraient permettre de déclencher une notification au personnel concerné.

7. Pour faciliter l'investigation numérique, l'IMF devrait s'assurer de ce qui suit :

    a. les anomalies et événements détectés sont consignés dans les journaux des systèmes ou les journaux d'événements;

    b. ces journaux contiennent l'information nécessaire pour appuyer les enquêtes (type d'événement, heure de l'événement, nom et adresse de l'utilisateur, etc.);

    c. il y a suffisamment d'espace de stockage pour les journaux nécessaires;

    d. les outils d'audit et l'information issue des audits sont protégés de sorte que personne ne peut y accéder et les modifier ou les supprimer sans autorisation.

8. L'IMF devrait veiller à ce que ses journaux soient sauvegardés dans un lieu sûr muni des contrôles nécessaires pour réduire le risque d'altération.

9. L'IMF devrait mettre en œuvre un mécanisme pour assurer la synchronisation des journaux corrélés.

---

[36] Exemples de contrôles s'appliquant à des 1) personnes : audits et rapprochements, analyses comportementales, rotation des postes, journalisation et surveillance; 2) processus : audit, analyse des écarts, journalisation et surveillance; et 3) technologies : surveillance continue de la sécurité, détection et intervention aux points terminaux, système de détection des intrusions, système de protection contre les intrusions et système de détection des maliciels.

10. L'IMF devrait mettre en place un processus visant à recueillir, à centraliser et à corréler l'information sur les événements (y compris sur les activités anormales) provenant de sources variées ainsi qu'à consigner ses analyses pour surveiller en continu l'environnement informatique (bases de données, serveurs et points terminaux, etc.). Le processus pourrait être accompli par l'entremise d'un centre des opérations de sécurité, d'un centre d'exploitation de réseau ou l'équivalent.

5 Intervention et rétablissement

5.1 Préambule

La stabilité financière peut dépendre de la capacité de l'IMF de régler ses obligations à l'échéance. C'est pourquoi les dispositifs de l'IMF devraient être conçus pour lui permettre de reprendre ses activités essentielles de façon sûre et rapide, avec des données exactes, afin de réduire le risque potentiellement systémique de manquer à ses obligations alors que les participants s'attendent à ce qu'elle les respecte. La planification de la continuité des opérations est essentielle à l'atteinte des objectifs connexes.

La présente section fournit des orientations générales concernant les capacités d'intervention et de rétablissement de l'IMF en cas de cyberattaque.

5.2 Intervention en cas d'incident, reprise des activités et rétablissement

L'IMF devrait développer de solides capacités de gestion des cyberincidents afin de réduire l'incidence que ceux-ci pourraient avoir sur elle-même et sur son écosystème. L'IMF devrait mettre en place des plans décrivant les mesures à prendre à diverses étapes de son processus de gestion des cyberincidents, notamment l'intervention, la reprise des activités et le rétablissement.

5.2.1 Planification et préparation

1. L'IMF devrait élaborer des plans exhaustifs d'intervention, de reprise des activités et de rétablissement afin de bien gérer les cyberincidents[37]. Ces plans devraient avoir pour objet de limiter les dommages et de prioriser les mesures de reprise des activités et de rétablissement qui facilitent le traitement des transactions critiques tout en réduisant le temps de récupération et les coûts connexes. Le plan d'intervention décrit les mesures à prendre dès qu'un cyberincident est détecté. Le plan de reprise des activités comprend des mesures visant la restauration et la relance des opérations essentielles de l'IMF – peut-être avec des capacités restreintes –, que celle-ci appliquerait aussitôt qu'il serait sûr et possible de le faire (le délai visé étant de deux heures). Et, le plan de rétablissement précise

[37] Si l'IMF ne dispose pas de plans distincts pour l'intervention, la reprise des activités et le rétablissement, son ou ses plans devraient néanmoins présenter séparément les étapes nécessaires pour intervenir en cas de cyberincident, reprendre ses activités et se rétablir.

les mesures permettant à l'IMF d'assurer un retour à un état de marche normal et pleinement fonctionnel en toute sécurité, ce qui peut exiger un certain temps.

2. Les plans d'intervention, de reprise des activités et de rétablissement devraient définir les politiques et procédures en la matière, ainsi que les rôles et responsabilités à l'égard du signalement des cyberincidents aux échelons supérieurs, de l'intervention et du rétablissement.

3. Dans le cadre de l'élaboration de ses plans, l'IMF devrait :

    a. intégrer une plage de scénarios extrêmes mais plausibles afin de déterminer l'incidence possible de ces scénarios sur elle-même et sur l'ensemble de l'écosystème;

    b. consulter toutes les unités organisationnelles et parties prenantes externes concernées, et travailler en concertation avec elles.

4. L'IMF devrait mettre ses plans à jour régulièrement. Il lui faut notamment :

    a. revoir sa plage de scénarios;

    b. effectuer des analyses des répercussions sur les opérations en fonction de l'évolution de l'ensemble des menaces;

    c. intégrer les leçons tirées des cyberincidents antérieurs, y compris les résultats des analyses des causes fondamentales.

5. L'IMF devrait tester régulièrement ses plans d'intervention, de reprise des activités et de rétablissement en fonction d'un éventail de scénarios.

6. L'IMF devrait consulter les parties prenantes externes concernées (p. ex., les participants, les fournisseurs de services et d'autres IMF) de l'écosystème pour peaufiner ses plans d'intervention, de reprise des activités et de rétablissement.

7. L'IMF devrait également mettre en place des processus pour améliorer constamment ses plans d'intervention, de reprise des activités et de rétablissement, en tenant compte des sources de renseignements sur les cybermenaces (p. ex., des flux), des informations mises en commun au sein de l'écosystème ainsi que des leçons tirées d'événements antérieurs.

5.2.2 Reprise des activités dans un délai de deux heures (objectif de temps de récupération)

8. Les objectifs de reprise des activités devraient être planifiés et testés. Conformément à la considération essentielle 17.6 des PIMF, l'IMF devrait concevoir et tester ses systèmes et processus de manière à assurer :

    a. la reprise en toute sécurité de ses opérations essentielles dans les deux heures suivant une cyberperturbation;

b. l'exécution de ses règlements avant la fin de la journée où a eu lieu la perturbation, même en cas de scénarios extrêmes mais plausibles.

9. Pour planifier une reprise des activités dans un délai de deux heures après un cyberincident, il faut très bien comprendre les différentes fonctions et les divers processus opérationnels de l'IMF. Il n'y a pas de solution unique pour l'ensemble des IMF. L'IMF devrait faire appel à son équipe technique et à son équipe opérationnelle pour planifier soigneusement la reprise des activités en tenant compte des risques propres à sa conception, à ses fonctions essentielles et à ses processus opérationnels. Même si elle a la capacité de reprendre ses opérations essentielles dans un délai de deux heures, l'IMF devrait exercer son jugement (en accord avec les autorités de réglementation et de surveillance et les parties prenantes concernées) au moment de les relancer. L'IMF doit se demander si la reprise de ses activités pourrait accroître les risques pour elle-même ou son écosystème, tout en gardant à l'esprit que l'exécution de ses règlements avant la fin de la journée est primordiale.

5.2.3 Plans d'urgence

10. En plus de planifier une reprise en toute sécurité de ses opérations essentielles dans les deux heures suivant une perturbation, l'IMF devrait prévoir des scénarios où elle ne réussirait pas à atteindre cet objectif. Elle devrait analyser les fonctions essentielles, les transactions et les interdépendances afin de prioriser les mesures de reprise des activités et de rétablissement qui, selon sa conception, pourraient l'aider à traiter les transactions essentielles tout en poursuivant ses efforts pour corriger la situation. L'IMF devrait également prévoir des cas où des personnes, processus ou systèmes essentiels seraient indisponibles pendant une longue période. Elle pourrait, par exemple, passer au traitement manuel (dans la mesure où il serait sûr et possible de le faire) si les systèmes automatisés ne fonctionnent pas.

11. L'IMF devrait établir un plan d'urgence fondé sur des scénarios où il lui serait impossible de reprendre ses activités dans un délai de deux heures. Ce plan devrait :

    a. indiquer comment l'IMF pourrait atteindre ses objectifs de rétablissement et respecter ses priorités en matière de restauration;

    b. définir les rôles et responsabilités;

    c. présenter des options pour réacheminer ou remplacer les fonctions et services essentiels susceptibles d'être perturbés pendant une longue période à la suite d'une cyberattaque réussie.

12. L'IMF doit planifier la façon dont elle pourrait mener ses activités avec des capacités restreintes ou rétablir ses services de manière sûre au fil du temps, en fonction de leur priorité relative, et avec des données exactes.

5.2.4 Intervention en cas d'incident et enquête

13. L'IMF devrait disposer de vastes capacités d'intervention en cas de cyberincident, dont la détection et l'analyse; l'endiguement, l'éradication et le rétablissement; et l'activité post-incident. Ces capacités devraient permettre à l'IMF d'analyser les cyberincidents dès qu'ils sont détectés, tout en minimisant les interruptions de service et en mettant en branle les processus de reprise des activités, d'endiguement et de rétablissement. L'IMF peut aussi conclure des accords de coopération directe ou des ententes contractuelles avec des organisations ou fournisseurs offrant des services d'intervention qui pourront l'aider rapidement à atténuer les risques. Elle pourrait également mettre directement à contribution ses unités organisationnelles pour prioriser ses activités.

