Ligne directrice

Titre	Intégrité et sécurité - Ligne directrice
Catégorie	Saines pratiques commerciales et financières
Date	31 janvier 2024
Secteur	Banques Associations coopératives de crédit Succursales de banques étrangères Succursales de sociétés d'assurance étrangères Sociétés d'assurance vie et de secours mutuels Sociétés des assurances multirisques Sociétés de fiducie et de prêts

Table des matières

A. Aperçu

La confiance du public envers le système financier canadien repose sur l'intégrité et la sécurité des institutions financières. C'est pourquoi la *Loi sur le Bureau du surintendant des institutions financières* renferme une disposition obligeant le BSIF à surveiller les institutions financières pour savoir si leurs politiques et leurs procédures les protègent bien contre les menaces à leur intégrité ou à leur sécurité, y compris contre l'ingérence étrangère. En conséquence, les institutions financières doivent prendre des mesures pour s'assurer qu'elles gèrent bien les risques liés à l'intégrité et à la sécurité en mettant en place de telles politiques et procédures.

A1. Objet

Établir les attentes en matière d'intégrité et de sécurité et souligner celles qui leur correspondent dans les lignes directrices actuelles.

A2. Portée

La ligne directrice précise les attentes, pour toutes les institutions financières fédérales, relatives aux politiques et aux procédures sur l'intégrité et la sécurité. Elle s'applique à toutes les institutions financières fédérales, y compris

les succursales de banques étrangères et de sociétés d'assurance étrangères, dans la mesure permise par les exigences applicables et les obligations légales concernant les activités qu'elles exercent au Canada.Les « succursales de banques étrangères » s'entendent des banques étrangères autorisées à exercer des activités au Canada par l'exploitation d'une succursale en vertu de la partie XII.1 de la *Loi sur les banques*. Les « succursales de sociétés d'assurance étrangères » s'entendent des institutions étrangères qui sont autorisées à garantir au Canada des risques par l'exploitation d'une succursale en vertu de la partie XIII de la *Loi sur les sociétés d'assurances*. Les attentes à l'endroit des succursales sont définies dans la ligne directrice E 4, Entités étrangères exploitant une succursale au Canada.

A3. Champ d'application

La présente ligne directrice s'applique en fonction du risque et dans une mesure proportionnelle à certains facteurs propres à l'institution, dont les suivants :

- la structure de propriété, y compris les relations entre la société mère et ses filiales, ou encore entre le siège social et les succursales, ainsi que les relations avec les parties liées et les actionnaires importants;
- les ententes commerciales, dont les coentreprises et les alliances stratégiques;
- la stratégie et le profil de risque;
- l'étendue, la nature et l'emplacement des activités.

Au moment de mettre en application les attentes de la présente ligne directrice, les institutions financières doivent prendre en considération leur sensibilité à l'influence indue, à l'ingérence étrangère et aux activités malveillantes.

Lorsque les institutions financières rencontrent des obstacles à la réalisation des attentes de la présente ligne directrice (par exemple, des lois ou des attentes réglementaires locales, des restrictions relatives aux locaux loués), elles doivent bien comprendre les risques auxquels elles sont exposées et prendre des mesures d'atténuation adéquates.

