SEPTEMBRE 2020

RENFORCER LA RÉSILIENCE DU SECTEUR FINANCIER DANS UN MONDE NUMÉRIQUE :

THÈMES CHOISIS EN LIEN AVEC LA TECHNOLOGIE ET LES RISQUES CONNEXES

DOCUMENT DE TRAVAIL

Bureau du surintendant des institutions financières Canada

BSIF
OSFI

TABLE DES MATIÈRES

RENFORCER LA RÉSILIENCE DU SECTEUR FINANCIER DANS UN MONDE NUMÉRIQUE

THÈMES CHOISIS EN LIEN AVEC LA TECHNOLOGIE ET LES RISQUES CONNEXES

TABLE DES MATIÈRES

RENFORCER LA RÉSILIENCE DU SECTEUR FINANCIER DANS UN MONDE NUMÉRIQUE

THÈMES CHOISIS EN LIEN AVEC LA TECHNOLOGIE ET LES RISQUES CONNEXES

TABLE DES MATIÈRES

RENFORCER LA RÉSILIENCE DU SECTEUR FINANCIER DANS UN MONDE NUMÉRIQUE

THÈMES CHOISIS EN LIEN AVEC LA TECHNOLOGIE ET LES RISQUES CONNEXES

SOMMAIRE

Le BSIF poursuit l'élaboration de ses approches de réglementation et de surveillance en matière de risque lié aux technologies et de risques non financiers connexes.

Le Bureau du surintendant des institutions financières du Canada (BSIF) surveille les institutions financières et les régimes de retraite fédéraux pour déterminer s'ils sont en bonne santé financière et s'ils respectent les exigences qui leur sont applicables. Le *Plan stratégique 2019 2022* du BSIF vise à faire en sorte que les institutions financières fédérales (IFF) et les régimes de retraite soient mieux préparés à déceler les risques non financiers et accroissent leur résilience à l'égard de ces risques avant qu'ils ne nuisent à leur situation financière. C'est pourquoi le BSIF poursuit l'élaboration de ses approches de réglementation et de surveillance en matière de risque lié aux technologies et de risques non financiers connexes. Ce faisant, il est conscient qu'il est impératif d'innover dans le secteur financier au Canada, tout en protégeant les intérêts des déposants, des souscripteurs, des créanciers et des participants des régimes de retraite. Entre-temps, la pandémie de COVID-19 a mis en lumière le besoin d'infrastructures technologiques résilientes, et le secteur et les organismes de réglementation pourront en tirer d'importantes leçons.

Dans le présent document, le BSIF fait part de ses réflexions et de ses derniers travaux, et invite les parties prenantes à communiquer leur avis sur diverses questions entourant la technologie et les risques connexes, notamment :

- le risque et la résilience opérationnels ainsi que la nécessité d'une évaluation globale de l'« architecture » réglementaire d'ensemble du risque lié aux technologies et des autres risques non financiers;
- la compréhension du risque lié aux technologies et du rôle des organismes de réglementation prudentielle dans la gestion des risques liés aux technologies et aux données;
- les principes de base permettant d'orienter l'élaboration de nouvelles consignes réglementaires dans trois axes prioritaires : la cybersécurité, l'analytique avancée et l'écosystème de tiers dans le domaine de la technologie. Ils sont résumés dans le schéma ci-dessous.

PRINCIPES DE BASE DE LA GESTION DU RISQUE LIÉ AUX TECHNOLOGIES, SELON LES AXES PRIORITAIRES

CYBERSÉCURITÉ
- Confidentialité
- Integralité
- Disponibilité

ANALYTIQUE AVANCÉE
- Solidité
- Explicabilité
- Responsabilité

ÉCOSYSTÈME DE TIERS
- Transparence
- Fiabilité
- Substituabilité

Le présent document se veut l'occasion d'engager le dialogue avec les parties prenantes pour déterminer la meilleure façon dont le BSIF peut positionner son cadre de réglementation dans un monde numérique complexe et en rapide évolution. Pour le moment, le BSIF ne fait pas de propositions fermes et entend suivre ce processus de consultation par l'intermédiaire d'un ou de plusieurs autres documents.

Les questions de la consultation sont reprises à l'annexe I, et les parties prenantes sont priées de transmettre leurs commentaires au plus tard le 15 décembre 2020 en écrivant à Tech.Paper@osfi-bsif.gc.ca.

> **La pandémie de COVID-19 a mis en lumière le besoin d'infrastructures technologiques résilientes, et le secteur et les organismes de réglementation pourront en tirer d'importantes leçons.**

1 INTRODUCTION

LE MANDAT DU BSIF

1.1 Le Bureau du surintendant des institutions financières du Canada (BSIF) est un organisme fédéral indépendant qui réglemente et surveille plus de 400 institutions financières fédérales (IFF) et plus de 1 200 régimes de retraite fédéraux pour déterminer s'ils sont en bonne santé financière et s'ils respectent les exigences réglementaires qui leur sont applicables. Il a pour mandat de protéger les déposants, les souscripteurs, les créanciers et les bénéficiaires des régimes de retraite en entreprenant les actions suivantes :

- **ÉLABORER UN CADRE DE RÉGLEMENTATION POUR GÉRER ET ATTÉNUER LES RISQUES;**
- **ÉVALUER LA SÛRETÉ ET LA SOLIDITÉ DES IFF ET DES RÉGIMES DE RETRAITE;**
- **INTERVENIR RAPIDEMENT LORSQUE DES MESURES CORRECTIVES S'IMPOSENT.**

1.2 Le BSIF est un organisme de réglementation prudentielle qui s'attache à contrôler les risques qui peuvent menacer la solvabilité d'une institution financière ou d'un régime de retraite. En bref, il a pour mission d'assurer la « sûreté et la solidité » des entités qu'il réglemente.

L'APPROCHE DE CONSULTATION DU BSIF

1.3 Conformément à ses objectifs stratégiques, le BSIF fait évoluer ses processus de consultation visant les consignes réglementaires afin de promouvoir une plus grande transparence et une participation d'entrée de jeu des principaux intervenants. Le présent document est l'occasion pour le BSIF de faire part de ses réflexions et d'inviter les parties prenantes à lui communiquer leurs impressions sur diverses questions. Cette information permettra ensuite d'orienter les travaux du BSIF en ce qui a trait à l'élaboration de propositions plus concrètes qui seront intégrées à de prochains documents de consultation ou à la révision de lignes directrices.

POURQUOI LE BSIF SE PENCHE-T-IL SUR LA TECHNOLOGIE ET LES RISQUES CONNEXES

SUIVRE LE RYTHME DES PROGRÈS TECHNOLOGIQUES DANS UN ENVIRONNEMENT RÉGLEMENTAIRE COMPLEXE EN CONSTANTE ÉVOLUTION

1.4 Les progrès technologiques rapides et la numérisation[1] continuent de façonner le secteur financier, tant au Canada qu'à l'échelle mondiale. La pandémie de COVID 19 a accéléré encore plus l'automatisation et la transformation numérique au sein des institutions financières, grâce notamment à la technologie et aux données. Les institutions financières, les marchés et les infrastructures sont plus liés que jamais et dépendent étroitement de la résilience de différents acteurs et processus en jeu dans le système financier global. Les entités évoluant au sein de cet écosystème[2] opèrent des transformations, sont de plus en plus nombreuses et axées sur des services que seul un petit petit nombre de fournisseurs importants offrent, et exercent souvent des activités qui ne sont pas visées par le champ traditionnel de la réglementation prudentielle.

1.5 Les technologies financières novatrices, la mondialisation et d'autres facteurs externes ont influé sur les modèles d'affaires et les profils de risque des entreprises depuis l'adoption de l'informatique et d'Internet dans le commerce. Bien que ces forces soient connues, elles génèrent aujourd'hui de nouveaux risques (non financiers) et amplifient les risques (financiers) dans les domaines traditionnels de la surveillance prudentielle.

1 La « numérisation » désigne généralement l'utilisation, par les entreprises, de données et de technologies numériques afin de transformer leurs modèles opérationnels.

2 Système d'interactions et de dépendances entre les entités traditionnelles (réglementées) du secteur financier et les autres entités (non réglementées) avec lesquelles elles font affaire.

MIEUX PRÉPARER LES IFF À DÉCELER LES RISQUES NON FINANCIERS ET ACCROÎTRE LEUR RÉSILIENCE À L'ÉGARD DE CES RISQUES

1.6 Le *Plan stratégique 2019-2022* du BSIF vise à faire en sorte que les IFF[3] soient mieux préparées à déceler les risques dits « non financiers »[4] et accroissent leur résilience à l'égard de ces risques avant qu'ils ne nuisent à leur situation financière. C'est pourquoi il poursuit l'élaboration de ses approches de réglementation et de surveillance en matière de technologie et de risques connexes.

1.7 Les technologies de l'information et des communications (TIC) sous-tendent pratiquement tous les aspects du secteur financier. Bien que la technologie soit un outil essentiel des institutions financières, son usage généralisé pose des risques dans bien des secteurs d'activité. Outre le risque lié aux technologies en lui-même, le présent document traite de plusieurs sujets liés à la technologie, autour de trois axes de risque prioritaires :

- **LA CYBERSÉCURITÉ;**
- **L'ANALYTIQUE AVANCÉE (C.-À-D. LES MODÈLES REPOSANT SUR L'INTELLIGENCE ARTIFICIELLE [IA] ET L'APPRENTISSAGE AUTOMATIQUE [AA]);**
- **L'ÉCOSYSTÈME DE TIERS.**

1.8 Ces trois axes constituent des domaines dans lesquels le BSIF a observé un nombre croissant d'incidents (p. ex., fuites de données, pannes technologiques), de changements dans la gravité des risques, et de risques émergents que les IFF et les organismes de réglementation devraient mieux comprendre (p. ex., l'intelligence artificielle et l'informatique quantique). Pour tous les risques liés aux technologies, le BSIF a déterminé qu'une solide gestion des données et une bonne gouvernance de celles-ci étaient des considérations essentielles.

1.9 Conformément à son approche de réglementation fondée sur des principes[5], le BSIF propose des principes de base pour chaque axe de risque prioritaire, sur lesquels il est possible de définir des attentes plus détaillées permettant de mettre en œuvre une saine gestion des risques.

STRUCTURE DU DOCUMENT DE TRAVAIL

1.10 Le présent document comporte huit sections. La section 2 permet, d'une part, de mieux comprendre le risque lié aux technologies et les liens qui peuvent être faits avec le risque et la résilience opérationnels et, d'autre part, d'établir une corrélation entre le rôle des organismes de réglementation prudentielle et les cadres existants de gestion du risque lié aux TIC. La section 3 donne une vue d'ensemble des principes de base préliminaires, qui sont abordés plus en détail dans les sections suivantes.

1.11 Les sections 4 à 7 portent respectivement sur la cybersécurité, l'analytique avancée, l'écosystème de tiers et les données. Ce dernier sujet constituant le fondement de chacun des thèmes abordés dans le présent document, qui se termine par une discussion distincte sur la gestion du risque lié aux données. Chaque section thématique présente le point de vue du BSIF dans le domaine en question et, le cas échéant, les consignes réglementaires et les travaux de surveillance actuels du BSIF. En contrepartie, le BSIF souhaite recueillir les impressions des parties prenantes qui sont invitées à répondre aux questions posées dans chaque section.

1.12 La section 8 invite les parties prenantes à participer à cette consultation, fournit des instructions, précise les délais de soumission des réponses et donne des renseignements sur les prochaines étapes du processus de consultation.