14. En outre, l'IMF devrait avoir des politiques et des procédures ainsi que les capacités nécessaires pour réaliser des enquêtes approfondies sur les cyberattaques, y compris des analyses des causes fondamentales et des investigations numériques. L'IMF peut faire appel à des ressources internes ou à des fournisseurs de services externes avec qui elle a conclu des ententes contractuelles pour s'assurer que les enquêtes sont amorcées rapidement lorsque des cyberattaques sont détectées.

15. Au moment où une cyberattaque réussie ou une tentative de cyberattaque est détectée et confirmée, l'IMF devrait mettre en œuvre ses capacités d'enquête pour être en mesure de déterminer la nature et l'ampleur de l'attaque ainsi que les dommages occasionnés.

16. Pendant l'enquête, l'IMF devrait prendre des mesures immédiates pour endiguer la cyberattaque ou la tentative de cyberattaque afin de limiter les dommages, et commencer les démarches pour reprendre ses activités selon son plan d'intervention. Les activités d'enquête peuvent s'étendre sur une période plus ou moins longue, tandis que les activités d'intervention sont plus rapides et visent principalement à minimiser les dommages, à prioriser la reprise des activités et à assurer l'exécution des règlements avant la fin de la journée.

17. L'IMF devrait établir des critères et des procédures pour signaler les cyberincidents au conseil d'administration et à la direction générale en fonction de l'incidence potentielle et de la criticité du risque.

18. L'IMF devrait également avoir des procédures en place pour porter les incidents à l'attention des forces de l'ordre, s'il y a lieu.

19. L'IMF devrait former les membres de son personnel pour qu'ils comprennent bien leur rôle et leurs responsabilités à l'égard de la gestion des preuves numériques, afin que celles-ci ne soient pas compromises et restent valides conformément aux exigences des autorités locales.

5.2.5 Capacité d'investigation numérique

20. L'IMF devrait acquérir la capacité d'appuyer les investigations numériques ou d'y contribuer. Elle devrait notamment se doter de contrôles de protection et de détection

sur le plan technique pour faciliter le processus d'enquête. L'IMF devrait établir des politiques pertinentes de journalisation système qui tiennent compte du contenu requis du journal d'audit, de la synchronisation des journaux et des événements ainsi que des périodes de conservation des fichiers journaux.

21. L'IMF devrait mettre en place des procédures visant à ce que les preuves numériques soient gérées, recueillies et conservées de manière sûre, et que leur authenticité et leur intégrité soient préservées, pour que des investigations numériques puissent être menées après l'événement ou après la reprise des opérations essentielles.

5.3 Éléments liés à la conception

Au moment de concevoir de nouveaux systèmes et processus, l'IMF devrait réfléchir à la manière dont ils pourront soutenir les activités d'intervention en cas d'incident. La conception de processus opérationnels, de systèmes d'information, et de contrôles des activités d'intervention et de rétablissement a une grande incidence sur la capacité de l'IMF à reprendre ses activités essentielles dans un délai de deux heures.

5.3.1 Conception et intégration opérationnelle

22. La conception des systèmes et processus et les contrôles des fonctions et opérations essentielles devraient faciliter le plus possible les activités d'intervention en cas d'incident. L'IMF devrait concevoir ses systèmes et processus de manière à limiter l'incidence des cyberincidents, à reprendre ses activités essentielles dans les deux heures suivant une perturbation, à effectuer ses règlements avant la fin de la journée et à préserver l'intégrité de ses transactions.

23. L'IMF devrait prendre en considération un éventail de scénarios ainsi que d'éventuelles mesures d'intervention et leurs effets potentiels au moment d'élaborer ses systèmes et processus. Afin d'atteindre l'objectif de reprise des activités dans un délai de deux heures, l'IMF doit soigneusement sélectionner et mettre en œuvre des méthodes et techniques lui permettant d'effectuer ses règlements ainsi que des outils et technologies pour rétablir la configuration de ses systèmes et récupérer les données de ceux-ci. Les solutions retenues dépendront de divers facteurs, notamment la conception et la complexité des systèmes, la fréquence et le volume de transactions, et l'étape où se situent les systèmes dans leur cycle de vie[38]. Il n'existe pas de solution unique pour l'ensemble des IMF et des systèmes essentiels.

---

[38] L'étape où se situent les systèmes de l'IMF dans leur cycle de vie est peut-être le facteur le plus important à considérer pour le choix de solutions favorisant une reprise rapide des activités. Dans le cas des systèmes que l'on commence à développer ou que l'on transforme ou renouvelle, les solutions peuvent être intégrées de façon globale : dans les processus opérationnels et l'interface humaine; dans les applications; dans le logiciel de base; et dans les infrastructures informatiques, réseau et de stockage. Pour les systèmes existants, par contre, le choix de solutions peut être très limité et, dans certains cas, leur coût peut s'avérer exorbitant. Cela dit, l'IMF devrait tout de même chercher les solutions permettant de réduire le plus possible le délai de reprise des activités, de manière progressive.

5.3.2 Intégrité des données

24. L'IMF devrait définir et identifier les données essentielles à la reprise des services et qui doivent être sauvegardées. Parmi ces données, que l'IMF devrait pouvoir récupérer dans un délai prévisible, on trouve non seulement celles sur les transactions, mais aussi d'autres données essentielles comme le code source, les données de référence de l'entreprise et les données de configuration.

25. L'IMF devrait avoir des plans permettant de connaître rapidement et en temps opportun l'état de toutes les transactions et la position des membres au moment d'une perturbation, ainsi que des objectifs de point de récupération à l'appui. L'IMF devrait donc concevoir et tester ses systèmes et processus pour permettre la récupération de données exactes à la suite d'une brèche. Des mesures rigoureuses de protection et de détection devraient assurer la préservation de l'information et des données.

26. Les objectifs de point de récupération, qui ont pour but de favoriser l'intégrité des données, devraient être cohérents avec l'objectif de temps de récupération des opérations essentielles établi par l'IMF.

27. Les objectifs de point de récupération et les options de récupération des données devraient être établis en étroite collaboration avec les fonctions opérationnelles et les services TI. Une telle collaboration peut aider une organisation à répondre à des questions fondamentales sur la façon d'effectuer des opérations essentielles lorsque des données sont corrompues.

28. Les solutions de sauvegarde de l'IMF devraient être configurées pour s'aligner sur la fréquence et le volume des transactions. Étant donné qu'une IMF effectue des milliers de transactions par heure tous les jours, une solution qui prévoit une seule sauvegarde de données par jour n'offrira pas une protection adéquate, à moins que d'autres solutions de récupération des transactions de la base de données soient aussi mises en place.

29. Le cadre de cyberrésilience devrait inclure des mesures de récupération des données et l'IMF devrait envisager différentes options à cet égard. Ces options devraient être choisies sur la base d'une analyse détaillée permettant de déterminer quelles données sont essentielles aux opérations de l'IMF. Celle-ci établira notamment quelles sont les données nécessaires pour assurer une reprise des activités dans un délai de deux heures, ainsi que l'incidence de divers cyberscénarios (dont la perte et la manipulation de données) sur l'intégrité de ces données.

30. Les données sauvegardées (au repos et en transit) devraient être protégées pour assurer leur confidentialité, leur intégrité et leur disponibilité. Les sauvegardes devraient être testées régulièrement pour vérifier leur disponibilité et leur intégrité.

31. Voici des exemples de solutions de récupération des données que les IMF devraient envisager :

    a. mettre en œuvre des mécanismes de récupération d'un enregistrement de la base de données, qui pourraient comprendre une récupération par régression et une

journalisation ou une récupération par progression pour réparer des données corrompues;

b. procéder à un rapprochement indépendant plus fréquent des positions des participants;

c. conserver une copie de toutes les données reçues et traitées, et l'information connexe;

d. utiliser des technologies sécurisées afin de stocker les fichiers les plus cruciaux pour la reprise des activités, notamment les données sur les transactions et les données de référence essentielles, les fichiers de configuration et les journaux. Il pourrait s'agir, par exemple, de bases de données à accès sécurisé (espace de stockage où l'on peut sauvegarder des données, mais qui restreint la consultation grâce à des procédés d'authentification et de gestion robustes) et de lecteurs non réinscriptibles.

5.4 Interconnexions

En cas de cyberincident, l'IMF devrait coordonner ses interventions avec ses entités et parties prenantes liées. Elle devrait mettre en œuvre des mesures pour faciliter cette coordination, et planifier la manière dont elle communiquera et coordonnera ses interventions dans l'éventualité d'une cyberattaque.

5.4.1 Accords de partage de données

32. L'IMF devrait avoir, au besoin, un accord de partage de données avec des tiers ou des participants qui facilitera l'obtention de données non corrompues de leur part, si nécessaire, pour reprendre ses activités rapidement, en temps opportun, et avec des données exactes.

33. L'IMF devrait revoir régulièrement les règles, accords et protocoles de partage d'information afin d'encadrer la publication et la distribution de l'information et d'empêcher la divulgation inappropriée de données sensibles, qui pourrait avoir des conséquences néfastes.

5.4.2 Contagion

34. En cas de cyberincident à grande échelle, une IMF risque de contaminer son écosystème ou d'être contaminée par celui-ci. Il y a donc un risque de contagion, c'est-à-dire la propagation de maliciels ou de données corrompues. L'IMF devrait élaborer des politiques et des procédures définissant la manière dont elle collaborera avec les entités interconnectées concernées pour permettre la reprise des activités (la priorité absolue étant ses fonctions et services essentiels) dès qu'il est sûr et possible de le faire sans causer de risque inutile pour le secteur au sens large ou le système financier.