A4. Termes clés

- **« activités malveillantes »** s'entend notamment des actions commises dans l'intention de nuire à autrui et comprend le vol, la contrainte, la fraude, la manipulation de l'information ou des perturbations qui sont par ailleurs illégales, malveillantes, clandestines ou trompeuses. Les activités malveillantes peuvent être le fait d'acteurs étrangers ou nationaux et peuvent avoir une incidence sur la sécurité nationale.
- **« dirigeant »** s'entend d'une personne investie de responsabilités en matière de gestion des ressources humaines.
- **« entrepreneur »** désigne une personne de l'extérieur de l'institution financière qui est embauchée pour effectuer des travaux ou rendre des services (par exemple, un travailleur autonome ou une personne embauchée par l'intermédiaire d'une autre entité, notamment un service de placement).
- **« influence indue »** désigne notamment les situations dans lesquelles une personne ou une entité, dans un but malveillant, commet des actions, manifeste des comportements, a recours à la tromperie ou à ses prérogatives pour influer sur des actions, des décisions ou des comportements, et ce, pour son propre compte ou pour le compte d'autrui. L'influence indue peut être le fait d'acteurs étrangers ou nationaux et peut avoir une incidence sur la sécurité nationale.
- **« ingérence étrangère »** désigne des activités qui touchent le Canada ou s'y déroulent, sont préjudiciables à ses intérêts et à sa sécurité, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque, y compris les tentatives secrètes d'influencer, d'intimider, de manipuler, de corrompre ou de discréditer des personnes, des organismes ou des gouvernements, ou d'y interférer, pour favoriser les intérêts d'un État étranger ou d'un acteur non étatique.
- **« intégrité »** désigne des actions, des comportements et des décisions qui respectent la lettre et l'esprit des attentes réglementaires, des lois et des codes de conduite.
- **« responsables »** désigne des personnes, notamment les administrateurs et les membres de la haute direction d'institutions financières au sens de la ligne directrice Gouvernance d'entreprise, ainsi que la direction des succursales de banques et de sociétés d'assurance étrangères en activité au Canada. D'autres personnes peuvent être désignées sous ce nom, selon leurs fonctions ou leurs responsabilités ou selon l'influence qu'elles exercent sur l'institution financière.

- **« sécurité »** s'entend de la protection contre les menaces malveillantes ou non intentionnelles, d'origine interne ou externe, envers :
    - les biens immobiliers, les infrastructures et le personnel (**« menaces physiques »**);
    - les actifs technologiques (**« menaces électroniques »**).

A5. Résultats

1. Des actions, des comportements et des décisions qui respectent la lettre et l'esprit des attentes réglementaires, des lois et des codes de conduite.
2. Des activités, des locaux, des personnes, des actifs technologiques et des données et de l'information qui sont résilients et protégés contre les menaces.

A6. Lignes directrices connexes

Si plusieurs lignes directrices contribuent de manière directe ou indirecte à améliorer l'intégrité et la sécurité des institutions financières, celles qui suivent contribuent de manière directe aux attentes en la matière :

- Gouvernance d'entreprise
- Gestion du risque lié aux tiers (B-10)
- Gestion du risque lié aux technologies et du cyberrisque (B-13)
- Entités étrangères exploitant une succursale au Canada (E-4)
- Gestion de la conformité à la réglementation (E-13)
- Évaluation des antécédents des administrateurs et dirigeants (E-17)
- Gestion du risque opérationnel et résilience opérationnelle (E-21)
- Gestion du risque lié à la culture

1. Lien entre l'intégrité et la sécurité

Bien que l'intégrité et la sécurité soient des notions distinctes et le résultat de pratiques de gestion différentes, les institutions financières peuvent améliorer leur sécurité en agissant de manière intègre. Par exemple, un manque

d'intégrité peut accroître la vulnérabilité d'une institution aux menaces à la sécurité physique ou électronique. Autrement dit, les manquements à la protection de la sécurité découlent souvent du non respect des attentes réglementaires, des lois ou des codes de conduite.

2. Politiques et procédures

Les institutions financières fédérales doivent établir, mettre en œuvre, tenir à jour et respecter des politiques et des procédures adéquates qui les protègent des menaces à leur intégrité ou à leur sécurité, y compris contre l'ingérence étrangère.

Elles doivent revoir leurs politiques et procédures existantes en fonction des attentes de la présente ligne directrice et des lignes directrices connexes. Elles doivent élaborer et tenir à jour des procédures et des systèmes efficaces de suivi, de contrôle et de signalement et déceler et corriger toute lacune ou insuffisance et en faire part à la haute direction. Elles doivent aussi, de façon périodique, évaluer l'efficacité des politiques et procédures et en apporter la preuve, notamment lorsqu'elles détectent de nouvelles menaces ou obtiennent de nouvelles informations.

3. Intégrité

Résultat : Des actions, des comportements et des décisions qui respectent la lettre et l'esprit des attentes réglementaires, des lois et des codes de conduite.