3 Même si l'on fait référence aux institutions financières (aux banques et aux sociétés d'assurance, par exemple) dans l'ensemble du présent document, les régimes de retraite fédéraux doivent souvent faire face aux mêmes risques et, par conséquent, les thèmes soulevés ici s'appliquent également à ces régimes.

4 Il s'agit des risques qui ne sont pas considérés comme des risques financiers traditionnels (p. ex., le risque opérationnel, le risque lié aux technologies, le risque lié à la culture et à la déontologie).

5 En préconisant des principes plutôt que des règles strictes, le BSIF cherche à faire en sorte que les IFF obtiennent de bons résultats en matière de gestion du risque plutôt qu'elles se conforment à des règles détaillées.

COMPRENDRE LE RISQUE LIÉ AUX TECHNOLOGIES

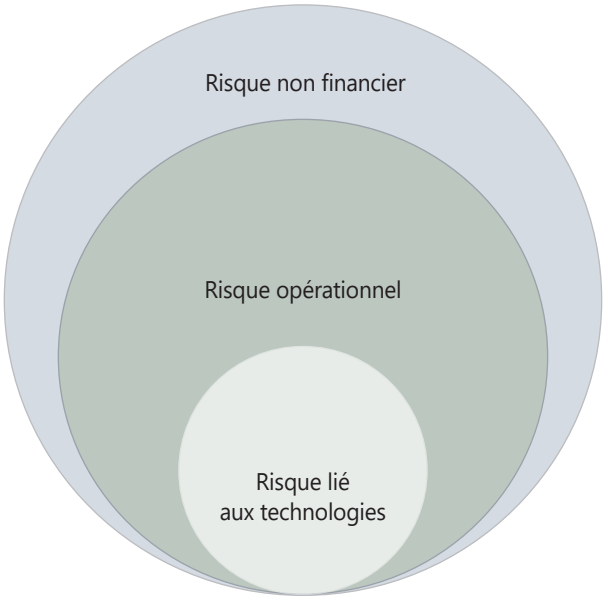
HARMONISATION AVEC LA GESTION DU RISQUE OPÉRATIONNEL

2.1 Nombre d'institutions financières et d'organismes de réglementation évaluent le risque lié aux technologies dans un cadre plus large de gestion du risque opérationnel (GRO), ce qui cadre avec les consignes établies par les organismes internationaux de normalisation[6] et l'expérience du BSIF en matière de surveillance, et tire parti des structures, processus, politiques et procédures en place au sein des IFF.

2.2 La ligne directrice E-21 du BSIF (*Gestion du risque opérationnel*) traite des attentes et des principes clés, comme les trois lignes de défense, ainsi que de nombreux outils et processus utilisés par les IFF pour gérer le risque lié aux technologies et les autres risques opérationnels, notamment les taxonomies des risques, la schématisation des processus opérationnels et l'analyse de scénarios.

LIENS AVEC LA RÉSILIENCE OPÉRATIONNELLE

2.3 De récents travaux à l'échelle mondiale ont permis de déterminer que la résilience opérationnelle est une priorité à l'égard des cadres de GRO et de gestion du risque lié aux technologies établis. En effet, si la GRO semble être axée sur les processus, l'approche adoptée en matière de résilience opérationnelle se concentre davantage sur les résultats découlant d'un événement défavorable particulier. On part du principe que des perturbations opérationnelles *surviendront*, et on encourage les institutions financières à envisager des moyens de réduire l'incidence de ces événements.



2.4 Les autorités, y compris le BSIF, commencent à évaluer les avantages que peut avoir la prise en compte de la résilience opérationnelle et à réévaluer l'adéquation des cadres de GRO en place à cet égard. Le BSIF sait que certaines IFF ont déjà adopté des programmes de résilience opérationnelle qui cadrent avec les programmes actuels de gestion du risque opérationnel ou du risque lié aux technologies.

2.5 Des organismes internationaux de normalisation, comme le Comité de Bâle sur le contrôle bancaire (CBCB) et certaines autorités nationales, s'emploient actuellement à définir des principes et des attentes en matière de résilience opérationnelle.

6 Par exemple, l'Association internationale des contrôleurs d'assurance (AICA) et le Comité de Bâle sur le contrôle bancaire (CBCB).

ÉLABORATION DE POLITIQUES INTERNATIONALES SUR LA RÉSILIENCE OPÉRATIONNELLE

Le 6 août 2020, le groupe de travail sur la résilience opérationnelle du CBCB a publié un document de consultation à l'intention des banques intitulé *Principles for operational resilience* (principes de résilience opérationnelle), dans lequel il définit la *résilience opérationnelle* comme étant la capacité d'une banque à accomplir les activités essentielles en période de perturbation[7]. Le Comité a également publié le document *Revisions to the principles for the sound management of operational risk* (révisions aux principes de saine gestion du risque opérationnel) à des fins de consultation. À titre de membre du CBCB, le BSIF participe à ces travaux et tiendra compte des résultats du processus de consultation.

2.6 La résilience opérationnelle n'est pas un concept « nouveau » pour les IFF ou les surveillants. Dans les évaluations effectuées par le personnel de surveillance du BSIF en matière de GRO, on s'attend habituellement à ce que les IFF soient en mesure de résister aux perturbations et de s'en remettre, et puissent poursuivre leurs activités essentielles malgré celles-ci. Parallèlement, la gestion traditionnelle du risque lié à la continuité des activités (une autre sous-catégorie du risque opérationnel) ne tient pas suffisamment compte de l'ampleur des liens de dépendance entre les diverses activités. De plus, elle ne va pas assez loin dans l'instauration d'une culture selon laquelle les entreprises doivent partir du principe que des perturbations se produiront, et se préparer et s'adapter en conséquence.

2.7 Une culture organisationnelle saine est une condition préalable au renforcement de la résilience opérationnelle. Dans une perspective de résilience, on s'appuie sur les capacités de l'ensemble de la GRO, y compris la gestion du risque lié aux technologies, ainsi que sur la culture organisationnelle, afin de veiller à ce que les institutions soient en mesure de résister à d'importantes perturbations opérationnelles.

RÉSILIENCE OPÉRATIONNELLE DES INSTITUTIONS FINANCIÈRES CANADIENNES PENDANT LA PANDÉMIE DE COVID-19

Depuis l'éclosion de la pandémie de COVID-19 au début de 2020, les IFF ont mis en œuvre et révisé leur plan de continuité des activités afin d'être en mesure de poursuivre leurs activités essentielles.

Voici les principales adaptations opérationnelles observées à ce jour au sein des IFF :

- **exiger qu'une grande partie du personnel travaille à domicile, même si celui-ci n'était que peu ou pas habitué et équipé pour le télétravail avant la crise;**
- **recenser le personnel essentiel et cerner ses besoins en matière d'accès (p. ex., à distance ou sur place) et établir des plans d'urgence au cas où celui-ci serait incapable de travailler;**
- **fermer temporairement des succursales de détail et offrir des services numériques ou téléphoniques comme solution de rechange;**
- **contrôler les fournisseurs de services tiers (y compris les fournisseurs étrangers) et, dans certains cas, trouver des solutions de rechange dans l'éventualité où ceux-ci ne seraient pas en mesure d'offrir des services essentiels conformément aux normes établies;**
- **préparer et mettre en œuvre des plans de communication sur mesure;**
- **concevoir des plans de « retour au bureau » qui priorisent la sécurité et le bien-être du personnel.**

Si la plupart des IFF n'ont pas subi de perturbation importante de leurs activités essentielles jusqu'ici, il n'en demeure pas moins que de nombreuses leçons peuvent être tirées de la pandémie sur le plan de la résilience opérationnelle et des différents paramètres sur lesquels elle repose. On peut citer notamment la gouvernance, les systèmes et l'infrastructure technologiques, la gestion du risque lié aux tiers, les personnes, la gestion du changement, la gestion de la continuité des activités, la gestion des incidents et les communications.

Le BSIF continuera d'évaluer le risque lié aux technologies et les cyberrisques que peut poser l'adoption du télétravail à long terme pour les IFF, et d'intégrer les leçons tirées de la pandémie à ses cadres de réglementation et de surveillance. Il encourage d'ailleurs les parties prenantes qui répondront au questionnaire à inclure les enseignements tirés de la pandémie dans leurs commentaires.

7 Bien que les travaux du Groupe de travail sur la résilience opérationnelle soient axés sur les institutions de dépôts, cette définition pourrait s'appliquer également à d'autres entités réglementées.

REFONTE DE L'« ARCHITECTURE » RÉGLEMENTAIRE DU RISQUE ET DE LA RÉSILIENCE OPÉRATIONNELS

2.8 À l'instar des travaux menés à l'échelle internationale sur la technologie et les risques connexes, le BSIF évalue les avantages que peut avoir le fait de mettre les objectifs de résilience opérationnelle au premier plan. Il estime qu'il est justifié d'adopter une vision globale de la GRO et de la résilience opérationnelle. Des travaux préliminaires ont été entrepris pour étudier comment intégrer la résilience opérationnelle aux cadres de réglementation et de surveillance du BSIF.

2.9 L'importance croissante du risque lié aux technologies et des autres risques non financiers exige un cadre stratégique général qui précise les attentes du BSIF à l'égard de plusieurs axes de risque connexes. Cette architecture devrait par ailleurs permettre de déterminer si différentes approches réglementaires doivent être adoptées pour les différentes sous-catégories du risque opérationnel.

2.10 Par exemple, le rythme rapide auquel sont mis en œuvre des changements technologiques exige des approches plus adaptatives et plus agiles pour communiquer les tendances et les saines pratiques en matière de risque lié aux technologies et de cyberrisque. Dans cette optique, le BSIF a créé de nouveaux outils de surveillance pour compléter les consignes réglementaires dans ce domaine. Ces outils sont abordés à la section 4.

DÉFINITION DU RISQUE LIÉ AUX TECHNOLOGIES

2.11 De manière générale, la technologie joue deux rôles importants. Premièrement, elle *facilite* la bonne marche des activités. Elle permet aux institutions financières de créer de la valeur opérationnelle, d'améliorer l'efficacité de leurs activités et de gérer efficacement le risque. Par conséquent, le fait de ne pas profiter pleinement de la technologie peut représenter un manque à gagner pour les institutions. Le fait de ne pas s'adapter à la technologie ou de ne pas investir à cet égard peut également entraîner des perturbations opérationnelles (p. ex., ralentissement prolongé ou interruption des principaux systèmes ou services opérationnels). Une mauvaise gestion de la technologie peut aussi entraîner l'échec de la réalisation des objectifs organisationnels, ce qui entraîne des coûts financiers importants.

2.12 Deuxièmement, la technologie *protège* les systèmes et les actifs des institutions. Plus précisément, elle assure la confidentialité, l'intégrité et la disponibilité des systèmes et des données qu'ils contiennent. Lorsque les technologies et les contrôles connexes tombent en panne, les systèmes et les actifs deviennent vulnérables et susceptibles de subir des dommages ou des pertes.

2.13 Il existe de nombreuses définitions du risque lié aux TIC, ou risque lié aux technologies, tant au sein du secteur financier qu'à l'extérieur. Le BSIF est conscient que les IFF peuvent avoir leurs propres définitions et prendre en compte ce risque de différentes façons dans leur fonction de gestion du risque à l'échelle de l'entreprise. Quelles que soient les définitions et l'approche adoptées, il est primordial de tenir compte de l'incidence négative que peut avoir le risque lié aux technologies sur les activités et sur les axes de risque connexes.