5.4.3 Communication en cas de crise

35. L'IMF devrait élaborer un plan de communication et des procédures pour communiquer avec les participants, les IMF liées, les autorités et d'autres entités (p. ex., des fournisseurs de services et les médias, s'il y a lieu). Ce plan de communication devrait être basé sur une planification et une analyse fondées sur des scénarios ainsi que sur l'expérience passée.

36. Le plan d'intervention en cas d'incident de l'IMF devrait énumérer les parties prenantes internes et externes à informer d'un incident, les responsabilités et autorités décisionnelles, l'information à partager et à communiquer, et le moment où l'information devrait être fournie.

37. L'IMF devrait aviser immédiatement les organismes de surveillance et de réglementation de tout cyberincident qui pourrait être important ou systémique. Elle devrait signaler à la Banque les cyberincidents conformément aux *Lignes directrices concernant le signalement des cyberincidents et des incidents liés aux technologies de l'information*.

38. L'IMF devrait aussi établir des procédures pour porter les incidents à l'attention des forces de l'ordre lorsqu'elle soupçonne une intention criminelle (p. ex., fraude, extorsion).

5.4.4 Politique de divulgation responsable

39. L'IMF devrait disposer d'une politique et de procédures permettant une divulgation responsable des vulnérabilités et des risques potentiels au sein de son écosystème, durant ses interventions en temps réel face à une cyberattaque ou à un incident. En particulier, l'IMF devrait divulguer en priorité l'information susceptible d'aider les participants et d'autres parties prenantes à intervenir promptement et à atténuer leurs propres risques, ce qui pourrait être bénéfique pour l'écosystème et la stabilité financière dans son ensemble.

6 Tests

6.1 Préambule

Tout cadre de cyberrésilience devrait prévoir des tests rigoureux de ses éléments pour déterminer leur efficacité globale. Ces tests, réalisés avant le déploiement au sein de l'IMF et régulièrement par la suite, permettent de vérifier si le cadre est mis en œuvre comme il se doit, s'il fonctionne comme prévu et s'il donne les résultats escomptés. Il est essentiel de comprendre l'efficacité globale du cadre de cyberrésilience dans l'IMF et son environnement pour définir les cyberrisques résiduels qui pèsent sur les opérations, les actifs et l'écosystème de l'IMF.

Un solide programme de tests donne des résultats qui aident à identifier les lacunes des objectifs de résilience énoncés, et apporte une contribution crédible et significative au processus de gestion des cyberrisques de l'IMF. L'analyse des résultats propose des pistes pour combler (au moins en partie) les faiblesses, les failles et les lacunes de l'IMF en matière de cyberrésilience globale.

Cette section donne un aperçu des composantes d'un programme de tests et de la manière dont l'IMF peut se servir des résultats obtenus pour améliorer sa cyberrésilience globale en continu. Le programme peut comprendre des évaluations des vulnérabilités, des tests basés sur des scénarios, des tests d'intrusion et des tests menés par une équipe rouge.

6.2 Programme exhaustif de tests

Une IMF devrait avoir un programme exhaustif de tests pour valider l'efficacité de son cadre de cyberrésilience. Les tests servent d'outil pour aider les IMF à identifier les failles de leurs contrôles de sécurité. Cependant, en raison des contraintes pratiques des tests, la réussite de ceux-ci ne signifie pas qu'aucune faille n'existe ni que le système répond adéquatement aux objectifs de sécurité concernant la confidentialité, l'intégrité, l'authentification, la disponibilité, l'autorisation et la non-répudiation.

1. Un programme exhaustif de tests devrait faire partie intégrante du cadre de cyberrésilience de l'IMF. Ce programme devrait être élaboré selon une approche basée sur le risque et faire appel à une vaste gamme de méthodes, de pratiques et d'outils permettant de suivre et d'évaluer l'efficacité des principales composantes du cadre.
2. Le programme devrait être revu et actualisé régulièrement pour tenir compte de l'évolution de l'ensemble des menaces et de la criticité des actifs informationnels.
3. L'IMF devrait se doter des capacités appropriées et faire participer toutes les parties prenantes internes concernées (y compris les secteurs d'activité et les unités organisationnelles) à la mise en œuvre du programme. Au besoin, les tests devraient mobiliser les équipes chargées de la continuité des opérations ainsi que des interventions en cas d'incident et de crise.
4. L'IMF devrait aussi collaborer avec les entités de son écosystème pour améliorer sa cyberrésilience globale, ce qui aide par le fait même à renforcer la résilience de l'écosystème.
5. L'IMF devrait faire jouer un rôle approprié aux membres de son conseil d'administration et de la direction générale (p. ex., au sein des équipes de gestion de crise), et les tenir informés des résultats des tests.
6. Afin d'améliorer en continu sa cyberrésilience globale, l'IMF devrait établir des politiques et des procédures lui permettant de déterminer à quels problèmes s'attaquer en priorité parmi ceux mis en lumière durant les différents tests et de les résoudre, et d'ensuite évaluer si les lacunes ont été entièrement comblées.

6.2.1 Méthodes, pratiques et outils

7. L'IMF devrait faire appel à tout un éventail de méthodes, de pratiques et d'outils, dont des évaluations des vulnérabilités, des tests basés sur des scénarios, des tests d'intrusion et des tests menés par une équipe rouge (qui peuvent se chevaucher ou être combinés).

6.2.1.1 Évaluation des vulnérabilités

8. L'IMF devrait élaborer un processus de gestion des vulnérabilités qu'elle actualisera régulièrement, afin de classifier, de hiérarchiser et de résoudre les faiblesses potentielles identifiées durant les évaluations des vulnérabilités, et ensuite évaluer si les lacunes ont été entièrement comblées.

9. Le processus de gestion des vulnérabilités de l'IMF devrait aider à repérer les faiblesses exploitables[39] des systèmes et technologies essentiels, de même que les conditions qui font que des erreurs humaines et des accidents peuvent nuire aux fonctions essentielles, aux processus connexes et aux actifs informationnels.

10. L'IMF devrait effectuer régulièrement des dépistages des vulnérabilités de ses services destinés à l'extérieur ainsi que de ses systèmes et réseaux internes. Ces tâches devraient être exécutées en rotation pour qu'au bout de l'année le dépistage de tous les environnements ait été réalisé.

11. L'IMF devrait mener des évaluations des vulnérabilités avant chaque déploiement ou redéploiement de services nouveaux ou existants qui soutiennent des fonctions, des applications et des composantes d'infrastructure essentielles, afin de corriger les bogues et les faiblesses. Ces évaluations devraient être effectuées conformément aux processus de gestion des changements et de gestion des versions qui sont en place.

12. L'IMF devrait réaliser périodiquement des évaluations des vulnérabilités touchant les services, applications et composantes d'infrastructure courants. Elle devrait s'assurer d'observer la réglementation, les politiques et les configurations, ainsi que suivre et évaluer l'efficacité des contrôles de sécurité adoptés pour réduire les vulnérabilités identifiées.

13. Dans le cadre de son processus de gestion des vulnérabilités, l'IMF devrait élaborer et adopter un éventail de pratiques et d'outils efficaces[40] ainsi que disposer de mesures de protection appropriées pour les gérer.

6.2.1.2 Tests basés sur des scénarios

14. L'IMF devrait réaliser différents tests, y compris pour des scénarios extrêmes mais plausibles, afin d'évaluer et d'améliorer ses capacités de détection des incidents ainsi que ses plans d'intervention, de reprise des activités et de rétablissement. Ces plans devraient être revus et testés périodiquement. Les tests basés sur des scénarios peuvent prendre la forme d'exercices sur table ou de simulations.

15. L'IMF devrait concevoir des tests qui :

    a. permettent de simuler un éventail assez large de scénarios, y compris des cyberattaques extrêmes, mais plausibles;

---

[39] Une faiblesse exploitable est une vulnérabilité ou une faille qu'un pirate peut utiliser pour compromettre la sécurité d'un système.

[40] Par exemple, un programme de prime aux bogues ou des examens de code statiques et dynamiques

b. remettent en question les hypothèses quant aux pratiques d'intervention, de reprise des activités et de rétablissement, y compris les modalités de gouvernance et les plans de communication;

c. simulent la destruction, la corruption et la perte de données, et qui mettent à l'épreuve la disponibilité des systèmes et des données;

d. couvrent des brèches touchant plusieurs parties de l'écosystème de l'IMF de manière à identifier et à analyser les difficultés potentielles, les interdépendances et la contagion possible à l'échelle de l'entreprise et des opérations.

16. L'IMF devrait utiliser les renseignements sur les cybermenaces et modéliser celles-ci de façon à imiter les caractéristiques uniques de ces menaces. Elle devrait aussi effectuer des exercices pour tester les processus et la capacité du personnel à réagir à des scénarios inhabituels, dans le but d'accroître la résilience des opérations.

17. Le conseil d'administration et la direction générale de l'IMF devraient prendre part aux tests basés sur des scénarios, s'il y a lieu.

6.2.1.3 Tests d'intrusion

18. L'IMF devrait effectuer des tests d'intrusion pour identifier les vulnérabilités qui pourraient toucher ses systèmes, ses réseaux, ses applications, son personnel ou ses processus. Pour évaluer en profondeur la sécurité des systèmes de l'IMF, ces tests devraient simuler des attaques réelles.

19. Les tests d'intrusion devraient être menés régulièrement et lorsque des systèmes sont déployés ou font l'objet de mises à jour majeures.

20. L'IMF devrait faire participer aux tests d'intrusion, s'il y a lieu, toutes les parties prenantes internes et externes jouant un rôle essentiel. Il pourrait notamment s'agir des propriétaires d'applications et de systèmes, ainsi que des équipes chargées de la continuité des opérations et des interventions en cas d'incident et de crise.