L'intégrité se manifeste par des actions, des comportements et des décisions qui respectent la lettre et l'esprit des attentes réglementaires, des lois et des codes de conduite. Ce sont des personnes œuvrant au sein d'entreprises qui commettent des actions ou négligent de le faire et qui prennent des décisions. Il est possible, par divers moyens, d'augmenter la probabilité qu'elles se comportent avec intégrité, notamment :

1. en veillant à ce qu'elles soient de bonne **moralité**;
2. en promouvant une **culture** qui prône la conformité, l'honnêteté et la responsabilité;

3. en soumettant leurs actions, leurs comportements et leurs décisions à une bonne **gouvernance**;
4. en vérifiant la **concordance** de leurs actions, de leurs comportements et de leurs décisions avec les attentes réglementaires, les lois et les codes de conduite.

L'intégrité est une valeur importante en soi. Le manque d'intégrité peut nuire à la réputation, entraîner de la fraude, causer des problèmes judiciaires et accroître la vulnérabilité à une influence indue, à une ingérence étrangère et à des activités malveillantes. La conformité créative, l'arbitrage réglementaire et d'autres mesures visant à contourner l'esprit des codes de conduite, des attentes réglementaires, des lois ou d'autres normes pertinentes peuvent remettre en question ou compromettre l'intégrité de l'institution financière. Enfin, les risques financiers naissent souvent d'un manque d'intégrité. L'amélioration de l'intégrité réduit donc les risques d'insolvabilité et favorise la sûreté et la stabilité de l'institution financière et, par voie de conséquence, du système financier.

3.1 Moralité

Principe 1 : Les responsables et les dirigeants sont de bonne moralité et font preuve d'intégrité par leurs actions, leurs comportements et leurs décisions.

La façon dont les personnes se comportent dépend d'une certaine mesure de leur moralité. Les responsables et les dirigeants qui se comportent de façon honnête et responsable montrent ainsi des signes de bonne moralité.

En général, plus on grimpe les échelons d'une entreprise, plus on a du pouvoir et de l'influence au sein de celle-ci. Il est donc particulièrement important que les responsables fassent preuve d'intégrité par leurs actions, leurs comportements et leurs décisions.

Consulter la ligne directrice E-17 sur l'évaluation des antécédents des administrateurs et dirigeants.

3.2 Culture

Principe 2 : Une culture qui défend l'intégrité est délibérément façonnée, évaluée et préservée.

La culture influe sur les normes comportementales, ce qui envoie des signaux dans toute l'entreprise sur ce qui est, ou ce qui n'est pas estimé, important et acceptable. Cela a une incidence sur les actions, les comportements et les décisions se rapportant à la gestion, à la conformité, à la prise de risques, à la réponse aux problèmes et à l'apprentissage et à la croissance.

La culture doit être délibérément façonnée, évaluée et préservée. Elle doit aussi concorder avec les attentes comportementales de l'institution financière à l'égard de ce qu'elle considère comme étant acceptable ou inacceptable. Toutefois, il n'y a pas de culture idéale; sa qualité dépend, dans une certaine mesure, du contexte. Néanmoins, toute culture doit être le reflet de normes qui incitent au comportement éthique.

Consulter l'avis intitulé Gestion du risque lié à la culture.

3.3 Gouvernance

Principe 3 : En vertu des structures de gouvernance, les actions, les comportements et les décisions font l'objet d'un examen attentif et d'une remise en question.

La bonne gouvernance passe par un examen attentif et la remise en question des actions, des comportements et des décisions. Une gouvernance efficace permet de gagner la confiance des parties prenantes, y compris les actionnaires, le grand public, les employés et les autorités de réglementation. Elle crée une approche structurée pour gérer les risques importants auxquels fait face l'institution financière.

En conséquence, les décisions importantes au sujet des plans d'affaires, des stratégies, de la propension à prendre des risques, de la culture, des contrôles internes et de la supervision de la haute direction doivent être soumises à une gouvernance efficace.

La supervision de la haute direction comprend l'établissement des responsabilités et la mise en place de mécanismes de reddition des comptes.

Les attentes comportementales doivent être consignées dans des documents normatifs, comme les codes de conduite et les politiques et procédures relatives aux conflits d'intérêts. Il est important de communiquer clairement les attentes aux employés, aux entrepreneurs et aux autres parties prenantes, y compris la façon d'aborder, de résoudre et de communiquer les cas de non respect des consignes.

Les codes de conduite, qui s'appliquent à tous les employés, établissent et communiquent les attentes comportementales et s'accompagnent d'une formation périodique.