2.14 Aux fins des travaux qu'il mène, le BSIF a établi une définition pratique du risque lié aux technologies qui s'appuie sur les pratiques et les consignes existantes, et qui est conforme aux cadres de gestion du risque opérationnel du secteur financier.

Le **risque lié aux technologies** découle de l'inadéquation, de la mauvaise utilisation, de l'interruption ou de la défaillance des systèmes, de l'infrastructure ou des données de technologie de l'information dans la satisfaction des besoins opérationnels.

PORTÉE ET PRINCIPES RÉGISSANT LE RISQUE LIÉ AUX TECHNOLOGIES

2.15 Le risque lié aux technologies comporte différentes sous-catégories dont le cyberrisque, qui concerne la *protection* des systèmes et des biens, mais aussi un éventail de sous-risques liés au rôle de *facilitateur* de la technologie (p. ex., les risques découlant de la configuration, des pannes et de la gestion de projets). Une taxonomie des risques liés aux technologies pourrait donc englober les domaines suivants :

- GESTION DES SERVICES
- GESTION DE L'INFRASTRUCTURE
- GESTION DES APPLICATIONS
- GESTION DE LA SÉCURITÉ ET DE L'ACCÈS
- GESTION DE LA PERFORMANCE ET DE LA CAPACITÉ
- GESTION DE LA CONFIGURATION ET DEVISE DE L'ACTIF
- GESTION DES VERSIONS
- GESTION DES INCIDENTS
- GESTION DE PROJETS ET DU CHANGEMENT
- GESTION DES RH ET DES FINANCES SE RAPPORTANT AUX TIC
- GESTION DE LA DISPONIBILITÉ, DE LA REPRISE ET DE LA CONTINUITÉ

2.16 La gestion du risque lié aux technologies est également guidée par un éventail tout aussi large de principes qui répondent à différents sous-risques. Tel qu'il est expliqué plus en détail à la section 4 du présent document, les principes bien connus que sont la *confidentialité, l'intégrité* et la *disponibilité* servent de fondement aussi bien pour le risque lié aux technologies, en général, que pour la cybersécurité, en particulier. Outre ces principes, les suivants gouvernent couramment la gestion du risque lié aux technologies :

- DROIT D'ACCÈS MINIMAL
- FIABILITÉ
- MAINTENABILITÉ
- FACILITÉ DE MAINTENANCE
- EXTENSIBILITÉ
- TRAÇABILITÉ
- AUDITABILITÉ
- AUTHENTIFICATION
- AUTORISATION
- NON-RÉPUDIATION

Certains de ces principes peuvent être appliqués différemment dans d'autres contextes, comme le principe de *fiabilité* dans la gestion du risque lié aux tiers (section 6). L'émergence de technologies comme l'intelligence artificielle (section 5) pousse le secteur et les organismes de réglementation à repenser et à développer les principes traditionnels pour y inclure, entre autres, l'*explicabilité*.

LE RISQUE LIÉ AUX TECHNOLOGIES RECOUPE PLUSIEURS AUTRES AXES DE RISQUE

2.17 La dépendance à la technologie dans l'ensemble des secteurs d'activité des institutions financières signifie que le risque lié aux technologies peut engendrer ou amplifier d'autres risques opérationnels et financiers. Par exemple, une fuite de données majeure qui touche des millions de consommateurs de produits et services financiers pourrait nuire à la réputation d'une IFF et entraîner des pertes financières attribuables à la perte de clients. De même, des projets de transformation des TIC mal exécutés peuvent causer des pertes financières importantes.

QUESTION 1

Que pensez-vous de la relation entre résilience opérationnelle, GRO et risque lié aux technologies? Comment les institutions devraient-elles intégrer ces concepts à leurs principes de gestion du risque d'entreprise au sens plus large?

QUESTION 2

Les risques émergents liés aux technologies peuvent-ils être gérés efficacement au moyen des outils et principes de GRO existants (p. ex., les trois lignes de défense, l'analyse de scénarios)? Quelles sont les lacunes des principes et outils actuels, et comment devrait-on les combler? Le BSIF devrait-il y adjoindre certaines pratiques exemplaires?

QUESTION 3

Quels facteurs influent sur le degré d'exposition aux pertes financières pouvant découler du risque lié aux technologies?

QUESTION 4

Que pensez-vous de la définition et de la portée du risque lié aux technologies proposées par le BSIF?

CADRES DE GESTION DE LA TECHNOLOGIE ET DES RISQUES CONNEXES

CADRES ACTUELS DE GESTION DU RISQUE LIÉ AUX TIC À L'ÉCHELLE DE L'ENTREPRISE

2.18 Les organismes de normalisation des technologies reconnus à l'échelle internationale[8] ont établi des cadres et des consignes que les entreprises peuvent utiliser pour gérer leurs systèmes et leurs biens de TIC, et ils ont adapté ces cadres au fil du temps en réaction aux changements technologiques et à l'évolution de l'environnement externe.

2.19 Le BSIF n'appuie aucun cadre en particulier et encourage les IFF à utiliser les cadres qui conviennent le mieux à leur contexte opérationnel. Parallèlement, il est important que les cadres choisis tiennent bien compte des risques inhérents auxquels les IFF font face, et qu'une gestion et des contrôles stricts soient en place pour atténuer ces risques.

2.20 À ce jour, le BSIF n'a pas élaboré de consignes réglementaires exhaustives sur la gestion du risque lié aux technologies. Les pratiques internationales varient quant à la portée et à la nature des attentes en matière de gestion de ce type de risque. Si certaines administrations ont élaboré des lignes directrices exhaustives sur le risque lié aux TIC ou aux technologies, d'autres ont mis l'accent sur des sous-éléments importants (p. ex., la cybersécurité). En revanche, d'autres autorités tiennent compte du risque lié aux technologies et d'autres risques dans des cadres plus généraux (p. ex., le risque opérationnel). Le BSIF évalue actuellement dans quelle mesure l'élaboration d'autres consignes réglementaires pourrait être utile pour accroître la résilience des IFF face au risque lié aux technologies.

8 Citons, à titre d'exemple, Organisation internationale de normalisation (ISO), Association des professionnels de la vérification et du contrôle des systèmes d'information (ISACA) et National Institute of Standards and Technology (NIST).

SURVEILLANCE DU RISQUE LIÉ AUX TECHNOLOGIES

2.21 Le *Cadre de surveillance* du BSIF aborde la question de la technologie à deux égards. Premièrement, il indique que les surveillants du BSIF tiennent compte de la technologie lorsqu'ils analysent les contextes opérationnels externe et interne d'une IFF pour évaluer les changements dans son profil de risque. Deuxièmement, il reconnaît que les systèmes de sécurité des données et de l'information et des TIC constituent une source de risque opérationnel inhérent.

2.22 Ces dernières années, le BSIF a effectué des travaux de surveillance liés à la technologie dans les domaines suivants, et ce, à l'échelle des sociétés d'assurance et des institutions de dépôt :

- GOUVERNANCE DES TIC ET GESTION DU RISQUE CONNEXE;
- GESTION DES CORRECTIFS;
- ÉVALUATION ET GESTION DES VULNÉRABILITÉS;
- GESTION DE L'ACCÈS;
- GESTION DES INCIDENTS ET INTERVENTION;
- GESTION DES BIENS DE TIC, Y COMPRIS LES DONNÉES ET LES SYSTÈMES EXISTANTS;
- CYBERSÉCURITÉ ET RÉSILIENCE;
- GESTION DU CHANGEMENT ET DE PROJETS LIÉS AUX TIC;
- CONTINUITÉ DES ACTIVITÉS ET REPRISE APRÈS SINISTRE.

2.23 Outre la cybersécurité et la résilience, qui sont traitées à la section 4, les travaux de surveillance du BSIF ont permis de mettre en évidence des domaines communs dans lesquels les IFF peuvent améliorer leurs capacités et leurs pratiques actuelles :

- GESTION DES ACTIFS DE TIC ET TAXONOMIES DES RISQUES LIÉS AUX TECHNOLOGIES;
- HARMONISATION DU CADRE DE GESTION DU RISQUE D'ENTREPRISE AVEC LE CADRE DE GESTION DU RISQUE LIÉ AUX TECHNOLOGIES;
- RECENSEMENT DES RÔLES ET DES RESPONSABILITÉS DES PREMIÈRE ET DEUXIÈME LIGNES DE DÉFENSE, CE QUI COMPREND UN EXAMEN INDÉPENDANT ET UNE ÉVALUATION OBJECTIVE;
- ÉVALUATIONS DU RISQUE LIÉ AUX TECHNOLOGIES, SUIVI ET RAPPORTS Y AFFÉRENTS.

QUESTION 5

Compte tenu des cadres établis à l'heure actuelle par les organismes de normalisation, comment le BSIF peut-il définir des attentes à valeur ajoutée dans ce domaine?

> **L'importance croissante du risque lié aux technologies et des autres risques non financiers exige un cadre stratégique général qui précise les attentes du BSIF à l'égard de plusieurs axes de risque connexes.**

3 PRINCIPES

PRINCIPES SERVANT DE FONDEMENT AUX CONSIGNES RÉGLEMENTAIRES

3.1 Le BSIF privilégie les principes plutôt que les règles et choisit délibérément dans quel cas et à quel moment recourir à des règles ou à des principes dans son cadre de réglementation. Compte tenu du rythme rapide des changements technologiques, les organismes de réglementation ont de plus en plus de difficulté à établir des consignes durables et pertinentes dans ce domaine. D'une part, les principes sont plus susceptibles de demeurer à jour et de conserver les caractéristiques des saines pratiques commerciales, quelles que soient les tendances technologiques dominantes. D'autre part, la réglementation doit toujours venir à l'appui d'une surveillance rigoureuse, et l'approche adoptée à l'égard des consignes doit être adaptée à la nature des risques. Dans certains cas, cela peut nécessiter des attentes plus normatives ou axées sur des règles.

QUESTION 6

L'approche de réglementation du BSIF, qui repose sur des principes, convient-elle à cet axe de risque? Quelles formes de consignes réglementaires favoriseraient le mieux une saine gestion du risque lié aux technologies (cadre général fondé sur des principes, consignes exhaustives sur la gestion du risque lié aux technologies, consignes détaillées portant sur des points particuliers, etc.)?

PROPOSITION DE PRINCIPES DANS TROIS AXES DE RISQUE PRIORITAIRES

3.2 D'après les études, les consultations et les travaux de surveillance effectués jusqu'à présent, le BSIF a cerné trois ensembles de principes de base visant la cybersécurité, l'analytique avancée et l'écosystème de tiers. Le BSIF a l'intention d'utiliser ces principes pour établir des attentes réglementaires plus précises dans ces trois domaines. Ces principes sont abordés plus loin en détail.

3.3 Le schéma ci-après résume les principes de base des axes prioritaires, à mi-chemin entre la technologie et les données, afin d'illustrer leur importance relative et leur interrelation. Les sections 2 et 7, qui portent respectivement sur le risque lié aux technologies et sur les données, traitent de ces interrelations.

3.4 Comme point de départ, le BSIF axe ses efforts de réglementation et de surveillance sur les risques inhérents et résiduels (après la mise en place de mesures de contrôle compensatoires) que pose une technologie, plutôt que sur la technologie elle-même. Cette façon de faire est conforme au mandat équilibré du BSIF, avec son *Cadre de surveillance* et avec une approche de réglementation fondée sur des principes qui s'efforce de demeurer pertinente au fil du temps.