21. L'IMF devrait intégrer les pratiques de tests à son processus de gestion des risques d'entreprise dans le but d'identifier, d'analyser et de corriger les vulnérabilités de cybersécurité découlant de nouveaux produits, services ou interconnexions.

22. L'IMF devrait effectuer des évaluations et des tests de sécurité, chaque fois que cela est nécessaire, à toutes les étapes du cycle de vie d'un système et à tous les niveaux (entreprise, application et technologie) pour le portefeuille d'applications au complet, y compris les applications mobiles.

23. L'IMF devrait adopter des pratiques exemplaires et des outils automatisés à l'appui des processus et procédures permettant de corriger les faiblesses techniques et organisationnelles décelées durant les tests. Elle devrait aussi avoir des pratiques et des outils pour vérifier le respect des politiques et configurations approuvées.

6.2.1.4 Tests menés par l'équipe rouge

24. L'IMF devrait mettre à l'épreuve son organisation et son écosystème en faisant appel à ce qu'on nomme des « équipes rouges » pour obtenir un point de vue de l'adversaire dans des conditions contrôlées. Ces équipes tentent de trouver des vulnérabilités et testent l'efficacité des mesures d'atténuation de l'IMF, y compris celles qui impliquent son personnel, ses processus et ses technologies. Une équipe rouge peut être constituée d'employés de l'IMF ou d'experts de l'extérieur qui, dans un cas comme dans l'autre, ne participent pas à la fonction faisant l'objet du test. L'équipe rouge devrait, régulièrement, effectuer des exercices et avoir des échanges avec l'équipe chargée de la cyberdéfense (p. ex., l'équipe bleue) concernant ses observations et les améliorations à apporter à la cyberrésilience globale de l'IMF.

25. L'IMF devrait aussi baser ses méthodes de tests sur des renseignements appropriés sur les cybermenaces, par exemple en concevant des tests pour simuler l'action d'auteurs de menaces ayant des capacités avancées et des scénarios extrêmes mais plausibles. L'équipe rouge de l'IMF devrait effectuer des exercices en se fondant sur des renseignements fiables et de qualité, et sur des scénarios de menace détaillés et plausibles.

6.3 Coordination

Pour identifier les difficultés, les interdépendances et les faiblesses potentielles de ses plans d'intervention, de reprise des activités et de rétablissement, l'IMF doit effectuer des tests en collaboration avec les entités de son écosystème. Cela aide à améliorer ces plans et accroît, au bout du compte, la résilience de l'IMF et de son écosystème.

26. L'IMF devrait, dans la mesure du possible, favoriser, concevoir, organiser et gérer des exercices permettant de tester ses plans et processus d'intervention, de reprise des activités et de rétablissement. Ces exercices devraient mettre à contribution les participants à l'IMF, les fournisseurs de services essentiels et les IMF liées, s'il y a lieu.

27. L'IMF devrait prendre part aux tests et exercices sectoriels organisés par les autorités pertinentes. Pour que la reprise des activités de l'ensemble du marché se fasse rapidement et dans les délais prévus, ces tests et exercices nécessitent une dimension supplémentaire. Habituellement, les tests effectués par une seule IMF supposent implicitement que les activités de tous les autres acteurs du marché se poursuivent normalement. En écartant cette hypothèse, l'IMF est en mesure d'identifier les difficultés, les interdépendances et les faiblesses potentielles qu'elle aurait pu négliger d'inclure dans ses plans d'intervention, de reprise des activités et de rétablissement. Par conséquent, les tests devraient prévoir des scénarios qui tiennent compte de brèches touchant plusieurs parties de l'écosystème de l'IMF.

7 Connaissance de la situation

7.1 Préambule

La connaissance de la situation, c'est la compréhension qu'a une IMF des cybermenaces qui émanent de son environnement, ainsi que des implications pour ses activités et le caractère adéquat de ses mesures d'atténuation des cyberrisques. Une bonne connaissance de la situation, acquise au moyen d'un processus efficace de renseignement sur les cybermenaces, peut considérablement aider à prévenir des cyberévénements ou à intervenir rapidement et efficacement quand ils se produisent. En particulier, une profonde connaissance de l'ensemble des menaces peut aider une IMF à mieux comprendre les vulnérabilités de ses fonctions opérationnelles essentielles et faciliter l'adoption de stratégies d'atténuation des risques appropriées. Elle peut également permettre de valider l'orientation stratégique, l'affectation des ressources, les processus, les procédures et les contrôles de l'IMF en vue de renforcer sa cyberrésilience. Une bonne connaissance de la situation d'une IMF et de son écosystème passe impérativement par une participation active de celle-ci à des accords de partage d'information, ainsi que par une collaboration avec des parties prenantes de confiance du secteur et de l'extérieur.

Cette section fournit aux IMF des conseils pour l'établissement d'un processus de renseignement sur les cybermenaces ainsi que de processus d'analyse et de partage d'information.

7.2 Renseignements sur les cybermenaces

Les renseignements sur les cybermenaces sont des informations agrégées, transformées, analysées, interprétées ou enrichies pour fournir le contexte nécessaire aux processus décisionnels.

1. L'IMF devrait identifier les cybermenaces qui pourraient avoir une incidence considérable sur sa capacité à exercer ses activités, à fournir des services de la manière attendue ou à remplir ses obligations, ou qui auraient des effets indirects sur son écosystème. L'analyse de l'IMF devrait faire état des menaces susceptibles de provoquer des cyberévénements extrêmes mais plausibles, même s'ils sont considérés comme étant improbables ou inédits. L'analyse devrait être revue et mise à jour régulièrement.

2. L'IMF devrait :

    a. établir un processus de collecte et d'analyse de renseignements pertinents sur les cybermenaces. Pour fournir un contexte propre à ses opérations, l'IMF devrait tenir compte des données internes et externes concernant ses activités et ses systèmes. Elle disposera ainsi de renseignements sur les cybermenaces exploitables et actuels qui lui permettront de prendre de meilleures décisions, puisqu'elle sera en mesure d'anticiper les capacités, les intentions et le *modus operandi* des pirates;

    b. avoir la capacité d'analyser l'information recueillie et d'évaluer la possible incidence sur son cadre de cyberrésilience;

c. avoir recours à de multiples sources de renseignements internes et externes[41], à des analyses de journaux corrélées, à des alertes, aux flux de trafic, ainsi qu'aux comptes rendus de cyberévénements survenus dans d'autres secteurs et d'incidents géopolitiques. Cela permettra à l'IMF de mieux comprendre l'évolution de l'ensemble des menaces et de prendre, en amont, des mesures appropriées pour renforcer ses capacités en matière de cyberrésilience.

3. Pour obtenir des renseignements sur les menaces, l'IMF devrait appartenir ou adhérer à une source de partage d'information ou à un centre d'analyse et de partage d'information sur les cybermenaces et les vulnérabilités. Les renseignements ainsi obtenus devraient comprendre des analyses des tactiques, techniques et procédures utilisées par de véritables pirates informatiques, et de l'information sur les enjeux géopolitiques susceptibles de déclencher des cyberattaques visant toute entité au sein de l'écosystème de l'IMF.

4. L'IMF devrait utiliser les renseignements sur les menaces recueillis auprès de diverses sources, en tenant compte de ses propres caractéristiques opérationnelles et techniques, de manière à :

   a. déterminer la motivation et les capacités des auteurs de menace (y compris leurs tactiques, leurs techniques et leurs procédures), et la mesure dans laquelle l'IMF risque de faire l'objet d'une attaque ciblée de leur part;

   b. réévaluer le risque que les systèmes d'exploitation, les applications et d'autres logiciels présentent des vulnérabilités techniques qui pourraient être exploitées pour attaquer l'IMF;

   c. analyser les incidents de cybersécurité survenus au sein d'autres organisations, y compris les types d'incidents, l'origine et les cibles des attaques, les événements menaçants ayant précédé l'incident et leur fréquence, et déterminer le risque potentiel que représentent ces incidents;

   d. analyser la probabilité d'une attaque de la part de ces auteurs de menace et l'incidence possible d'une telle attaque sur la confidentialité, l'intégrité et la disponibilité des processus opérationnels de l'IMF et sur sa réputation;

   e. analyser l'incidence sur l'écosystème des attaques déjà menées par des auteurs de menace.

5. L'IMF devrait constamment utiliser les renseignements sur les cybermenaces qu'elle a produits pour évaluer et gérer les menaces à la sécurité et les vulnérabilités afin de mettre en œuvre des contrôles de cybersécurité dans ses systèmes et, plus généralement, améliorer son cadre et ses capacités de cyberrésilience en continu.

[41] Par exemple : journaux d'applications, de systèmes et de réseaux; solutions de sécurité comme des coupe-feu et des systèmes de détection des intrusions; fournisseurs de confiance de renseignements sur les menaces; et information accessible au public.

6. L’IMF devrait :

   a. veiller à ce que les renseignements sur les cybermenaces soient mis à la disposition du personnel approprié qui est chargé d’atténuer les cyberrisques de l’IMF sur les plans stratégique, tactique et opérationnel;

   b. intégrer et harmoniser son processus de renseignement sur les cybermenaces avec celui de son centre des opérations de sécurité; utiliser l’information fournie par le centre pour améliorer ses renseignements sur les cybermenaces et, en retour, fournir des renseignements au centre;

   c. se baser sur les renseignements sur les cybermenaces pour concevoir et mettre à jour son programme de tests afin de veiller à ce qu’il soit adapté à l’évolution de l’ensemble des menaces, du *modus operandi* des pirates et des vulnérabilités.