Ils doivent faire valoir l'importance :

- de respecter les lois et les attentes réglementaires, les politiques, les procédures et les processus pertinents;
- d'éviter les conflits d'intérêts, comme la corruption et les autres marques d'influence inacceptables;
- de garder une objectivité et d'éviter de faire reposer les processus décisionnels sur des préjugés;
- d'assurer la sécurité et la confidentialité des biens, des communications et de l'information.

Ils doivent traiter de la détection, de la communication, de l'évitement et de la gestion des conflits d'intérêts réels, potentiels ou perçus.

Périodiquement, il conviendrait d'évaluer leur efficacité et de les tenir à jour.

Le respect de ces codes, y compris ceux qui traitent des conflits d'intérêts, doit faire l'objet d'un suivi en fonction du risque, compte tenu des rôles et des fonctions de chacun et de l'exposition potentielle à une influence indue, à une ingérence étrangère et aux activités malveillantes.

Consulter la ligne directrice Gouvernance d'entreprise.

Les succursales de banques étrangères et de sociétés d'assurance étrangères sont invitées à consulter la ligne directrice E-4, Entités étrangères exploitant une succursale au Canada.

3.4 Conformité

Principe 4 : Il existe des mécanismes efficaces permettant de déterminer et de vérifier la conformité aux attentes réglementaires, aux lois et aux codes de conduite.

Il est essentiel d'assurer la gestion du risque de non-conformité afin de maintenir l'intégrité. Il faut veiller à ce que la conformité puisse être vérifiée rapidement et avec exactitude. Il faut aussi veiller à ce que les personnes aient à leur disposition des canaux efficaces pour exprimer leurs inquiétudes quant au respect des attentes réglementaires, des lois et des codes de conduite. La conformité n'est pas seulement l'observation à la lettre de ces attentes, c'est aussi respecter leur esprit compte tenu des conséquences associées pour la réputation de l'entreprise et la confiance du public.

La gestion adéquate du risque de non-conformité passe par l'établissement, dans l'ensemble de l'entreprise, d'un cadre efficace de gestion de la conformité à la réglementation (GCR). Cela doit permettre de valider rapidement et avec exactitude les actions, les comportements et les décisions en fonction des attentes réglementaires, des lois et des codes de conduite applicables, du point de vue de la lettre et de l'esprit.

Le cadre de GCR de l'institution financière doit aussi prévoir des canaux internes efficaces pour qu'on puisse y exprimer ses inquiétudes et des commentaires constructifs, par exemple, par le biais de rapports périodiques et de programmes internes de dénonciation anonyme. La question de l'efficacité de ces canaux internes dépend de l'entreprise en question et de son contexte. Dans tous les cas, les canaux doivent faire l'objet d'un examen et d'une révision périodiques et doivent être communiqués aux employés.

Les canaux externes qui servent à la communication des inquiétudes, comme les programmes de dénonciation gérés par des organismes publics ou des autorités judiciaires, doivent aussi être portés à l'attention des employés.

Consulter la ligne directrice E-13, Gestion de la conformité à la réglementation.

4. Sécurité

Résultat : Des activités, des locaux, des personnes, des actifs technologiques et des données et de l'information qui sont résilients et protégés contre les menaces.

La sécurité comprend la protection contre les menaces malveillantes ou non intentionnelles, d'origine interne ou externe, pour les biens immobiliers, les infrastructures et le personnel (menaces physiques) et pour les actifs technologiques (menaces électroniques). Ces menaces peuvent être le résultat d'une erreur humaine ou la conséquence involontaire d'une activité par ailleurs sans danger. Elles peuvent aussi être le résultat d'une influence indue, d'une ingérence étrangère ou d'autres activités malveillantes.

L'intégrité aide à réduire la vulnérabilité aux menaces. Autrement dit, la sécurité se trouve renforcée du fait que les personnes sont de bonne moralité, que la culture est axée sur la bonne gouvernance et qu'il existe un cadre de GCR adéquat et bien établi.