PRINCIPES DE BASE DE LA GESTION DU RISQUE LIÉ AUX TECHNOLOGIES, SELON LES AXES PRIORITAIRES

TECHNOLOGIE

Principes de Cybersécurité

- Confidentialité
- Intégrité
- Disponibilité

Principes d'Analytique avancée

- Solidité
- Explicabilité
- Responsabilité

Principes d'Écosystème de tiers

- Transparence
- Fiabilité
- Substituabilité

DONNÉES

Le BSIF se concentre sur les risques inhérents et résiduels que pose la technologie et ne prend jamais partie pour ou contre l'utilisation d'une technologie en particulier.

CYBERSÉCURITÉ

4.1 Le recours généralisé à la technologie pour recueillir, stocker et utiliser des données dans les services financiers s'est accompagné de cyberattaques toujours plus complexes et fréquentes visant les institutions financières et les entités tierces avec lesquelles elles entretiennent des relations d'affaires. Outre les attaques malveillantes, les IFF doivent faire face à une foule d'autres cyberévénements qui pourraient compromettre la sécurité de leurs renseignements, miner la confiance du public ou enfreindre autrement les politiques et procédures internes.

ÉVOLUTION DU RÔLE DU BSIF EN MATIÈRE DE CYBERSÉCURITÉ

4.2 En 2013, le BSIF a publié des *Conseils sur l'auto-évaluation en matière de cybersécurité* qui énoncent les propriétés et les caractéristiques souhaitables des pratiques de cybersécurité. Le BSIF continue d'encourager les IFF à suivre ces conseils pour évaluer leur niveau de préparation et pour élaborer et maintenir des pratiques de cybersécurité efficaces. Ces conseils peuvent également servir à déterminer la solidité des processus de cybersécurité, ainsi que la cyberposture et la cyberrésilience des IFF.

4.3 Bien que cet outil soit utilisé depuis plusieurs années, le BSIF constate encore des lacunes dans bon nombre de politiques, procédures et outils de cybersécurité des IFF. Ces dernières ont plus de possibilités d'améliorer la solidité de leurs programmes globaux de cybersécurité. Par exemple, les autoévaluations des IFF qui étaient encore valides il y a seulement quelques mois peuvent rapidement devenir désuètes dans le contexte de menace actuel.

PRINCIPES DE CYBERSÉCURITÉ

La *confidentialité*, *l'intégrité* et la *disponibilité* sont des principes fondamentaux de la gestion de la technologie et du cyberrisque qui font généralement l'unanimité et qui jettent les bases de plusieurs définitions de la cybersécurité[9] reconnues à l'échelle internationale.

Confidentialité : L'information n'est ni mise à la disposition ni communiquée à des personnes, entités, processus ou systèmes non autorisés. La confidentialité englobe les outils de protection de la vie privée et des renseignements exclusifs.

Intégrité : L'information n'est pas modifiée de manière incorrecte ou supprimée. L'intégrité englobe aussi l'authenticité et la non-répudiation de l'information.

Disponibilité : L'information est accessible et utilisable de façon fiable et en temps opportun.

9 Par exemple, le Cyber Lexicon (lexique de la cybersécurité) du Conseil de stabilité financière définit la cybersécurité comme étant la préservation de la *confidentialité*, de l'*intégrité* et de la *disponibilité* de l'information ou des systèmes d'information dans l'espace cybernétique. En outre, d'autres propriétés, comme l'authenticité, la responsabilité, la non-répudiation et la fiabilité, peuvent aussi intervenir.

4.4 En 2017-2018, le BSIF a effectué un examen de surveillance pansectoriel portant sur la cyberrésilience. Les IFF choisies devaient réagir à un scénario de crise cybernétique grave, mais plausible. Ces travaux ont donné lieu à plusieurs recommandations qui ont été communiquées aux IFF pour améliorer la cyberrésilience[10] dans des domaines comme le recensement, la prévention et la détection des cyberrisques, les mesures d'intervention à l'égard de ce type de risque et les outils de reprise advenant une cyberattaque.

4.5 Le BSIF continuera de faire évoluer son approche d'évaluation des risques liés aux technologies et des cyberrisques auxquels font face les IFF. Cela comprendra des examens pansectoriels, des tests d'intrusion axés sur le renseignement ainsi que des moyens plus rapides de communiquer l'information aux IFF.

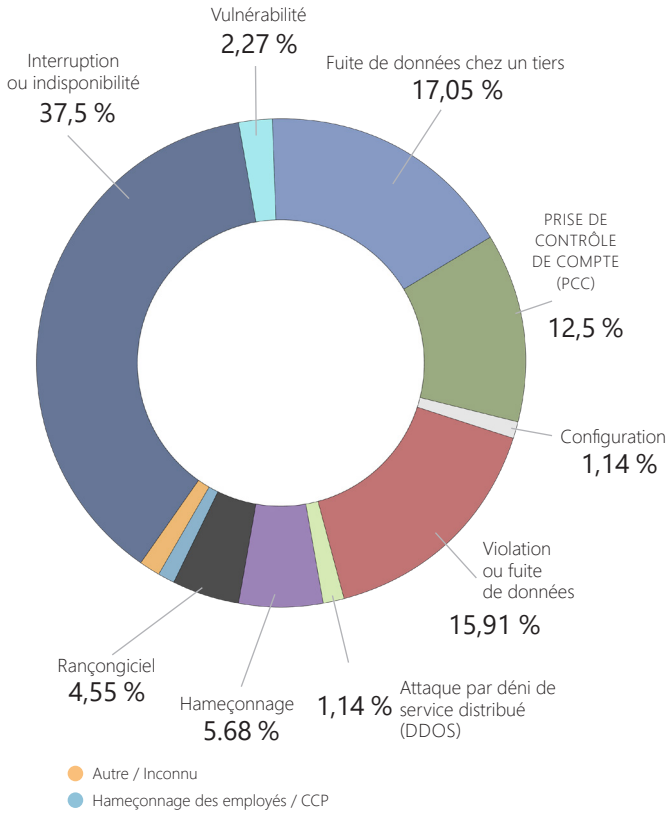
ÉVOLUTION DU RÔLE DU BSIF EN MATIÈRE DE SIGNALEMENT DES INCIDENTS LIÉS À LA TECHNOLOGIE ET DES CYBERINCIDENTS

4.6 En janvier 2019, le BSIF a publié un préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité* qui énonce ses attentes à l'égard du signalement, par les IFF, des incidents liés à la sécurité de la technologie et des cyberincidents qui touchent leurs activités.

4.7 Le BSIF avait cependant commencé à faire le suivi de ces incidents avant de publier le préavis. Le graphique ci-après montre la répartition des incidents majeurs signalés entre la fin d'octobre 2018 et la fin de juin 2020, selon le type d'incident (cause première).

4.8 Outre les fuites de données et les attaques, les pannes liées à la technologie représentent une part importante de l'ensemble des incidents. L'ampleur des incidents fait ressortir l'importance de mettre en place des mesures de gestion des incidents à l'échelle de l'entreprise, lesquelles sont à la fois documentées et reproductibles, afin de pouvoir réagir efficacement aux incidents liés aux TIC et autres cyberincidents.

CYBERINCIDENTS ET INCIDENTS LIÉS À LA TECHNOLOGIE SIGNALÉS AU BSIF (D'OCTOBRE 2018 À JUIN 2020)



NOUVEAUX OUTILS DE SURVEILLANCE TECHNOLOGIQUE ET CYBERNÉTIQUE

4.9 Étant donné que les cyberrisques et les risques liés aux technologies évoluent rapidement, le BSIF doit veiller à ce que ses consignes à l'intention des IFF soient adaptées aux risques émergents. Dans cette optique, le BSIF a créé deux types de bulletins qui viennent s'ajouter à sa Trousse d'outils du surveillant.

4.10 *Les bulletins de renseignements* sont un nouvel outil de surveillance que le BSIF utilise pour aider les institutions à mieux se préparer à faire face aux cyberévénements, et pour mieux protéger le secteur financier dans son ensemble. Le BSIF a distribué son premier bulletin de renseignements à toutes les IFF en août 2019, à la suite d'une grave fuite de données ayant touché le secteur financier canadien. On y trouvait une description générale des tactiques, techniques et procédures qui ont été utilisées pour accéder aux données, ainsi que des moyens de défense, de détection et de prévention pertinents que les IFF devraient prendre en considération.

10 Le Cyber Lexicon (lexique de la cybersécurité) du Conseil de stabilité financière définit la cyberrésilience comme étant la capacité d'une organisation à poursuivre sa mission en anticipant les cybermenaces et autres changements pertinents dans l'environnement et en s'y adaptant, et en résistant aux cyberincidents, en les maîtrisant et en étant capable de reprendre rapidement ses activités après de tels incidents. Elle est donc liée au concept de résilience opérationnelle dont il a été question précédemment, tout en étant distincte.

4.11 En outre, le BSIF a amorcé la publication d'un *Bulletin sur le risque lié aux technologies* à l'intention des IFF, lequel présente des observations sur les questions de cybersécurité et de technologie actuelles. Le BSIF utilise ce bulletin, qui peut facilement être adapté en fonction de l'actualité, pour diffuser de saines pratiques à l'usage du secteur. Le premier portait sur l'authentification multifactorielle. Parmi les sujets qui seront abordés dans les prochains bulletins, on peut citer les suivants : l'interface de programmation ouverte, la chaîne de blocs et l'informatique quantique. Le choix des sujets sera fonction des données des rapports d'incidents des IFF, des nouvelles tendances en matière de technologie et de cyberrisque, et des travaux en cours en matière de surveillance du risque. Le BSIF compte envoyer ces bulletins aux IFF périodiquement, par exemple, tous les trimestres.

4.12 Les nouveaux bulletins constituent une forme de communication prudentielle et visent à compléter les consignes réglementaires du BSIF (lignes directrices, préavis, etc.). À l'instar des autres communications prudentielles, les bulletins sont envoyés en privé aux IFF.

BULLETINS DE RENSEIGNEMENTS	BULLETIN SUR LE RISQUE LIÉ AUX TECHNOLOGIES
▪ METTENT EN ÉVIDENCE LES CYBERMENACES ET VULNÉRABILITÉS ACTUELLES ▪ OUVRENT DES PISTES SUR LES MOYENS DE DÉFENSE APPLICABLES	▪ FOURNIT DES OBSERVATIONS ET DES BONNES PRATIQUES SUR DES QUESTIONS IMPORTANTES EN MATIÈRE DE CYBERSÉCURITÉ ET DE TECHNOLOGIE

Communications prudentielles opportunes qui complètent les consignes réglementaires

AMÉLIORATION DE LA CYBERRÉSILIENCE ET DE LA COOPÉRATION

4.13 Les efforts déployés par le BSIF pour améliorer ses capacités et ses attentes en matière de technologie et de cyberrisque s'inscrivent dans le contexte plus large de la Stratégie nationale de cybersécurité du gouvernement du Canada et s'effectuent en étroite collaboration avec d'autres autorités. Mentionnons à ce titre les travaux du Groupe sur la résilience du secteur financier canadien (GRSFC), qui est chargé d'assurer la coordination d'une procédure d'intervention de l'ensemble du secteur en cas d'incident opérationnel systémique, et d'apporter un soutien aux initiatives permanentes en matière de résilience, comme les exercices réguliers de simulation de crise et d'analyse comparative. Le BSIF collabore aussi régulièrement avec le Centre canadien pour la cybersécurité (CCC). Le CCC transmet ses connaissances sur les menaces, risques et vulnérabilités systémiques, et fournit de l'information sur la connaissance de la situation, des conseils techniques et des consignes.