7.3 Partage d'information

Le partage d'information, c'est le fait pour des organisations, des personnes et des technologies d'échanger de l'information de leur propre gré.

7. L'IMF devrait définir :

    a. les objectifs du partage d'information, conformément à ses objectifs opérationnels et à son cadre de cyberrésilience. Ces objectifs devraient prévoir, à tout le moins, la collecte et l'échange rapides, au moment opportun, de renseignements qui pourraient faciliter la détection des cyberattaques, suivie d'une intervention, de la reprise des activités et du rétablissement de ses propres systèmes et de ceux des participants à l'IMF;

    b. la portée du partage d'information, notamment :

        i. les types d'information pouvant être échangés;

        ii. les circonstances où le partage d'information est permis;

        iii. les entités avec qui il est permis et souhaitable de partager de l'information;

    c. comment elle donnera suite à l'information qui lui est fournie (p. ex., en ayant recours au protocole TLP, le *Traffic Light Protocol*).

8. L'IMF devrait établir des règles et ententes de partage d'information et les revoir régulièrement. Elle devrait mettre en place des procédures qui permettent de partager de l'information rapidement et conformément aux objectifs et à la portée établis, tout en respectant ses obligations de protéger les données potentiellement sensibles dont la communication inappropriée pourrait avoir des conséquences néfastes.

9. L'IMF devrait établir et mettre en œuvre avec les employés des protocoles concernant le partage d'information sur les menaces, les vulnérabilités et les cyberincidents, en fonction de leurs rôles et responsabilités.

10. L'IMF devrait participer activement à des groupes et mécanismes existants de partage d'information, dont des groupes intersectoriels, intergouvernementaux et transfrontaliers, afin de recueillir, de diffuser et d'évaluer des renseignements sur les pratiques de cybersécurité, les cybermenaces et les signes précurseurs de ces menaces.

11. Au besoin, une IMF devrait envisager d'échanger de l'information sur son cadre de cyberrésilience avec des parties prenantes de confiance, afin de favoriser la compréhension des approches de protection de systèmes liés qui sont appliquées par les diverses parties. Un tel échange d'information soutiendrait les efforts d'une IMF et de ses partenaires visant à harmoniser leurs mesures de sécurité pour accroître leur cyberrésilience.

12. L'IMF devrait prendre part à l'identification des lacunes des mécanismes actuels de partage d'information et s'efforcer de les combler pour faciliter les interventions à l'échelle de l'écosystème en cas d'incidents de grande ampleur.

13. L'IMF devrait prévoir le partage d'information par l'entremise de canaux de confiance en cas d'incident, de même que la collecte et l'échange rapides, au moment opportun, de renseignements qui pourraient faciliter la détection des cyberattaques, suivie d'une intervention, de la reprise des activités et du rétablissement de ses propres systèmes et de ceux d'entités faisant partie de son écosystème.

8 Apprentissage et évolution

8.1 Préambule

Le cadre de cyberrésilience d'une IMF doit permettre d'assurer la résilience continue de celle-ci dans un contexte où les menaces changent constamment et rapidement. Pour réussir à suivre le rythme, une IMF devrait mettre en œuvre un cadre qui évolue pour s'adapter à des cyberrisques dynamiques par leur nature. Ce cadre devrait aussi permettre à l'IMF d'identifier, d'évaluer et de gérer les menaces informatiques et les vulnérabilités dans le but de mettre en place des mesures appropriées pour protéger ses systèmes. La sensibilisation aux cyberrisques devrait être au cœur de la culture d'une IMF, et celle-ci doit procéder à une réévaluation régulière et fréquente de sa résilience globale, à tous les niveaux.

8.2 Apprentissage continu

Une IMF peut renforcer sa cyberrésilience globale en tirant des leçons de cyberincidents passés, en acquérant de nouvelles connaissances et capacités en continu, et en évaluant ses capacités à l'aide d'indicateurs et de modèles de maturité appropriés.

8.2.1 Leçons tirées des cyberévénements

1. L'IMF devrait identifier et catégoriser les leçons (stratégiques, tactiques et opérationnelles) tirées de cyberincidents réels, qui l'ont touché elle-même ou d'autres entités, pour renforcer sa cyberrésilience.

2. L'IMF devrait assimiler ces grandes leçons tirées de cyberincidents réels ou des résultats de tests auxquels elle-même ou d'autres organisations ont été soumises afin d'améliorer ses capacités d'atténuation des risques, ses interventions, la reprise de ses activités et son rétablissement en cas de cyberincident, ainsi que ses plans d'urgence.

3. L'IMF devrait faire en sorte que les documents de sensibilisation à la cybersécurité soient à la disposition du personnel lorsque des cyberévénements ayant beaucoup de visibilité se produisent ou en cas d'alerte par les autorités réglementaires.

4. L'IMF devrait constamment incorporer les leçons apprises dans la formation, les programmes de sensibilisation et le matériel destinés au personnel, et valider leur

efficacité. Elle devrait également se servir des outils de sensibilisation et de formation créés par le secteur et les autorités, dans la mesure du possible.

8.2.2 Acquisition de connaissances et de capacités

5. L'IMF devrait :

   a. avoir un programme de formation continue sur la cyberrésilience. Cette formation, qui devrait être offerte aux membres du conseil d'administration et de la direction générale au moins une fois par an, devrait traiter des interventions, des cybermenaces courantes et des enjeux émergents[42];

   b. continuellement passer en revue les capacités et les compétences nécessaires ainsi que les besoins de formation pour veiller à ce que le personnel soit préparé à l'évolution de la technologie et des risques. Le personnel devra notamment être en mesure de mettre en œuvre et d'utiliser les technologies de l'information acquises par l'IMF;

   c. explorer de nouvelles capacités technologiques et approches qui pourraient accroître, globalement, la sécurité. Par exemple, certaines organisations envisagent un modèle à vérification systématique parce que leur effectif est nomade et utilise des appareils mobiles, parce qu'elles ont adopté des services infonuagiques, pour contrer les menaces internes et pour éviter les brèches dans le périmètre du réseau[43].

8.2.3 Capacité prédictive

6. Les pratiques de gestion des cyberrisques de l'IMF ne devraient pas se limiter à des mesures réactives, elles devraient aussi comprendre des mesures proactives de protection contre les cyberévénements. L'IMF devrait s'efforcer de développer ses capacités prédictives en recueillant des données de multiples sources internes et externes, en définissant des exigences de base pour les comportements et les activités sur les systèmes, et en analysant les activités qui s'écartent de ces exigences.

8.3 Évaluation comparative de la cyberrésilience

8.3.1 Indicateurs

Un indicateur de la cyberrésilience provient d'un élément du cadre de cyberrésilience ou y est lié.

7. Les indicateurs et les modèles de maturité permettent à une IMF d'évaluer son niveau de cyberrésilience par rapport à un ensemble de critères prédéfinis, qui correspondent généralement à ses objectifs de fiabilité opérationnelle. Pour procéder à cette évaluation comparative, l'IMF doit analyser les résultats d'audits, d'évaluations de la vulnérabilité,

---

[42] Par exemple, l'hameçonnage, le harponnage, le piratage psychologique et la sécurité des appareils mobiles

[43] NIST (2020), *Zero Trust Architecture*, Special Publication 800-207

d'informations de gestion, d'incidents survenus ou évités de justesse, de tests et d'exercices[44], et les corréler avec des renseignements externes et internes. L'utilisation d'indicateurs peut aider l'IMF à identifier les lacunes de son cadre de cyberrésilience afin de les combler, et à accroître systématiquement son niveau de cyberrésilience.

8. L'IMF devrait élaborer, surveiller et analyser des indicateurs permettant d'évaluer l'efficacité de son programme de tests. Elle devrait se servir de l'analyse effectuée pour améliorer encore plus ce programme.

9. L'IMF devrait élaborer une gamme d'indicateurs et d'informations de gestion visant à mesurer et surveiller régulièrement l'efficacité de la mise en œuvre de la stratégie et du cadre de cyberrésilience, ainsi que son évolution au fil du temps. Voici quelques exemples d'informations et d'indicateurs pertinents :

    a. le pourcentage d'employés de l'IMF qui ont suivi une formation sur la cybersécurité;

    b. le pourcentage d'incidents signalés dans le délai prévu pour chaque catégorie d'incident applicable;

    c. le pourcentage de vulnérabilités atténuées dans un délai défini après leur découverte;

    d. des rapports annuels faisant le suivi de l'évolution des indicateurs.

[44] Par exemple, les tests d'intrusion et les tests menés par l'équipe rouge

Annexe A : Glossaire

Ce glossaire recense un ensemble de termes employés dans le présent document, qui sont définis dans les normes du secteur ou dans les publications réglementaires. Une liste complète des sources est publiée à la fin du glossaire. Certains termes normalement formés du préfixe « cyber » ont une portée plus étendue dans le contexte du présent document. C'est pourquoi ce préfixe a parfois été retiré dans le glossaire. Ainsi, on y trouve par exemple les termes « goût du risque » et « tolérance au risque » au lieu de « goût du cyberrisque » et « tolérance au cyberrisque ».

Lorsque la source citée est en anglais seulement, les termes et définitions ont été traduits par la Banque du Canada.