La résilience opérationnelle et la saine gestion du risque opérationnel permettent elles aussi de réduire la vulnérabilité aux menaces sous-jacente, et plus particulièrement les menaces susceptibles de perturber les activités. Cela dit, certaines menaces, et plus particulièrement celles découlant d'une influence indue, d'une ingérence étrangère ou d'autres activités malveillantes, ne provoquent pas toujours de perturbation. Ces menaces non perturbatrices peuvent nécessiter que l'on adopte d'autres méthodes de détection et de prévention en complément des pratiques courantes touchant à la résilience opérationnelle et à la gestion du risque opérationnel.

On ne peut confier à des tiers la responsabilité de la sécurité. Les services rendus par des tiers doivent être soumis à des mesures adéquates de gestion du risque.

Il faut établir et tenir à jour des politiques et procédures régissant tous les types de menaces, qu'elles soient internes ou externes, et prendre en considération les menaces associées à l'influence indue, à l'ingérence étrangère ou aux activités malveillantes. L'efficacité de ces politiques et procédures doit être évaluée et celles-ci doivent faire l'objet d'un examen et d'une révision périodiques ou continus.

L'environnement de menaces, y compris en ce qui concerne les tiers, doit faire l'objet d'une évaluation et d'un rapport interne au moins tous les ans et s'accompagner de la prise de précautions pour protéger les locaux, les personnes, les actifs technologiques et les données et de l'information.

Consulter la ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle.

4.1 Locaux

Principe 5 : Les locaux sont sûrs et sécurisés et font l'objet d'un contrôle adéquat.

Il faut adopter des normes et des moyens qui régissent le contrôle de l'accès et la surveillance :

- des immeubles et des espaces de bureaux physiques, y compris les biens, les entrepôts et le matériel compris dans ces espaces;
- de tout lieu où peuvent se tenir des discussions ou des travaux de nature délicate.

Il faut effectuer des inspections techniques de sécurité afin de protéger les actifs physiques et numériques, ce qui comprend la recherche périodique d'appareils de surveillance, d'écoute ou de suivi clandestins. L'étendue et la fréquence de ces inspections doivent refléter l'intensité de l'environnement de menaces.

Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque, et la ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle.

4.2 Personnes

Principe 6 : Il faut procéder à une vérification appropriée des antécédents des personnes, et mettre en place des stratégies pour bien gérer le risque.

Il conviendrait d'établir et de tenir à jour des normes et des contrôles de sécurité pour protéger les personnes contre l'influence indue, l'ingérence étrangère et les activités malveillantes. Le fait de bien vérifier les antécédents des personnes permettrait de déceler la vulnérabilité à ces facteurs et faciliterait la préparation de stratégies pour réduire au minimum les risques. Ces normes et contrôles doivent prendre en considération des facteurs comme la position d'autorité, l'ancienneté et l'accès à l'information de nature délicate.

4.2.1 Vérification des antécédents

Il faut soumettre tous les responsables, employés et entrepreneurs à une vérification appropriée des antécédents qui est fondée sur le risque et qui est :

- réalisée avant leur entrée en fonction;
- renouvelée périodiquement;
- revue hors cycle en fonction de certains critères.

Pour être jugées appropriées, les vérifications doivent au moins porter sur l'identité et les antécédents, mais elles doivent aussi souvent porter sur :

- les acquis de formation et les titres professionnels;
- les références personnelles et professionnelles.

En outre, en ce qui concerne les responsables, les employés et les entrepreneurs dont les fonctions comportent plus de risque, il faudrait à tout le moins effectuer :

- une vérification du casier judiciaire;
- une enquête financière (vérification du dossier de crédit).

Le BSIF pourrait exiger de certaines personnes de l'institution financière qu'elles obtiennent une autorisation de sécurité supérieure, selon leurs attributions.

Consulter la ligne directrice E-17 sur l'évaluation des antécédents des administrateurs et dirigeants.

4.3 Actifs technologiques

Principe 7 : Il faut sécuriser les actifs technologiques, déceler leurs faiblesses et les corriger, mettre en place des mécanismes de défense efficaces et recenser les problèmes rapidement et avec exactitude.

Les auteurs de menaces peuvent perturber, détruire, endommager et modifier les actifs technologiques, y accéder ou les utiliser de façon malveillante. Pareils incidents peuvent entraîner une perte financière, entacher la réputation, causer un préjudice aux déposants et aux souscripteurs et avoir incidence sur la sécurité nationale. L'intensité des moyens de défense établis doit être proportionnelle à la vraisemblance des menaces et à la gravité des répercussions de la compromission d'un actif technologique sur l'institution financière, ses employés, ses clients et les autres parties prenantes.

Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque.

4.4 Données et information

Principe 8 : Il faut soumettre les données et l'information à des normes et des contrôles adéquats afin d'assurer leur confidentialité, leur intégrité et leur disponibilité.

Il faut préserver la sécurité des données, y compris leur confidentialité, leur intégrité et leur disponibilité. Les attentes et les moyens de protection doivent être définis et établis tout au long du cycle de vie des données, et des contrôles doivent être en place à l'égard des données au repos, les données en transit et les données utilisées.

Les données structurées et non structurées doivent être bien recensées, classées et protégées en fonction des besoins d'accès du personnel. Au moment de classer les données, il faut prendre en considération leur vulnérabilité aux activités malveillantes, à l'influence indue ou à l'ingérence étrangère. Les normes et les contrôles de protection des données doivent définir les besoins d'accès du personnel aux données de nature délicate, et des mécanismes permettant de détecter et de signaler les accès non autorisés aux données de la part de personnes ou de systèmes doivent être mis en place. L'intensité des moyens de défense établis doit être proportionnelle à la vraisemblance des menaces et à la gravité des répercussions de la compromission des données sur l'institution financière, ses employés, ses clients et les autres parties prenantes.

Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque et la ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle.

4.5 Risques liés aux tiers

Principe 9 : Il faut soumettre les tiers à des évaluations équivalentes et proportionnelles afin de se protéger des menaces.

C'est à l'institution financière qu'appartient la responsabilité d'assurer sa propre sécurité, même en ce qui concerne les activités imparties à des tiers, ce qui comprend les menaces que posent l'influence indue, l'ingérence étrangère ou les activités malveillantes.

Les ententes avec les tiers ne présentent pas toutes le même degré de risque pour la sécurité de l'institution financière. Du point de vue de l'intégrité et de la sécurité, le contrôle préalable des tiers doit être proportionnel au degré d'accès des tiers aux locaux, aux personnes, aux actifs technologiques et aux données et à l'information de l'institution financière.

Sur la base de cette évaluation préliminaire de la proportionnalité, les éléments suivants doivent être évalués avant de faire appel aux services d'un tiers et continuellement par la suite :

- la vraisemblance des menaces pour le tiers;
- la capacité du tiers de répondre aux menaces;
- l'existence et l'adéquation des politiques et des procédures de protection du tiers contre les menaces;
- l'adéquation des processus de vérification des antécédents du tiers.

En ce qui concerne l'ingérence étrangère, l'information suivante au sujet du tiers et de ses sous traitants doit aussi être prise en considération :

- l'emplacement des activités;
- le lieu du siège social;
- les liens entretenus avec des États étrangers;
- la structure de propriété.

Il importe également de veiller à l'objectivité du processus de sélection afin de réduire la possibilité de préjugés, d'une influence indue ou d'une ingérence étrangère.

Consulter la ligne directrice B-10, Gestion du risque lié aux tiers.

4.6 Influence indue, ingérence étrangère et activités malveillantes

Principe 10 : Les menaces découlant de la suspicion d'une influence indue, d'une ingérence étrangère et d'activités malveillantes doivent être détectées et signalées rapidement.

Des mesures doivent être mises en place pour détecter rapidement les menaces et procéder à une enquête minutieuse, et il faut veiller, entre autres choses, à l'imposition de justes limites relativement à l'accès à l'information et assurer la confidentialité, l'indépendance et l'intégrité de l'enquête.

Les institutions financières sont encouragées à communiquer avec les autorités compétentes, notamment le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC), lorsqu'elles ont des motifs raisonnables de croire qu'un incident ou un événement s'est produit et que celui-ci découle d'une influence indue, d'une ingérence étrangère ou d'une activité malveillante. Le BSIF doit être informé immédiatement de ces cas de signalement.

Les incidents et événements détectés, y compris ceux qui ne sont pas jugés assez importants pour être signalés au BSIF ou aux autres autorités, doivent être consignés et répertoriés par l'institution financière en tant qu'information que la direction communique à la haute direction.