4.14 Le BSIF continue d'établir de solides partenariats et d'évaluer son rôle et sa contribution à mesure que le cadre législatif du gouvernement en matière de cybersécurité évolue, notamment la place qu'il occupe actuellement dans le signalement des incidents et la communication rapide de l'information sur les menaces aux autorités responsables.

PRÉPARATION À L'INFORMATIQUE QUANTIQUE

4.15 L'informatique quantique est une nouvelle technologie qui applique les principes de la mécanique quantique pour traiter l'information avec plus d'efficacité et de puissance. L'application de l'informatique quantique dans le secteur financier pourrait apporter de nombreux avantages par rapport à l'informatique conventionnelle. Les cas d'utilisation vont des applications de l'IA et de l'AA à la détection de la fraude et à la répartition du portefeuille. L'adoption de cette technologie devrait permettre de réaliser des économies de temps, d'efforts et d'argent.

4.16 L'émergence de l'informatique quantique introduit également de nouveaux risques. Du point de vue de la cybersécurité, la principale menace que pose cette technologie est le risque que la cryptographie à clé publique traditionnelle, sur laquelle reposent de nombreux systèmes d'information, puisse être mise à mal par la vitesse et la puissance de calcul associées à l'informatique quantique. Si les spécialistes ne s'accordent pas encore sur le moment où les menaces liées à l'informatique quantique pourraient se matérialiser, ils conviennent que des procédés de cryptographie pouvant résister aux attaques quantiques devraient rapidement être intégrés aux systèmes, particulièrement ceux qui renferment de l'information de grande valeur conservée pour une longue durée.

4.17 Un ordinateur quantique assez puissant pourrait multiplier les vecteurs d'attaque traditionnels, comme un rançongiciel ou une infiltration dans un réseau pour voler des renseignements privés ou commerciaux de nature délicate. Des malfaiteurs mènent déjà des attaques de type « collecte et déchiffrement », lesquelles consistent à accéder à des données chiffrées, à les copier et à les stocker à des fins de déchiffrement ultérieur, quand celui-ci sera rendu possible par l'utilisation d'un ordinateur quantique puissant.

4.18 À ce jour, les efforts portent sur la mise au point d'une cryptographie capable de résister aux attaques d'un ordinateur quantique. La recherche de pointe sur les techniques de communication par technologies quantiques, telles que la cryptographie quantique (QKD), pourrait apporter des solutions aux défis que posera cette technologie à l'avenir. Jusqu'ici, les bonnes pratiques du secteur se sont axées sur la préparation à l'arrivée de l'informatique quantique (p. ex., capacité d'évaluation du risque quantique, planification des investissements nécessaires à la transition vers une cryptographie pouvant résister aux attaques quantiques).

QUESTION 7

Les consignes actuelles du BSIF sur l'autoévaluation en matière de cybersécurité et le signalement des incidents sont-elles suffisantes compte tenu des risques émergents (p. ex., l'informatique quantique)? Quelles sont les lacunes des consignes actuelles du BSIF, et comment devrait-on les combler? Le BSIF devrait-il y adjoindre certaines pratiques exemplaires?

QUESTION 8

Outre les considérations relatives à la cybersécurité, comment l'informatique quantique devrait-elle être gérée, en tant que risque émergent, dans le contexte de la gestion du cycle de vie des technologies au sens plus large?

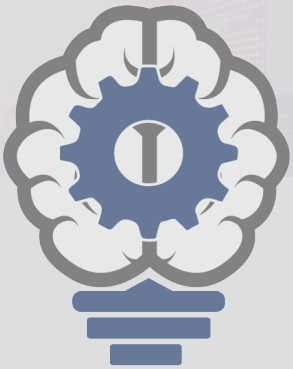
> **Le BSIF continue d'encourager les IFF à suivre ces conseils pour évaluer leur niveau de préparation et pour élaborer et maintenir des pratiques de cybersécurité efficaces.**

ANALYTIQUE AVANCÉE

5.1 La puissance informatique accrue influe sur la capacité à analyser des sources de données plus nombreuses et de plus en plus diverses. L'analytique avancée, y compris l'IA et l'AA, a largement dépassé les outils traditionnels d'informatique décisionnelle et permet une meilleure compréhension du comportement des clients afin de faire des prédictions ou des recommandations aux fins de prises de décisions. Ces progrès technologiques permettent aux institutions financières d'offrir de nouveaux produits et services, de réaliser des gains d'efficience et de réduire leurs coûts.

5.2 Pour les besoins du présent document, le BSIF a adopté les définitions d'IA et d'AA suivantes :

- **INTELLIGENCE ARTIFICIELLE** : MISE EN APPLICATION D'OUTILS INFORMATIQUES POUR ACCOMPLIR DES TÂCHES QUI EXIGENT HABITUELLEMENT DES QUALITÉS COMPLEXES PROPRES À L'HOMME (P. EX., RECONNAISSANCE D'IMAGES ET ANALYSE DU LANGAGE NATUREL AU MOYEN DE L'AA)[11].
- **APPRENTISSAGE AUTOMATIQUE** : SOUS-ENSEMBLE DE L'IA QUI DÉSIGNE UNE TECHNOLOGIE QUI APPREND D'ELLE-MÊME ET S'AMÉLIORE, ET QUI PEUT CRÉER DES MODÈLES PRÉDICTIFS À PARTIR D'EXEMPLES, DE DONNÉES ET DE L'EXPÉRIENCE, AU LIEU DE SUIVRE DES RÈGLES PROGRAMMÉES[12].



PRINCIPES DE L'ANALYTIQUE AVANCÉE

Les études, les analyses et les consultations du BSIF auprès des IFF ont permis de déterminer que la solidité, l'explicabilité et la responsabilité constituaient les principes fondamentaux de la gestion des risques accrus dus à l'analytique avancée, y compris l'IA et l'AA.

Solidité : Qualité d'un modèle reposant sur l'IA ou l'AA qui est exact, fiable, auditable et conçu pour être équitable.

Explicabilité : Aptitude à comprendre et à décrire les rouages d'un modèle, outil ou système reposant sur l'IA ou l'AA, et à expliquer avec rigueur les résultats aux parties concernées.

Responsabilité : Les cadres de gestion du risque intègrent l'IA et l'AA, et des rôles et responsabilités bien définis sont attribués dans l'ensemble de l'institution.

11 Conseil de stabilité financière. « Artificial intelligence and machine learning in financial services », novembre 2017.

12 Conseil stratégique des DPI. « Conception éthique et utilisation des systèmes de décision automatisés », Norme nationale du Canada, CAN/CIOSC 101:2019, octobre 2019.

INCIDENCE DE L'ANALYTIQUE AVANCÉE SUR LE RISQUE DE MODÉLISATION

5.3 Bien que l'analytique avancée offre de nombreux avantages et possibilités, son application fait naître de nouveaux risques en plus d'amplifier certains risques existants. Le BSIF s'intéresse principalement à l'application de l'analytique avancée par les IFF, ce qui comprend les risques liés à l'élaboration, au déploiement et à l'utilisation des modèles reposant sur l'IA et l'AA.

5.4 Le BSIF est conscient qu'il n'est pas toujours facile de déterminer ce qui constitue un « modèle » dans le contexte de l'IA ou de l'AA, et que les IFF peuvent donc classer certaines méthodes d'IA ou d'AA différemment. Toutefois, les principes énoncés dans le présent document peuvent s'appliquer à toute méthode reposant sur l'IA ou l'AA qui est substantiellement semblable à un modèle[13] . Quelle que soit la classification interne, il importe qu'une gouvernance et des contrôles adéquats régissent l'utilisation de l'IA et de l'AA.

5.5 Il n'existe actuellement pas de consignes générales sur le risque de modélisation qui s'applique à tous les secteurs. Les attentes du BSIF en matière de gestion du risque de modélisation sont énoncées dans la ligne directrice B-9, *Saines pratiques de gestion de l'exposition au risque de tremblement de terre,* la ligne directrice E-23, *Gestion du risque de modélisation à l'échelle de l'entreprise dans les institutions de dépôts* et la ligne directrice E-25, *Cadre de surveillance des modèles internes*, qui s'applique aux sociétés d'assurance multirisque. Les commentaires des parties prenantes sur ce document de travail éclaireront les travaux ultérieurs dans ce domaine, y compris la question de savoir s'il y a lieu d'émettre des consignes générales sur le risque de modélisation et, le cas échéant, la méthode à privilégier.

SONDAGE ET RECHERCHE SUR LES MODÈLES REPOSANT SUR L'INTELLIGENCE ARTIFICIELLE ET L'APPRENTISSAGE AUTOMATIQUE

5.6 Afin de mieux comprendre le risque lié aux modèles reposant sur l'IA et l'AA, le BSIF a étudié les mesures prises par les organismes de réglementation prudentielle et les autorités d'autres administrations pour élaborer des consignes réglementaires sur l'utilisation des mégadonnées et de l'analytique avancée par les institutions financières.

5.7 En septembre 2019, le BSIF a sondé un certain nombre d'IFF des secteurs des banques et de l'assurance pour en savoir plus sur leur utilisation de l'IA et de l'AA dans les activités de modélisation. Les résultats du sondage ont fait ressortir un éventail de risques, dont bon nombre peuvent entraîner une diminution de la confiance dans une institution, notamment :

- **MODÈLES** – RISQUE DE MODÉLISATION ACCRU, TRANSPARENCE, EXPLICABILITÉ ET PERFORMANCE;
- **RISQUES CONNEXES** – RISQUE D'ATTEINTE À LA RÉPUTATION, RISQUE OPÉRATIONNEL, CYBERRISQUE ET RISQUE LIÉ AUX TIERS;
- **DONNÉES** – GOUVERNANCE, QUALITÉ, SÉCURITÉ, BIAIS ET PROTECTION DE LA VIE PRIVÉ.

PRINCIPES D'UTILISATION RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE ET DE L'APPRENTISSAGE AUTOMATIQUE

5.8 Le BSIF estime que ses consignes actuelles sur le risque de modélisation demeurent pertinentes, mais qu'elles pourraient être mieux harmonisées et renforcées pour tenir compte du recours accru à l'analytique avancée. Il étudie la possibilité et la manière d'intégrer les principes de solidité, d'explicabilité et de responsabilité à ses cadres de réglementation et de surveillance pour tenir compte des risques émergents découlant de l'IA et de l'AA.

SOLIDITÉ

5.9 Les modèles solides sont exacts, auditables, stables et conçus pour être équitables, ce qui accroît leur fiabilité. De légères différences dans l'architecture ou les données d'entrée d'un modèle peuvent produire des résultats inattendus ou biaisés qui peuvent passer inaperçus dans des systèmes qui ne sont pas solides.

5.10 Compte tenu des risques nouveaux ou accrus découlant de l'utilisation de l'IA et de l'AA, le BSIF a relevé plusieurs domaines où le cadre actuel de gestion du risque de modélisation pourrait évoluer pour renforcer la solidité d'un modèle :

13 Par exemple, certaines IFF considèrent les assistants virtuels comme étant des « modèles », tandis que d'autres ne le font pas.

- **GESTION ET GOUVERNANCE DES DONNÉES** – EN INSISTANT SUR LA QUALITÉ DES DONNÉES DONT DÉPENDENT L'EXACTITUDE ET LA PERFORMANCE DES MODÈLES REPOSANT SUR L'IA OU L'AA (LA SECTION 7 TRAITE PLUS EN DÉTAIL LA QUESTION DES DONNÉES).