Terme	**Définition**
Actif	Ce qui a une valeur, tangible ou non, et mérite d'être protégé, notamment les personnes, l'information, les infrastructures, les finances et la réputation. Source : cyberlexique du CSF
Actif informationnel	Élément de données, appareil ou autre composante de l'environnement qui appuie les activités liées à l'information. Dans le contexte du présent document, les actifs informationnels comprennent les données, le matériel et les logiciels. Ces actifs ne se limitent pas uniquement à ceux qui appartiennent à l'entité; ils englobent aussi ceux qui sont loués et ceux qui sont utilisés par des fournisseurs de services. Sources : CPIM et OICV
Activité	Ensemble de tâches cohérentes liées à un processus. Source : glossaire du NIST
Activité anormale	Activités qui sortent du cadre des comportements attendus. Source : CPA Canada
Analyse des répercussions sur les opérations (ARO)	Processus consistant à déterminer la criticité des opérations et les besoins connexes en ressources pour assurer la résilience et la continuité des opérations pendant et après une perturbation des activités. L'ARO quantifie les répercussions des perturbations sur la prestation de services, sur les risques liés à celle-ci, ainsi que sur les objectifs de temps de récupération et les objectifs de point de récupération. Ces exigences en matière de rétablissement servent ensuite à élaborer des stratégies, des solutions et des plans. Source : glossaire de Gartner
Approche fondée sur les risques	Approche permettant aux IMF d'identifier, d'évaluer et de comprendre les risques auxquels elles sont exposées, et de prendre des mesures proportionnelles à ces risques. Sources : CPIM et OICV

Terme	Définition
Architecture d'entreprise	Description de l'ensemble des systèmes d'information d'une entreprise : leur configuration, leur intégration, leur interface avec l'environnement externe à la frontière de l'entreprise, leur exploitation pour appuyer la mission de l'entreprise et leur contribution à la posture globale en matière de sécurité de l'entreprise. Source : glossaire du NIST
Attaque du jour zéro	Attaque qui exploite une vulnérabilité matérielle, logicielle ou d'un microprogramme jusque-là inconnue. Source : glossaire du NIST
Attaque par déni de service distribué	Attaque par déni de service menée au moyen de nombreuses sources en simultané. Source : cyberlexique du CSF
Auteur de menace	Personne, groupe ou organisation que l'on soupçonne d'agir en ayant des intentions malveillantes. Source : cyberlexique du CSF
Authenticité	Propriété consistant à être authentique, vérifiable et digne de confiance; confiance en la validité d'une transmission, d'un message ou d'un émetteur. Source : glossaire du NIST
Authentification	Vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif, souvent comme condition préalable à l'autorisation d'accéder aux ressources d'un système d'information. Source : glossaire du NIST
Authentification multifacteur	Processus d'authentification faisant appel à au moins deux facteurs. Parmi ces facteurs, on trouve « ce que l'on sait » (p. ex., mot de passe ou numéro d'identification personnel), « ce que l'on possède » (p. ex., dispositif ou jeton d'identification cryptographique) et « ce que l'on est » (p. ex., renseignements biométriques). Source : glossaire du NIST
Autorisation	Droits d'accès accordés à un utilisateur, programme ou processus. Source : glossaire du CCC
Brèche	Compromission de la sécurité entraînant, de façon fortuite ou illicite, la destruction, la perte, l'altération ou la diffusion non autorisée de données transmises, stockées ou traitées, ou l'accès à de telles données. Source : cyberlexique du CSF
Cadre de cyberrésilience	Politiques, procédures et contrôles instaurés par une IMF pour identifier les sources plausibles de cyberrisques auxquels elle est exposée, les détecter, s'en protéger, intervenir et se rétablir par la suite. Sources : CPIM et OICV

Terme	Définition
Capacité d'investigation numérique	Capacité d'une IMF de maximiser l'utilisation de preuves numériques pour déterminer la nature d'une cyberattaque. Sources : CPIM et OICV
Capacités	Personnes, processus et technologies ayant pour but d'identifier, d'atténuer et de gérer les cyberrisques d'une IMF pour favoriser l'atteinte des objectifs de l'organisation. Source : BCE
Centre des opérations de sécurité	Fonction ou service chargé de surveiller, de détecter et d'isoler les incidents. Sources : CPIM et OICV
Compromission	Violation de la sécurité d'un système d'information. Source : cyberlexique du CSF
Confidentialité	Propriété selon laquelle l'information n'est pas mise à disposition ni divulguée à des personnes, entités, processus ou systèmes non autorisés. Source : cyberlexique du CSF
Configuration de base	Ensemble documenté de spécifications pour un système d'information, ou élément de configuration dans un système, qui a été officiellement revu et approuvé à un moment donné, et qui ne peut être modifié qu'en suivant des procédures de contrôle des modifications. Source : glossaire du NIST
Connaissance de la situation	Aptitude à reconnaître, à traiter et à comprendre les éléments essentiels de l'information grâce à un processus de renseignement sur les cybermenaces qui fournit un niveau de compréhension permettant d'agir de manière à atténuer les conséquences d'un événement potentiellement nuisible. Sources : CPIM et OICV
Contrôle de l'accès	Moyens pour s'assurer que l'accès aux actifs est autorisé et restreint en fonction des exigences opérationnelles et de sécurité. Source : cyberlexique du CSF
Contrôles de sécurité	Exigences générales de sécurité gestionnaires, opérationnelles ou techniques de prescrites pour un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs informatiques connexes. Ces contrôles sont appliqués au moyen de diverses solutions, notamment des produits, des politiques, des pratiques et des procédures de sécurité. Source : glossaire du CCC
Cyber	Qui se rapporte à l'infostructure interconnectée englobant les interactions entre les personnes, les processus, les données et les systèmes d'information, qui est au sein de cette infrastructure ou qui se fait par l'intermédiaire de celle-ci. Source : cyberlexique du CSF

Terme	Définition
Cyberattaque	Exploitation d'une ou de plusieurs failles par un adversaire dans le but de provoquer des répercussions négatives dans l'environnement des technologies de l'information et des communications. Sources : CPIM et OICV
Cyberévénement	Tout événement observable dans un système d'information. Les cyberévénements indiquent parfois l'existence d'un cyberincident. Source : cyberlexique du CSF
Cyberincident	Cyberévénement qui : 1) compromet la cybersécurité d'un système d'information ou l'information que le système traite, stocke ou transmet; ou 2) enfreint les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, que l'incident résulte ou non d'une activité malveillante. Source : cyberlexique du CSF
Cyberrésilience	Capacité d'une IMF à prévoir une cyberattaque, à y résister et à la contenir, et à se rétablir rapidement par la suite. Sources : CPIM et OICV
Cyberrisque	Mesure de l'ampleur d'une menace liée à une circonstance ou à un événement potentiel, et à laquelle une entité est exposée. Cette ampleur est généralement fonction : 1) des répercussions négatives qu'auraient la circonstance ou l'événement s'ils se concrétisaient et 2) de la probabilité qu'ils se produisent (vraisemblance). Source : glossaire du NIST
Cybersécurité	Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information et/ou des systèmes d'information dans le cyberespace. D'autres propriétés, comme l'authenticité, la reddition de comptes, la non-répudiation et la fiabilité, peuvent aussi s'appliquer. Source : cyberlexique du CSF
Cycle de vie d'un système	Ensemble des activités associées à un système, ce qui comprend le lancement, le développement et l'acquisition, la mise en œuvre, l'exploitation et la maintenance et, en fin de compte, l'élimination du système qui entraîne le lancement d'un autre système. Source : glossaire du NIST
Défense en profondeur	Application de nombreuses contre-mesures superposées pour atteindre des objectifs en matière de sécurité. La méthode consiste à mettre en place des couches de technologies de sécurité hétérogènes dans les vecteurs d'attaque courants. Les attaques non détectées par une de ces technologies peuvent donc être contrées par une autre. Source : glossaire du NIST Voir « protection par couches » et « détection en couches »

Terme	Définition
Déni de service	Fait d'empêcher l'accès autorisé à l'information ou aux systèmes d'information, ou de ralentir l'exploitation et les fonctions des systèmes d'information, ce qui entraîne une perte de disponibilité pour les utilisateurs autorisés. Source : cyberlexique du CSF
Détecter (fonction)	Élaborer et mettre en œuvre des activités appropriées pour identifier un cyberévénement. Source : cadre du NIST
Détection en couches	Application, par une IMF, de multiples mesures (couches) de détection (plutôt qu'une seule) pour assurer la cyberrésilience. Voir « protection par couches » et « défense en profondeur ». Source : Banque du Canada
Disponibilité	Propriété consistant à être accessible et utilisable à la demande par une entité autorisée. Source : cyberlexique du CSF
Écosystème	Système ou groupe d'éléments interconnectés entre lesquels il existe des liens et des dépendances. Dans le cas d'une IMF, il peut s'agir des participants, des IMF liées, des fournisseurs de produits et services, et des produits de fournisseurs. Sources : CPIM et OICV
Équipe d'intervention en cas d'incident	Équipe de l'organisation composée de personnes de confiance adéquatement formées pour prendre en charge les incidents pendant leur cycle de vie. Source : cyberlexique du CSF
Équipe rouge	Groupe indépendant qui met à l'épreuve la cyberrésilience d'une organisation pour tester ses mécanismes de protection et en accroître l'efficacité. Une équipe rouge perçoit la cyberrésilience d'une IMF du point de vue de l'adversaire. Sources : CPIM et OICV
Établissement d'une liste blanche	Mise en place, au sein de l'environnement informatique d'une organisation, d'une politique consistant à tout interdire ou à permettre à titre exceptionnel, ainsi que d'un processus d'autorisation clair, concis, rapide et efficace pour ajouter des exceptions lorsque nécessaire afin d'assurer l'accomplissement de la mission. Source : glossaire du NIST
Évaluation des menaces	Processus officiel visant à évaluer la gravité de la menace qui pèse sur un système d'information ou une entreprise et à décrire la nature de la menace. Source : glossaire du NIST
Évaluation des risques	Processus consistant à identifier, à estimer et à prioriser les risques liés à la sécurité de l'information. L'évaluation des risques exige une analyse attentive de l'information relative aux menaces et vulnérabilités afin de déterminer l'ampleur des effets négatifs que pourraient avoir sur une organisation des situations ou incidents particuliers, ainsi que la probabilité que ces situations ou incidents se produisent.