Annexe : Résumé des attentes énoncées dans la ligne directrice sur l'intégrité et la sécurité

Résumé des attentes en matière d'intégrité

Principe	Lignes directrices connexes du BSIF	Nouvelle attente	Attentes élargies
1. Les responsables et les dirigeants sont de bonne moralité et font preuve d'intégrité par leurs actions, leurs comportements et leurs décisions.	Ligne directrice E-17, Évaluation des antécédents des administrateurs et dirigeants	Sans objet	Moralité des responsables, comme en témoignent leurs actions, leurs comportements et leurs décisions.
2. Une culture qui défend l'intégrité est délibérément façonnée, évaluée et préservée.	Avis Risques liés à la culture et au comportement	Sans objet	La culture reflète la volonté d'avoir des normes qui encouragent le comportement éthique.
3. En vertu des structures de gouvernance, les actions, les comportements et les décisions font l'objet d'un examen attentif et d'une remise en question.	Ligne directrice Gouvernance d'entreprise Ligne directrice E-4, Entités étrangères exploitant une succursale au Canada	Sans objet	Une gouvernance en vertu de laquelle les actions, les comportements et les décisions sont supervisés. Les attentes comportementales sont énoncées dans des documents normatifs, tels que des codes de conduite et des politiques et procédures de gestion des conflits d'intérêts.
4. Il existe des mécanismes efficaces permettant de déterminer et de vérifier la conformité aux attentes réglementaires, aux lois et aux codes de conduite.	Ligne directrice E-13, Gestion de la conformité à la réglementation	Sans objet	Une conformité par rapport non seulement à la lettre des attentes, mais aussi à leur esprit. Des canaux efficaces, comme les programmes de dénonciation, par où l'on peut signaler les cas de non conformité.

Résumé des attentes en matière de sécurité

Principe	Lignes directrices connexes du BSIF	Nouvelle attente	Attentes élargies
5. Les locaux sont sûrs et sécurisés et font l'objet d'un contrôle adéquat.	Ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque Ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle	Des normes et des contrôles relativement aux immeubles, aux espaces de bureaux et aux entrepôts de fichiers physiques, ainsi que des inspections techniques de sécurité.	Sans objet
6. Il faut procéder à une vérification appropriée des antécédents des personnes et mettre en place des stratégies pour bien gérer le risque.	Ligne directrice E-17, Évaluation des antécédents des administrateurs et dirigeants	Vérification des antécédents de tous les employés et entrepreneurs en fonction du risque qu'ils présentent et selon les fonctions qu'ils exercent.	Sans objet
7. Il faut sécuriser les actifs technologiques, déceler leurs faiblesses et les corriger, mettre en place des mécanismes de défense efficaces et recenser les problèmes rapidement et avec exactitude.	Ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque	Sans objet	Description améliorée de ce qui constitue des activités malveillantes à l'endroit de l'infrastructure des technologies de l'information.

Principe	Lignes directrices connexes du BSIF	Nouvelle attente	Attentes élargies
8. Il faut soumettre les données et l'information à des normes et des contrôles adéquats afin d'assurer leur confidentialité, leur intégrité et leur disponibilité.	Ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque Ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle	Prise en compte de la vulnérabilité aux activités malveillantes, à l'influence indue et à l'ingérence étrangère, aux fins du classement des données.	Les besoins d'accès du personnel pour empêcher l'influence indue et l'ingérence étrangère.
9. Il faut soumettre les tiers à des évaluations équivalentes et proportionnelles afin de se protéger des menaces.	Ligne directrice B-10, Gestion du risque lié aux tiers	La gestion du risque lié aux tiers est réalisée du point de vue de l'intégrité et de la sécurité et est proportionnelle au degré d'accès du tiers aux locaux, aux personnes, aux actifs technologiques et aux données et à l'information de l'institution financière. Des processus d'approvisionnement transparents et objectifs.	Sans objet
10. Les menaces découlant de la suspicion d'une influence indue, d'une ingérence étrangère et d'activités malveillantes doivent être détectées et signalées rapidement.	Ligne directrice E-13, Gestion de la conformité à la réglementation	Notification au BSIF lorsqu'une influence indue, une ingérence étrangère ou une activité malveillante est signalée à la GRC, au SCRS ou à d'autres autorités.	Sans objet