- **ÉLABORATION ET VALIDATION DU MODÈLE** – L'EXPLICABILITÉ, LA SIMPLICITÉ ET LA TOLÉRANCE AU RISQUE GUIDENT LE CHOIX DU « BON » MODÈLE. LA FORMATION OU LE RECYCLAGE SUR LES MODÈLES DOIT PORTER SUR LES PRINCIPALES DIFFICULTÉS TECHNIQUES[14] , ET IL EST IMPORTANT DE PROCÉDER À UN SUIVI ET À UNE REVALIDATION CONTINUS APRÈS LA VALIDATION INITIALE ET LE DÉPLOIEMENT.

- **AUDITABILITÉ** – L'ENSEMBLE DU PROCESSUS DE CONCEPTION, DE MISE AU POINT, DE VALIDATION, DE DÉPLOIEMENT ET D'EXPLOITATION DU MODÈLE REPOSANT SUR L'IA OU L'AA DEVRAIT PRODUIRE UNE PISTE D'AUDIT DÉTAILLÉE PERMETTANT DE COMPRENDRE CE QUI A MENÉ AUX DÉCISIONS COMPLEXES EN MATIÈRE D'IA OU D'AA.

- **ÉQUITÉ** – L'ÉQUITÉ DOIT ÊTRE PRISE EN COMPTE TOUT AU LONG DU CYCLE DE VIE DE L'IA OU DE L'AA AFIN DE RÉDUIRE LE RISQUE DE DISCRIMINATION NON VOULUE OU ILLÉGALE. BIEN QU'IL S'AGISSE PRINCIPALEMENT D'UN RISQUE LIÉ À LA DÉONTOLOGIE, UN MANQUE D'ÉQUITÉ, RÉEL OU PRÉSUMÉ, PEUT ACCROÎTRE LE RISQUE D'ATTEINTE À LA RÉPUTATION, LE RISQUE JURIDIQUE ET LE RISQUE DE NON-CONFORMITÉ DES IFF. LES EFFORTS VISANT À COMPRENDRE, À DÉCELER ET À ÉLIMINER DIVERSES FORMES DE BIAIS(P. EX., ÉCHANTILLON, MESURE, ALGORITHME) SONT ÉGALEMENT IMPORTANTS.

EXPLICABILITÉ

5.11 Une approche robuste permettant de rendre le modèle explicable, comme l'indiquent les travaux d'analyse et de surveillance du BSIF, passe par des données de qualité bien gérées, une excellente interprétabilité des algorithmes (p. ex., les liens entre les variables d'entrée et les résultats sont bien compris et documentés), des processus transparents à toutes les étapes du cycle de vie du modèle (p. ex., conception, mise au point, validation, déploiement et exploitation), et la détermination et le respect des limites du modèle.

5.12 Le degré d'explicabilité nécessaire pour gérer adéquatement le risque de modélisation dépend d'un certain nombre de facteurs, dont l'importance relative des conséquences qui pourraient découler des résultats erronés du modèle. Les autres facteurs généralement pris en compte pour déterminer le niveau d'explicabilité sont l'application du modèle et le contexte réglementaire dans lequel il sera utilisé, les attentes des clients, et la mesure dans laquelle la logique décisionnelle pourrait changer[15].

5.13 Dans le secteur de l'assurance, par exemple, dans les administrations où les hausses de primes sont assujetties à une approbation réglementaire, l'explicabilité est une qualité essentielle des modèles de tarification qui reposent sur l'IA ou l'AA. En revanche, l'explicabilité revêt moins d'importance s'il s'agit d'un modèle reposant sur l'IA ou l'AA qui aide l'équipe des ventes à répertorier les souscripteurs qui sont moins susceptibles de renouveler leurs polices.

RESPONSABILITÉ

5.14 Les applications reposant sur l'IA ou l'AA sont complexes et souvent développées et déployées par des équipes pluridisciplinaires. En l'absence d'une chaîne de responsabilité bien définie, les risques et les possibilités d'obtenir des résultats indésirables imprévus sont plus importants (p. ex., mauvaise utilisation des modèles, gouvernance et supervision inadéquates des modèles).

5.15 Les travaux d'analyse et de surveillance du BSIF ont permis de mettre en évidence que l'intégration des processus d'IA et d'AA d'une institution à son cadre de gestion du risque d'entreprise était un élément déterminant de la bonne gestion des risques associés à l'IA et à l'AA. Il s'agit notamment de veiller à ce que l'utilisation des applications reposant sur l'IA ou l'AA soit conforme aux valeurs, aux normes éthiques et à la propension à prendre des risques de l'institution.

14 Il s'agit notamment de la détérioration du modèle, de la stabilité des caractéristiques, du surajustement, des perturbations des données d'entrée, des liens de dépendance entre modèles et du compromis entre précision (exactitude) et rappel (exhaustivité).

15 Association de Genève. « Promoting Responsible Artificial Intelligence in Insurance », janvier 2020.

QUESTION 9
Les principes proposés tiennent-ils adéquatement compte des risques élevés qui découlent de l'utilisation des techniques d'IA et d'AA? Le BSIF devrait-il prendre en considération d'autres principes ou d'autres risques?

QUESTION 10
En ce qui concerne les modèles reposant sur l'IA ou l'AA, prévoyez-vous d'autres difficultés liées à l'auto-évaluation des IFF au regard des principes de responsabilité, d'explicabilité et de solidité (y compris l'auditabilité et l'équité) qui pourraient être intégrées dans une nouvelle version des consignes? Veuillez préciser.

QUESTION 11
Pouvez-vous décrire les niveaux d'explicabilité appropriés pour l'éventail des utilisations possibles de l'IA et de l'AA, ou les complexités techniques sous-jacentes?

QUESTION 12
Que faut-il pour réduire au minimum (ou gérer) les risques d'atteinte à la réputation découlant de l'utilisation de l'IA ou de l'AA?

> **Le BSIF estime que ses consignes actuelles sur le risque de modélisation demeurent pertinentes, mais qu'elles pourraient être mieux harmonisées et renforcées pour tenir compte du recours accru à l'analytique avancée.**

6 L'ÉCOSYSTÈME DE TIERS DANS LE DOMAINE DE LA TECHNOLOGIE

6.1 Les institutions financières comptent sur un large éventail de tiers pour mener leurs activités. Bon nombre de ces relations ont pris la forme d'ententes d'impartition selon lesquelles une entité tierce exerce une activité, une fonction ou un processus opérationnel qui est ou pourrait être exécuté par l'institution elle-même.

6.2 Bien que l'écosystème de tiers englobe beaucoup plus que les seuls accords technologiques, bon nombre des nouveaux débouchés et risques avec lesquels doivent composer les IFF dans ce domaine découlent de la technologie et des données.

MODERNISATION DE L'APPROCHE DU BSIF EN MATIÈRE DE GESTION DU RISQUE LIÉ AUX TIERS

6.3 Les attentes du BSIF à l'égard de l'impartition d'activités, de fonctions et de méthodes commerciales (ligne directrice B-10) ont été définies en 2001 et révisées pour la dernière fois en 2009[17]. De nombreuses ententes avec des tiers ne correspondent pas à la définition d'« entente d'impartition » donnée dans la ligne directrice B-10, y compris certains accords technologiques ou relatifs aux données qui sont de plus en plus courants (p. ex., échange et agrégation de données). En outre, l'évolution des tendances en matière d'ententes technologiques avec des tiers justifie un examen des attentes du BSIF envers les IFF et la prise en considération d'autres principes.

PRINCIPES DE GESTION DU RISQUE LIÉ AUX TIERS DANS LE DOMAINE DE LA TECHNOLOGIE

Au moyen d'analyses et de consultations auprès des IFF, le BSIF a déterminé que la transparence, la fiabilité et la substituabilité étaient des principes fondamentaux de la gestion du risque lié aux tiers dans le domaine de la technologie.

Transparence : Les IFF sont responsables de leurs activités[16] et de leurs fonctions et processus opérationnels, y compris ceux fournis par des tiers, et doivent donc avoir accès aux activités des fournisseurs tiers et à celles de leurs sous-traitants.

Fiabilité : Les IFF doivent être en mesure de recevoir les services fournis par des tiers en permanence au niveau de rendement attendu et de poursuivre leurs activités en cas de perturbation des services.

Substituabilité : Les services de technologie fournis par des tiers peuvent être transférés à un autre fournisseur et offerts par celui-ci.

16 Bien que la ligne directrice B-10 fasse généralement allusion aux « activités », d'autres termes (p. ex., « services ») sont également valables.

17 En 2012, le BSIF a publié une note d'information intitulée Ententes d'impartition des nouveaux services technologiques (p. ex., l'infonuagique) qui affirme que les attentes de la ligne directrice B-10 s'appliquent toujours à ces ententes.

6.4 Parallèlement, certains des principes énoncés dans la ligne directrice B-10 (p. ex., la responsabilité des IFF à l'égard des services impartis, la diligence raisonnable des fournisseurs de services) demeurent pertinents.

6.5 Le BSIF entreprendra un processus de consultation distinct au sujet des attentes énoncées dans la ligne directrice B-10. Les résultats de la présente consultation, les discussions stratégiques à l'échelle internationale et les travaux de surveillance du BSIF éclaireront cette démarche. À noter que le BSIF a entrepris en 2019 une étude sur le risque lié aux tiers qui porte sur un sous-ensemble d'IFF; la gestion du risque lié à l'infonuagique en constitue l'un des points de mire. Vous trouverez les résultats sommaires de cette étude sur le site Web du BSIF.

INFONUAGIQUE

6.6 L'infonuagique est de plus en plus populaire dans le secteur financier au Canada. Comme dans d'autres secteurs, les institutions cherchent à tirer parti d'une sécurité et d'une efficacité accrues, lesquelles sont rendues possibles par le transfert des fonctions de TIC dans le nuage. L'extensibilité des services infonuagiques offre également la flexibilité nécessaire pour répondre aux divers besoins opérationnels des différentes institutions.

6.7 À titre d'organisme de réglementation prudentielle, le BSIF se concentre sur les risques inhérents à l'utilisation de la technologie de tous types, et sur la façon dont les institutions gèrent ces risques. Bien que l'infonuagique offre de nombreux avantages, certaines caractéristiques du marché des fournisseurs de services infonuagiques (FSI) soulèvent d'importantes questions stratégiques pour les organismes de réglementation et les institutions (p. ex., la concentration du marché), dont il est question ci-après.

ADOPTION DE L'INFONUAGIQUE ET GESTION DU RISQUE CONNEXE

6.8 Dans le cadre de ses travaux de surveillance, le BSIF constate que, pour certaines IFF, l'adoption de l'infonuagique a largement dépassé l'étape de la validation de principe pour atteindre un stade où l'intégration du nuage passe avant tout. Toutefois, les normes, la gouvernance et les mécanismes de supervision propres à l'infonuagique en sont encore à leurs balbutiements, et ce, à bien des égards.

6.9 À ce jour, les principaux défis auxquels font face les IFF en matière d'adoption de l'infonuagique sont les suivants : gestion efficace de la migration vers le nuage, pertinence des processus internes de gestion de l'infonuagique, et transférabilité des services infonuagiques à un autre FSI. Le besoin accru de compétences visant l'utilisation et le soutien des services infonuagiques, et l'établissement de contrats juridiques exigeant beaucoup de ressources posent également un défi de taille.