Terme	Définition
	Source : *Managing Information Security Risk*, NIST, p. 6.
Évaluation des vulnérabilités	Examen systématique d'un système d'information ainsi que de ses contrôles et processus pour : déterminer si les mesures de sécurité sont appropriées; cerner les failles de sécurité; obtenir des données permettant de prédire l'efficacité des mesures de sécurité proposées; et confirmer le caractère adéquat de ces mesures après leur mise en œuvre. Source : cyberlexique du CSF
Exploitation	Technique qui consiste à tirer profit d'une vulnérabilité d'un réseau ou d'un système d'information en violation des politiques de sécurité. Source : glossaire du NIST
Gestion de la configuration	Activité consistant à gérer la configuration d'un système d'information tout au long de son cycle de vie. Source : BCE
Gestion de l'identité et de l'accès	Ensemble des personnes, des processus et des technologies qui identifient et gèrent les données servant à authentifier les utilisateurs d'un système d'information et à accorder ou refuser les droits d'accès aux données et aux ressources informatiques. Source : cyberlexique du CSF
Gestion des correctifs	Notification, identification, déploiement, installation et vérification systématiques des révisions de code de systèmes d'exploitation et de logiciels d'application. Ces révisions peuvent prendre la forme de correctifs, de correctifs d'urgence et d'ensembles de modifications provisoires. Source : glossaire du NIST
Gestion des cyberrisques	Processus utilisé par une IMF pour établir un cadre à l'échelle de l'organisation visant à gérer la probabilité d'une cyberattaque et élaborer des stratégies pour en atténuer les répercussions, intervenir, en tirer des leçons et coordonner ses interventions face aux conséquences d'un cyberincident. La gestion des cyberrisques devrait appuyer les processus opérationnels de l'IMF et être intégrée dans son cadre général de gestion des risques. Sources : CPIM et OICV
Goût du risque	Niveau de risque général qu'une entreprise est prête à accepter pour réaliser sa mission et sa vision. Source : adaptation de la définition du glossaire du NIST
Gouvernance (catégorie de la gestion des risques dans le présent document)	Ensemble des relations entre les propriétaires, le conseil d'administration (ou son équivalent), la direction et les autres parties concernées d'une IMF, y compris les participants, les autorités et d'autres parties prenantes (telles que les clients des participants, d'autres IMF interdépendantes et le marché dans son ensemble). La gouvernance énonce les processus par lesquels une IMF définit ses objectifs en matière de

Terme	Définition
	cyberrésilience, détermine par quels moyens elle pourra les réaliser et mesure l'atteinte de ces objectifs. Source : PIMF du CSPR et de l'OICV (adaptation de la note explicative 3.2.1, sous Principe 2 : Gouvernance)
Hameçonnage	Technique utilisée par un malfaiteur qui se fait passer pour une entreprise légitime ou une personne de bonne réputation dans le but d'obtenir des données sensibles (p. ex., un numéro de compte bancaire) par une sollicitation frauduleuse dans un courriel ou un site Web. Source : glossaire du NIST
Identifier (fonction)	Acquérir une compréhension organisationnelle permettant la gestion des risques de cybersécurité auxquels sont exposés les systèmes, les personnes, les actifs, les données et les capacités. Source : cadre du NIST
Indicateur de compromission	Artéfact qui sert à prouver des intrusions potentielles dans un ordinateur ou un réseau hôte. Les indicateurs de compromission permettent aux professionnels de la sécurité de l'information et aux administrateurs de systèmes de détecter des tentatives d'intrusion ou d'autres activités malveillantes. Ils fournissent également des renseignements exploitables sur les menaces qui peuvent être communiqués au sein de l'écosystème. Source : adaptation de la définition de Trend Micro
Infrastructure de marchés financiers (IMF)	Système multilatéral entre les institutions participantes, y compris l'exploitant du système, utilisé pour la compensation, le règlement ou l'enregistrement de paiements, de titres, de dérivés ou d'autres transactions financières. Sources : CPIM et OICV
Intégrité	Propriété d'une information, d'un système d'information ou d'une composante de système qui n'a pas fait l'objet d'une modification ou d'une destruction non autorisée. Sources : CPIM et OICV
Intégrité des données	Propriété qui indique qu'aucune modification non autorisée n'a été apportée aux données depuis leur création, leur transmission ou leur stockage. Source : glossaire du NIST
Intervenir (fonction)	Élaborer et mettre en œuvre les activités appropriées pour réagir à un événement de cybersécurité détecté. Source : glossaire du NIST
Investigation numérique	Application de techniques d'enquête et d'analyse pour recueillir et conserver des éléments de preuve tirés d'un appareil numérique touché par une cyberattaque. Sources : CPIM et OICV
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système d'information à l'insu du propriétaire du système. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires. Source : glossaire du CCC

Terme	Définition
Menace	Circonstance ou événement susceptible de permettre d'exploiter, intentionnellement ou non, une ou plusieurs vulnérabilités des systèmes d'une IMF, ce qui porterait atteinte à la confidentialité, à l'intégrité ou à la disponibilité des systèmes. Sources : CPIM et OICV
Menace interne	Entité ayant des droits d'accès (c'est-à-dire qui fait partie du domaine de sécurité) et qui pourrait nuire à un système d'information ou à une entreprise par la destruction, la divulgation ou la modification de données, ou par un déni de service. Source : glossaire du NIST
Mesures de protection	Mesures prescrites pour satisfaire aux exigences de sécurité (c.-à-d. les exigences de confidentialité, d'intégrité et de disponibilité) indiquées pour un système d'information. Parmi les mesures de protection, on trouve des dispositifs de sécurité, des contraintes de gestion, ainsi que des mesures visant le personnel, l'infrastructure matérielle, les lieux et les appareils. Synonymes : contrôles de sécurité et contre-mesures. Source : glossaire du NIST
Modèle de maturité	Mécanisme permettant d'évaluer les mesures de contrôle de la cyberrésilience ainsi que les méthodes et processus connexes conformément aux pratiques de gestion exemplaires, par rapport à un ensemble de critères externes clairement définis. Sources : CPIM et OICV
Non-répudiation	Capacité de faire la preuve qu'une action ou un événement prétendu a bel et bien eu lieu, et de confirmer sa provenance. Source : cyberlexique du CSF
Objectif de point de récupération	Mesure de la perte de données jugée tolérable pour une organisation. Source : *Élaboration d'un plan de reprise informatique personnalisé*, CCC
Objectif de temps de récupération	Laps de temps visé pour la restauration et le rétablissement des fonctions ou ressources, établi selon le temps d'arrêt et le niveau de service jugés acceptables, en cas de perturbation des opérations. Source : glossaire du DRII
Opérations essentielles	Activité, fonction, processus ou service dont l'interruption, même pendant un court laps de temps, aurait des répercussions marquées sur la poursuite des activités d'une IMF, de ses participants, du marché qu'elle sert et/ou du système financier dans son ensemble. Sources : CPIM et OICV
Perturbation	Événement nuisant à la capacité d'une organisation à effectuer ses opérations essentielles. Sources : CPIM et OICV

Terme	Définition
Piratage psychologique	Terme général désignant une attaque visant à amener les gens (par la ruse) à révéler de l'information délicate ou à faire certaines choses, comme télécharger ou ouvrir un fichier qui semble inoffensif, mais qui est en fait malveillant. Source : glossaire du NIST
Politique	Énoncés, règles ou assertions définissant le comportement adéquat ou attendu d'une entité. À titre d'exemple, une politique d'autorisation peut définir les règles de contrôle d'accès adéquates pour un composant logiciel. Source : glossaire du NIST
Principales normes, lignes directrices et pratiques	Normes, lignes directrices et pratiques exemplaires de gestion des cybermenaces comportant des solutions de cyberrésilience généralement considérées comme les plus efficaces qui soient. Sources : CPIM et OICV
Procédure d'exploitation standard	Série de directives utilisée pour décrire un processus ou une procédure qui déclenche une opération ou une réaction spécifique dans une situation donnée. Source : glossaire du NIST
Processus opérationnel	Série d'activités interdépendantes qui transforment un ou plusieurs types d'intrants en un extrant utile pour les parties prenantes d'une IMF. Un processus opérationnel peut englober plusieurs actifs, notamment des informations, des ressources liées aux technologies de l'information et des communications, du personnel, des moyens logistiques et une structure organisationnelle, qui contribuent directement ou indirectement à la valeur ajoutée du service. Sources : CPIM et OICV
Profil de cyberrisque	Cyberrisque véritablement assumé, mesuré à un moment donné. Sources : CPIM et OICV

Protection par couches	Puisqu'un seul mécanisme défensif pourrait ne pas suffire, une IMF peut recourir à une série de dispositifs différents pour pallier les lacunes d'un mécanisme en particulier et renforcer les autres. Par exemple, les coupe-feu, les systèmes de détection d'intrusions, les scanneurs de maliciels, les procédures d'audit de l'intégrité et les outils de chiffrement de données stockées localement peuvent protéger les actifs informationnels de façon complémentaire et se renforcer mutuellement. Terme équivalent : « défense en profondeur ». Sources : CPIM et OICV
Protéger (fonction)	Élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services et limiter ou atténuer l'impact des cyberincidents. Source : cyberlexique du CSF
Protocole de sécurité IP (IPSec)	Protocole de sécurité de la couche réseau OSI qui permet l'authentification et le chiffrement sur des réseaux IP. Source : glossaire du NIST
Protocole TLS	Protocole d'authentification et de chiffrement largement utilisé par les navigateurs et les serveurs Web. Le trafic HTTP acheminé à l'aide de ce protocole est appelé HTTPS. Source : glossaire du NIST
Registre des risques	Fichier central des risques courants, et des renseignements connexes, pour un domaine d'activité ou une organisation donnés. Les risques courants comprennent les risques acceptés et ceux pour lesquels un plan d'atténuation a été établi. Source : glossaire du NIST
Renseignements sur les cybermenaces	Information sur les menaces qui a été agrégée, transformée, analysée, interprétée ou enrichie pour fournir le contexte nécessaire aux processus décisionnels. Source : définition de *Threat Intelligence* dans le cyberlexique du CSF
Reprendre	Relancer des opérations après un cyberincident. Une IMF devrait recommencer à fournir ses services essentiels dès qu'il lui est possible de le faire de façon sûre, sans entraîner de risques inutiles pour l'ensemble du secteur et sans nuire davantage à la stabilité financière. Le plan d'action devrait prévoir le recours à un site secondaire et être conçu de manière à ce que les systèmes d'information et de communication essentiels puissent reprendre leur fonctionnement dans les deux heures qui suivent une perturbation. Sources : CPIM et OICV
Résilience dès la conception	Intégration de dispositifs de sécurité dans les technologies et les systèmes dès les premières étapes de leur conceptualisation et de leur conception. Sources : CPIM et OICV
Résilience opérationnelle	Capacité d'une IMF : 1) d'assurer le maintien de ses capacités opérationnelles

	essentielles dans des circonstances difficiles ou en période de tensions, même si elles sont réduites ou affaiblies; et 2) de rétablir ses capacités opérationnelles effectives dans un délai compatible avec la prestation de services économiques essentiels. Sources : CPIM et OICV
Restaurer	Ramener un système ou des données à leur état antérieur, ou encore à leur état initial ou normal. Source : Banque du Canada
Rétablir (fonction)	Concevoir et mettre en œuvre des activités et des programmes appropriés pour maintenir des plans de cyberrésilience, notamment de manière à pouvoir restaurer les capacités perturbées à la suite d'un cyberincident. Source : adaptation de la définition du cadre du NIST
Stratégie de cyberrésilience	Principes généraux et plans à moyen terme d'une IMF pour atteindre son objectif de gestion des cyberrisques. Sources : CPIM et OICV
Surface d'attaque	Ensemble des caractéristiques qui composent les grands volets (logiciel, matériel, réseau, processus et facteur humain) d'un système d'information permettant à un pirate d'explorer, de pénétrer, d'attaquer le système ou d'y maintenir une présence et de causer potentiellement des dommages à une IMF. Une surface d'attaque réduite signifie que l'IMF est moins vulnérable et qu'une attaque est moins probable. Toutefois, en réduisant la surface d'attaque, on ne diminue pas nécessairement les dommages qu'une attaque peut infliger. Sources : CPIM et OICV
Système d'information	Ensemble des applications, des services, des ressources informatiques ou des autres composantes servant au traitement de l'information, ce qui englobe l'environnement d'exploitation. Source : cyberlexique du CSF
Tactiques, techniques et procédures (TTP)	Comportement d'un *auteur de menace*. Une tactique est la description la plus générale de ce comportement. Les techniques décrivent plus en détail le comportement dans le contexte d'une tactique. Les procédures dressent un portrait encore plus précis et détaillé du comportement dans le contexte d'une technique. Source : cyberlexique du CSF
Test d'intrusion	Méthode de mise à l'essai selon laquelle des évaluateurs tentent de contourner les dispositifs de sécurité d'un *système d'information* en utilisant toute la documentation disponible (p. ex., information sur la conception du système, code source et manuels) et en travaillant sous certaines contraintes. Source : glossaire du NIST
Test d'intrusion mené par l'équipe rouge	Tentative maîtrisée de compromettre la cyberrésilience d'une entité en simulant les tactiques, les techniques et les

	procédures utilisées par de vrais auteurs de menace. Elle se fonde sur des renseignements ciblés concernant les menaces à l'encontre d'une entité et elle s'axe sur les personnes que l'entité emploie, les processus qu'elle met en œuvre et les technologies qu'elle utilise, avec une connaissance préalable et un impact sur les opérations limités. Source : *G-7 – Éléments fondamentaux pour les tests de pénétration fondés sur les menaces*
Tolérance au risque	Niveau de variation acceptable (selon le goût du risque d'une entité) par rapport à l'atteinte d'un objectif particulier. Au moment de définir le seuil de tolérance au risque, la direction tient compte de l'importance relative de l'objectif connexe et met en adéquation la tolérance au risque avec le goût du risque. Mener ses activités en conformité avec son degré de tolérance au risque permet à l'entité de respecter son goût du risque. Source : adaptation de la définition de *Understanding and Communicating Risk Appetite*, COSO
Vecteur de menace	Chemin d'accès ou trajet qu'emprunte un *auteur de menace* pour accéder à la cible. Source : cyberlexique du CSF
Voix sur IP (VoIP)	Technique qui permet d'intégrer la voix aux données transmises par paquets sur un réseau utilisant le protocole IP, et qui consiste en des protocoles de signalisation et des protocoles multimédias. Sources : glossaire du NIST et GDT
Vulnérabilité	Faiblesse d'un système d'information, de procédures de sécurité informatique, de contrôles internes ou lors de la mise en œuvre d'un système qui pourrait être exploitée ou provoquée par un auteur de menace. Source : glossaire du NIST
Zone démilitarisée	Secteur moins sécurisé d'un réseau, situé entre Internet et les réseaux internes, la zone démilitarisée (aussi appelée « réseau périmétrique ») sert à héberger les services Internet d'une organisation sans l'exposer à des risques d'accès non autorisé à son réseau privé. Source : adaptation de la définition du glossaire du CCC

Sources (le renvoi utilisé dans le texte et le glossaire est indiqué à la fin des sources, entre parenthèses)

Banque centrale européenne (2018). *Cyber resilience oversight expectations for financial market infrastructures*, décembre. Internet: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. (BCE)

Centre canadien pour la cybersécurité (2021). *Élaboration d'un plan de reprise informatique personnalisé*, janvier. Internet : https://cyber.gc.ca/fr/orientation/elaboration-dun-

plan-de-reprise-informatique-personnalise-itsap40004. (Élaboration d'un plan de reprise informatique personnalisé, CCC)

Centre canadien pour la cybersécurité (2021). *Glossaire*. Internet : https://cyber.gc.ca/fr/glossaire. (glossaire du CCC)

Comité sur les paiements et les infrastructures de marché et Organisation internationale des commissions de valeurs (2016). *Guidance on cyber resilience for financial market infrastructures*, juin. Internet : https://www.bis.org/cpmi/publ/d146.pdf. (CPIM et OICV)

Comité sur les systèmes de paiement et de règlement et Organisation internationale des commissions de valeurs (2012). *Principes pour les infrastructures de marchés financiers*, avril. Internet : https://www.bis.org/cpmi/publ/d101_fr.pdf. (PIMF du CSPR et de l'OICV)

Committee of Sponsoring Organizations de la Treadway Commission (2012). *Understanding and Communicating Risk Appetite*, janvier. Internet : https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf. (COSO)

Conseil de stabilité financière (2018). *Cyber Lexicon*, novembre. Internet : https://www.fsb.org/wp-content/uploads/P121118-1.pdf. (cyberlexique du CSF)

CPA Canada (2019). *20 Questions que les administrateurs devraient poser sur la cybersécurité*. Internet: https://www.cpacanada.ca/fr/ressources-en-comptabilite-et-en-affaires/domaines-connexes/technologies-et-gestion-de-linformation/publications/questions-administrateurs-cybersecurite. (CPA Canada)

Disaster Recovery Institute International (2020). *Glossary for Resilience*. Internet: https://drii.org/resources/viewglossary. (glossaire du DRII)

Gartner (2021). *Information Technology Glossary*. Internet : https://www.gartner.com/en/information-technology/glossary. (glossaire de Gartner)

Ministère des Finances Canada (2018). *G-7 – Éléments fondamentaux pour les tests de pénétration fondés sur les menaces,* octobre. Internet : https://www.canada.ca/content/dam/fin/documents/g7/G7-penetration-testing-tests-penetration-fra.pdf. (G-7 – Éléments fondamentaux pour les tests de pénétration fondés sur les menaces)

National Institute of Standards and Technology Information Technology Laboratory Computer Security Resource Centre (2021). *Glossary*, mai. Internet: https://csrc.nist.gov/glossary. (glossaire du NIST)

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, avril. Internet: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. (cadre du NIST)

National Institute of Standards and Technology (2011). *Managing Information Security Risk*, mars. Internet:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf. (Managing Information Security Risk, NIST)

Office québécois de la langue française (2006). *Le grand dictionnaire terminologique*. Internet : http://gdt.oqlf.gouv.qc.ca/. (GDT)

Trend Micro (2021). *Definition*. Internet : https://www.trendmicro.com/vinfo/us/security/definition/a. (Trend Micro)

Unified Compliance Framework (2021). *Compliance Dictionary*. Internet : https://compliancedictionary.com/. (dictionnaire de l'UCF)