6.10 Les modèles de service les plus courants au sein des IFF sont le logiciel-service (SaaS), suivi de la plateforme-service (PaaS). Le nuage privé est le modèle de déploiement le plus courant, suivi du nuage public et du nuage hybride. Quelle que soit l'ampleur de l'adoption de l'infonuagique ou des modèles de service et de déploiement choisis, la gestion des services infonuagiques est une responsabilité partagée entre les institutions et les FSI. Dans le cadre d'un modèle SaaS, par exemple, les IFF demeurent notamment responsables de la gestion des données, de l'identité et de l'accès.

6.11 D'après les développements et les pratiques du secteur observés à ce jour, les principaux risques liés à l'infonuagique se résument comme suit :

- **MAUVAISE COMPRÉHENSION DES RISQUES ET DES MENACES, QUE VIENT COMPLIQUER LA PARTICIPATION DE NOMBREUX FOURNISSEURS À L'OFFRE GLOBALE DE SERVICES;**
- **ABSENCE DE CONTRÔLES ADÉQUATS SUR LE PLAN DE LA PROTECTION DES DONNÉES ET DE LA GESTION DE L'ACCÈS ET DE LA CONFIGURATION;**
- **ABSENCE DE MESURES DE SUPERVISION ET DE SUIVI APPROPRIÉES EN RAISON DE LA TROP FORTE DÉPENDANCE AU FSI;**
- **ABSENCE DE STRATÉGIE DE SORTIE EN CE QUI CONCERNE LES ACTIVITÉS COMMERCIALES, LES PLANS D'URGENCE ET LA RÉCUPÉRATION DES DONNÉES.**

Les travaux de surveillance du BSIF indiquent que certaines IFF ont déjà établi ou prévoient d'établir des pratiques propres à l'infonuagique visant l'évaluation du risque, les contrôles de sécurité, la supervision et les tests, et les stratégies de sortie.

QUESTIONS STRATÉGIQUES D'ORDRE PLUS GÉNÉRAL CONCERNANT LES FSI EXERÇANT UNE POSITION DOMINANTE

6.12 Le marché mondial des FSI est dominé par plusieurs « Big Tech »[18]. Même si la gamme de services offerts par ces entreprises et la complexité de ces services peuvent être avantageuses pour les IFF, il n'en demeure pas moins qu'ils posent des difficultés singulières. Par exemple, même les plus grandes institutions financières d'importance systémique peuvent avoir moins de possibilités de personnaliser leurs ententes contractuelles avec les FSI qui exercent une position dominante, ce qui peut limiter la transparence et la capacité des IFF d'auditer les pratiques des FSI et d'évaluer les expositions au risque. De plus, même si un FSI offre des modalités contractuelles visant les droits d'accès et d'audit, en réalité, celles-ci peuvent être difficiles à mettre en pratique.

6.13 Par ailleurs, la concentration du marché des FSI et la capacité des IFF à assurer la continuité des fonctions commerciales essentielles en cas de panne ou de défaillance importante chez un FSI exerçant une position dominante posent également problème. Un tel scénario souligne l'importance d'une saine gestion de la continuité des activités et de la résilience opérationnelle.

RELATIONS ENTRE LES IFF ET LES ENTREPRISES DE TECHNOLOGIE FINANCIÈRE

6.14 L'importance des relations qu'entretiennent les IFF avec les entreprises de technologie financière (entreprise de FinTech[19]) tierces ne cesse d'augmenter. Ces entreprises ont un rôle bénéfique à jouer dans le système financier au Canada. En effet, soit elles livrent concurrence aux IFF, soit elles collaborent avec ces dernières pour offrir une gamme de services novateurs aux consommateurs et aux autres entreprises.

6.15 En 2018, le gouvernement du Canada a mis la dernière main aux modifications apportées à la loi régissant les IFF, qui, une fois en vigueur, permettront à ces dernières de participer plus aisément à des offres qui combinent des activités financières et des activités non financières. Elles seront notamment plus à même de réseauter avec les entreprises de technologie financière ou de les acquérir.

6.16 Dans cette perspective, et compte tenu d'autres développements, on s'attend à ce que les relations entre les IFF et les entreprises de technologie financière s'intensifient au fil du temps. Jusqu'ici, le BSIF a constaté que les IFF qui font affaire avec des entreprises de technologie financière s'exposaient à un risque lié aux technologies sur le plan de la cybersécurité et de la gestion des données. Le BSIF continue de suivre les tendances dans ce domaine et de travailler en étroite collaboration avec ses homologues fédéraux pour suivre l'évolution de la situation.

6.17 Le BSIF tient à s'assurer que ses consignes réglementaires à l'intention des IFF restent au fait des tendances actuelles, et offrent un juste équilibre entre la protection des intérêts des déposants, souscripteurs et créanciers, et la possibilité pour les IFF de faire face à la concurrence et de prendre des risques raisonnables.

QUESTION 13

Les principes de gestion du risque lié aux tiers dans le domaine de la technologie proposés tiennent-ils adéquatement compte des risques actuels et émergents? Quels autres principes proposeriez-vous?

QUESTION 14

Comment les consignes actuelles du BSIF sur la gestion du risque lié aux tiers (ligne directrice B-10) peuvent-elles être renforcées compte tenu des tendances actuelles en matière d'ententes avec des tiers dans le domaine de la technologie? Ces ententes méritent-elles d'être soumises à des exigences distinctes de celles s'appliquant aux ententes d'impartition traditionnelles? Dans l'affirmative, veuillez préciser pourquoi. Comment le BSIF devrait-il s'y prendre pour élaborer ces attentes distinctes?

QUESTION 15

Pensez-vous qu'il est justifié d'émettre d'autres consignes réglementaires visant spécifiquement la gestion du risque lié à l'infonuagique? Dans l'affirmative, sur quels éléments celles-ci devraient-elles porter?

QUESTION 16

Quels facteurs de risque le BSIF devrait-il prendre en compte lorsqu'il évalue les relations entre les IFF et les entreprises de technologie financière?

18 Les « BigTech » sont de grandes entreprises spécialisées dans la technologie

19 Les entreprises FinTech ont un modèle d'affaires axé sur les technologies financières novatrices.

DONNÉES

7.1 De grandes quantités de données numériques sont produites et traitées quotidiennement au sein du secteur financier au Canada. Outre la technologie, les données constituent pour les IFF un catalyseur d'affaires essentiel. Les institutions tirent parti des données pour créer de la valeur et gérer efficacement le risque à l'échelle de l'entreprise.

7.2 Bien que la gestion des données ne soit pas une activité nouvelle, la numérisation est venue modifier l'ampleur, la vitesse et l'incidence des risques liés aux données qui interagissent avec de nombreux autres axes de risque, dont la cybersécurité, l'analytique avancée et l'écosystème de tiers. Le vol à grande échelle de données de nature délicate sur les consommateurs de produits et services financiers, par exemple, peut nuire à la réputation d'une IFF et accroître son exposition au risque juridique et au risque de non-conformité.

7.3 L'une des principales leçons tirées de la crise financière mondiale de 2007-2008 est que les institutions financières n'ont pas été en mesure d'agréger rapidement et précisément les expositions au risque et de reconnaître les concentrations de risque dans l'ensemble des secteurs d'activité et des entités de groupe. La crise a révélé dans quelle mesure l'inadéquation des TIC et des infrastructures de données avait contribué à cette défaillance et a mis en évidence la nécessité d'améliorer l'agrégation des données sur les risques et la notification des risques au sein des institutions d'importance systémique[20] . Le maintien de saines pratiques de gestion et de gouvernance des données est une tâche importante et continue pour toutes les institutions financières.

GESTION DU RISQUE TOUT AU LONG DU CYCLE DE VIE DES DONNÉES

7.4 À l'instar du risque lié aux technologies, le BSIF constate que nombre d'IFF intègrent le risque lié aux données à leur cadre de risque d'entreprise. Les risques sont souvent analysés en fonction du cycle de vie des données, qui comprend généralement les activités de création et de saisie, de maintenance et de traitement ainsi que les activités d'utilisation, de publication, de conservation et d'élimination.

7.5 Un cadre de gestion du risque lié aux données solide prévoit divers éléments importants, notamment :

- DES RÔLES ET DES RESPONSABILITÉS BIEN DÉFINIS EN MATIÈRE DE GOUVERNANCE DES DONNÉES, Y COMPRIS UNE ARCHITECTURE QUI PRÉCISE LA PROPRIÉTÉ DES DONNÉES, AINSI QUE LEUR UTILISATION, L'ÉVALUATION DE LEUR QUALITÉ, ET LES RISQUES ET CONTRÔLES CONNEXES;
- DES CONTRÔLES VISANT À RESTREINDRE L'ACCÈS AUX DONNÉES AUX PERSONNES ET AUX FINS AUTORISÉES;
- UN CONTRÔLE DE LA QUALITÉ DES DONNÉES, NOTAMMENT PAR LA VALIDATION ET LE NETTOYAGE DES DONNÉES;
- DES PROCÉDURES DE SUIVI CONTINU DE LA CONFORMITÉ;
- DES PROGRAMMES PÉRIODIQUES DE FORMATION DU PERSONNEL ET DES INITIATIVES DE SENSIBILISATION.

20 CBCB. « Principes aux fins de l'agrégation des données sur les risques et de la notification des risques, » janvier 2013.

7.6 En 2006, le BSIF a publié des notes de mise en œuvre sur la tenue des données par les institutions de dépôts appliquant des approches de mesures avancées pour calculer le niveau de fonds propres requis au regard des expositions au risque de crédit et au risque opérationnel, conformément à la ligne directrice Normes de fonds propres (NFP). Les deux documents énoncent des principes de gestion des données liées au risque de crédit et au risque opérationnel à chaque étape du cycle de vie des données.

FAITS NOUVEAUX INFLUANT SUR LA GESTION DU RISQUE LIÉ AUX DONNÉES

SÉCURITÉ DES DONNÉES ET PROTECTION DE LA VIE PRIVÉE

7.7 En mai 2019, le gouvernement a annoncé deux initiatives importantes. Il a instauré la Charte numérique du Canada en action, qui énonce dix principes visant à servir de guide à la croissance et à l'innovation numérique, y compris la sécurité des données et des renseignements personnels. Il a également annoncé des propositions pour moderniser la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui ont pour but d'accroître le contrôle que les particuliers exercent sur leurs renseignements personnels et leur vie privée, de favoriser l'innovation responsable et de renforcer l'application de la loi et le contrôle, tout en préservant une approche fondée sur des principes.

7.8 La collecte et l'utilisation des données des consommateurs peuvent poser un risque d'atteinte à la réputation ou un risque juridique ou de non-conformité pour les IFF. Dans le secteur de l'assurance, par exemple, l'obtention du consentement à la collecte et à l'utilisation de données de consommateurs qui ne concernent pas l'assurance (p. ex., à partir de produits portables)[21] et la protection des données recueillies peuvent poser problème.

7.9 Les possibles répercussions de l'exposition ou de l'utilisation abusive des données des consommateurs de produits et services financiers fait ressortir l'importance de mettre en place de solides contrôles de la sécurité et de la confidentialité de l'information. Dans le secteur, une pratique exemplaire consiste à intégrer à l'architecture technologique générale de l'entreprise, et d'un bout à l'autre du cycle de vie des données, les principes de sécurité et de protection de la vie privée dès la conception.

CADRES RÉGISSANT LES INTERFACES DE PROGRAMMATION OUVERTES

7.10 De nombreux pays, dont le Canada, ont mis en place des cadres régissant les interfaces de programmation ouvertes, ou songent à le faire[22], afin que les développeurs puissent tirer parti des données financières que les consommateurs consentent à mettre à leur disposition pour créer des applications et des services novateurs. À la suite de la nomination du Comité consultatif sur un système bancaire ouvert, en septembre 2018, le gouvernement a lancé des consultations et publié un document sur les avantages d'un système bancaire ouvert, en janvier 2019.

7.11 En janvier 2020, le gouvernement a annoncé que le Comité consultatif entreprendra la deuxième étape des travaux sur le système bancaire ouvert en se penchant sur la sécurité des données dans les services financiers. Il s'agira notamment de collaborer avec les parties prenantes pour examiner des questions comme la gouvernance, le contrôle des données personnelles par les consommateurs, la protection de la vie privée et la sécurité. Le BSIF surveille de près l'évolution de l'adoption d'interfaces de programmation ouvertes et de ce que cela signifie pour les IFF.

QUESTION 17

Quels risques liés aux données le BSIF devrait-il prendre en compte au moment de modifier son cadre réglementaire?

QUESTION 18

En plus des éléments de saine gestion des données décrits précédemment, quels autres éléments de la gestion des données les consignes réglementaires devraient-elles prendre en considération? Quels critères devraient servir à déterminer l'importance relative des risques liés aux données, et dans quelle mesure cela devrait-il éclairer le niveau de gouvernance à appliquer à la gestion de ces risques?

21 AICA. Issues Paper on the Use of Big Data Analytics in Insurance, février 2020.

22 Les termes connexes comprennent « système bancaire ouvert » et « finances dirigées par les consommateurs ».

8

RENFORCER LA RÉSILIENCE DU SECTEUR FINANCIER DANS UN MONDE NUMÉRIQUE : UN DÉBAT OUVERT

8.1 Les commentaires des parties prenantes sur le présent document de travail et les réponses aux questions contenues dans les sections précédentes sont demandés au plus tard le **15 décembre 2020.** Les réponses et les commentaires doivent être envoyés à Tech.Paper@osfi-bsif.gc.ca.

8.2 En envoyant leurs réponses au BSIF, les parties prenantes acceptent implicitement que le BSIF intègre leurs commentaires de manière anonyme dans une publication sommaire des résultats de la consultation ou dans des documents semblables.

8.3 Le BSIF demande aux parties prenantes d'indiquer clairement les questions auxquelles ils répondent et de faire renvoi, s'il y a lieu, aux paragraphes du présent document. Ils ne sont pas tenus de répondre à toutes les questions.

8.4 Au cours des prochains mois, les réponses et commentaires seront analysés au regard de l'objectif du BSIF, qui est de mieux préparer les IFF à déceler les risques non financiers et à accroître leur résilience à l'égard de ceux-ci avant qu'ils ne nuisent à leur situation financière. Le BSIF pourrait inviter les parties prenantes à participer à d'autres discussions, de façon bilatérale ou dans le cadre d'une tribune multilatérale.

ANNEXE 1

LISTE DES QUESTIONS DE LA CONSULTATION

COMPRENDRE LE RISQUE LIÉ AUX TECHNOLOGIES

QUESTION 1

Que pensez-vous de la relation entre résilience opérationnelle, GRO et risque lié aux technologies? Comment les institutions devraient-elles intégrer ces concepts à leurs principes de gestion du risque d'entreprise au sens plus large?

QUESTION 2

Les risques émergents liés aux technologies peuvent-ils être gérés efficacement au moyen des outils et principes de GRO existants (p. ex., les trois lignes de défense, l'analyse de scénarios)? Quelles sont les lacunes des principes et outils actuels, et comment devrait-on les combler? Le BSIF devrait-il y adjoindre certaines pratiques exemplaires?

QUESTION 3

Quels facteurs influent sur le degré d'exposition aux pertes financières pouvant découler du risque lié aux technologies?

QUESTION 4

Que pensez-vous de la définition et de la portée du risque lié aux technologies proposées par le BSIF?

QUESTION 5

Compte tenu des cadres établis à l'heure actuelle par les organismes de normalisation, comment le BSIF peut-il définir des attentes à valeur ajoutée dans ce domaine?

PRINCIPES

QUESTION 6

L'approche de réglementation du BSIF, qui repose sur des principes, convient-elle à cet axe de risque? Quelles formes de consignes réglementaires favoriseraient le mieux une saine gestion du risque lié aux technologies (cadre général fondé sur des principes, consignes exhaustives sur la gestion du risque lié aux technologies, consignes détaillées portant sur des points particuliers, etc.)?

CYBERSÉCURITÉ

QUESTION 7

Les consignes actuelles du BSIF sur l'autoévaluation en matière de cybersécurité et le signalement des incidents sont-elles suffisantes compte tenu des risques émergents (p. ex., l'informatique quantique)? Quelles sont les lacunes des consignes actuelles du BSIF, et comment devrait-on les combler? Le BSIF devrait-il y adjoindre certaines pratiques exemplaires?

QUESTION 8

Outre les considérations relatives à la cybersécurité, comment l'informatique quantique devrait-elle être gérée, en tant que risque émergent, dans le contexte de la gestion du cycle de vie des technologies au sens plus large?

ANALYTIQUE AVANCÉE

QUESTION 9

Les principes proposés tiennent-ils adéquatement compte des risques élevés qui découlent de l'utilisation des techniques d'IA et d'AA? Le BSIF devrait-il prendre en considération d'autres principes ou d'autres risques?

QUESTION 10

En ce qui concerne les modèles reposant sur l'IA ou l'AA, prévoyez-vous d'autres difficultés liées à l'auto-évaluation des IFF au regard des principes de responsabilité, d'explicabilité et de solidité (y compris l'auditabilité et l'équité) qui pourraient être intégrées dans une nouvelle version des consignes? Veuillez préciser.

QUESTION 11

Pouvez-vous décrire les niveaux d'explicabilité appropriés pour l'éventail des utilisations possibles de l'IA et de l'AA, ou les complexités techniques sous-jacentes?

QUESTION 12

Que faut-il pour réduire au minimum (ou gérer) les risques d'atteinte à la réputation découlant de l'utilisation de l'IA ou de l'AA?

ÉCOSYSTÈME DE TIERS

QUESTION 13

Les principes de gestion du risque lié aux tiers dans le domaine de la technologie proposés tiennent-ils adéquatement compte des risques actuels et émergents? Quels autres principes proposeriez-vous?

QUESTION 14

Comment les consignes actuelles du BSIF sur la gestion du risque lié aux tiers (ligne directrice B-10) peuvent-elles être renforcées compte tenu des tendances actuelles en matière d'ententes avec des tiers dans le domaine de la technologie? Ces ententes méritent-elles d'être soumises à des exigences distinctes de celles s'appliquant aux ententes d'impartition traditionnelles? Dans l'affirmative, veuillez préciser pourquoi. Comment le BSIF devrait-il s'y prendre pour élaborer ces attentes distinctes?

QUESTION 15

Pensez-vous qu'il est justifié d'émettre d'autres consignes réglementaires visant spécifiquement la gestion du risque lié à l'infonuagique? Dans l'affirmative, sur quels éléments celles-ci devraient-elles porter?

QUESTION 16

Quels facteurs de risque le BSIF devrait-il prendre en compte lorsqu'il évalue les relations entre les IFF et les entreprises de technologie financière?

DONNÉES

QUESTION 17

Quels risques liés aux données le BSIF devrait-il prendre en compte au moment de modifier son cadre réglementaire?

QUESTION 18

En plus des éléments de saine gestion des données décrits précédemment, quels autres éléments de la gestion des données les consignes réglementaires devraient-elles prendre en considération? Quels critères devraient servir à déterminer l'importance relative des risques liés aux données, et dans quelle mesure cela devrait-il éclairer le niveau de gouvernance à appliquer à la gestion de ces risques?

ANNEXE 2

GLOSSAIRE ET SIGLES

Le BSIF s'appuie sur des définitions tirées de diverses sources nationales et internationales, notamment le Centre canadien pour la cybersécurité (CCC) et le National Institute of Standards and Technology (NIST). Le Cyber Lexicon (lexique de la cybersécurité) du Conseil de stabilité financière (CSF) est une autre source courante et renvoie à d'autres normes et glossaires généralement reconnus. Le BSIF est conscient que certains termes peuvent être définis et utilisés différemment dans certains contextes.

Attaque par déni de service
Activité visant à rendre un service inutilisable ou à ralentir l'exploitation et les fonctions d'un système donné. (*CCC*)

Attaque par déni de service distribué
Attaque par laquelle une multitude de systèmes compromis visent une même cible. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé et l'interruption des services offerts aux utilisateurs légitimes. (*CCC*)

Cryptographie
Étude des techniques permettant de chiffrer l'information pour la rendre inintelligible ou de rendre lisible une information chiffrée. (*CCC*)

Cyberévénement
Tout fait observable dans un système d'information. Les cyberévénements sont parfois une indication qu'un *cyberincident* a lieu. (*CSF*)

Cyberincident
Cyberévénement qui :
i. met en péril la *cybersécurité* d'un système d'information ou de l'information que celui-ci traite, stocke ou transmet; ou
ii. enfreint les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, qu'il résulte ou non d'une activité malveillante. (*CSF*)

Cybermenace
Circonstance susceptible d'exploiter une ou plusieurs vulnérabilités compromettant la *cybersécurité*. (*CSF*)

Cyberrésilience
Capacité d'une organisation à poursuivre sa mission en anticipant les cybermenaces et autres changements pertinents dans l'environnement et en s'y adaptant, et en résistant aux cyberincidents, en les maîtrisant et en étant capable de reprendre rapidement ses activités après de tels incidents. (*CSF*)

Cyberrisque
Risque de perte financière, de perturbation des opérations ou de dommages découlant de la défaillance des technologies numériques utilisées pour les fonctions d'information ou opérationnelles introduites dans un système [...] par des moyens électroniques par suite de l'accès, de l'utilisation, de la divulgation, de la perturbation, de la modification ou de la destruction non autorisé du système [...]. (*NIST*)

Cybersécurité
Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ou des systèmes d'information dans l'espace cybernétique. En outre, d'autres propriétés comme l'authenticité, la responsabilité, la non-répudiation et la fiabilité, peuvent aussi intervenir. (*CSF*)

Fuite de données
Compromission de la sécurité entraînant, de manière accidentelle ou illégale, la destruction, la perte, la modification, la divulgation non autorisée de données transmises, stockées ou autrement traitées, ou l'accès à celles-ci. (*CSF*)

Technologies de l'information et des communications
Ensemble des technologies de saisie, de stockage, d'extraction, de traitement, d'affichage, de représentation, d'organisation, de gestion, de sécurité, de transfert et d'échange de données et d'information. (*NIST*)

Remarque : Pour les termes tirés des lexiques du NIST et du CSF, les définitions en français sont des traductions libres.

PRINCIPAUX SIGLES UTILISÉS DANS LE PRÉSENT DOCUMENT :

AA	Apprentissage automatique
AICA	Association internationale des contrôleurs d'assurance
API	Interface de programmation
BSIF	Bureau du surintendant des institutions financières
CBCB	Comité de Bâle sur le contrôle bancaire
CCC	Centre canadien pour la cybersécurité
CCP	Compromission de courriels professionnels
CSF	Conseil de stabilité financière
DDoS	Attaque par déni de service distribué
DoS	Attaque par déni de service
FSI	Fournisseur de services infonuagiques
GRO	Gestion du risque opérationnel
GRSFC	Groupe sur la résilience du secteur financier canadien
IA	Intelligence artificielle
IFF	Institution financière fédérale
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
PCC	Prise de contrôle des comptes
QKD	Cryptographie quantique
TIC	Technologies de l'information et des communications