LE BSIF AJOUTE LA LIGNE DIRECTRICE B-13 À SA GESTION DU RISQUE LIÉ AUX TECHNOLOGIES ET DU CYBERRISQUE

Publié le 31 juillet, 2022

Catégories: Perspectives, Publications

Le 13 juillet 2022, le Bureau du surintendant des institutions financières (le « **BSIF** ») a publié sa version définitive de la *Ligne directrice B-13 : Gestion du risque lié aux technologies et du cyberrisque* (la « **Ligne directrice B-13** »)[1]. Ayant pour but d'améliorer la résilience des institutions financières fédérales (les « **IFF** ») aux risques liés aux technologies et aux cyberrisques, elle s'ajoute au préavis intitulé *Signalement des incidents liés à la technologie et à la cybersécurité*[2] du BSIF (qui exige, entre autres, que soit signalé par écrit au superviseur en chef des IFF et à la Division du risque lié à la technologie du BSIF tout incident technologique ou de cybersécurité à signaler dans les 24 heures suivant l'incident) ainsi qu'à l'outil d'autoévaluation en matière de cybersécurité[3] (utilisé pour évaluer le degré de préparation des IFF aux atteintes à la cybersécurité), deux ressources parues en août 2021.

Le BSIF a publié une version provisoire de la Ligne directrice B-13 en novembre 2021, puis l'a retravaillée à la suite de consultations avec les principales parties prenantes. Comparativement à la version de novembre 2021, la version définitive est plus simple et moins prescriptive; ses définitions et exigences ont également été clarifiées[4].

Elle se concentre sur trois thèmes :

1. **Gouvernance et gestion du risque.** Ce thème englobe les attentes du BSIF envers les IFF en ce qui concerne la définition de responsabilités et de structures claires ainsi que de stratégies et de cadres exhaustifs pour la gestion du risque lié aux technologies et du cyberrisque (les risques d'insuffisance, d'interruption, de destruction, de défaillance ou de dommages découlant de la consultation non autorisée, de la modification ou de l'utilisation malveillante des outils, ressources humaines ou processus de technologie de l'information nécessaires aux besoins opérationnels, et qui peuvent causer des pertes financières et/ou des torts à la réputation. L'accent est mis sur la présence d'un cadre de gestion du risque et d'une structure organisationnelle nécessaires pour instaurer un système de responsabilisation clair. Plus précisément, la Ligne directrice B-13 charge la haute direction de diriger les activités de sécurité des technologies et de cybersécurité des IFF, et d'assigner aux cadres supérieurs des responsabilités claires en matière de gouvernance des risques. Le BSIF appelle aussi les IFF à faire preuve

d'initiative dans la prévision des risques et la préparation aux nouveaux problèmes à mesure qu'évolue la technologie.

2. **Activités technologiques et résilience.** Ce thème englobe les attentes du BSIF envers les IFF relativement à la création d'un environnement technologique stable, évolutif et résilient. Cet environnement doit aussi être supervisé pour qu'il reste à jour, et appuyé par des processus d'exploitation et de sauvegarde robustes et viables. On y aborde plusieurs sujets, notamment l'architecture technologique, la gestion des actifs, la gestion de projet, le cycle de développement des systèmes, la gestion des lancements et correctifs, la gestion des problèmes, la surveillance et la reprise après sinistre.
3. **Cybersécurité.** Ce thème englobe les attentes du BSIF quant à l'adoption d'une optique de sécurité à l'égard de la technologie pour le maintien de la confidentialité, de l'intégrité et de la disponibilité des biens technologiques des IFF. Le BSIF appelle les IFF à faire preuve d'initiative dans la détection des risques et menaces, plutôt que de réagir passivement, et énonce les critères à respecter pour ce faire. Il énumère aussi les mesures à mettre en place pour détecter et prévenir les menaces liées aux technologies et les cybermenaces (comme l'utilisation de technologies cryptographiques solides) ainsi que pour traiter les incidents de sécurité, s'en remettre et en tirer des leçons.

Il est admis qu'il n'existe aucune méthode universelle et que les IFF doivent donc avoir la liberté de choisir la manière d'atteindre chacun de ces objectifs en fonction de leur taille, de leur profil de risques et de la nature, l'ampleur et la complexité de leurs activités.

La Ligne directrice B-13 entrera en vigueur le 1er janvier 2024, ce qui laissera aux IFF le temps de s'autoévaluer et de voir à leur conformité. Les IFF doivent l'étudier attentivement pour déterminer dans quelle mesure leurs politiques et procédures actuelles la respectent et s'il est nécessaire de les modifier d'ici l'entrée en vigueur de la Ligne directrice.

À noter que des exigences semblables ont également été élaborées à l'intention d'institutions financières sous régime provincial ces dernières années (par exemple, les lignes directrices sur la sécurité de l'information[5] en Colombie-Britannique ou le questionnaire d'autoévaluation en matière de cybersécurité[6] en Saskatchewan).

Si vous avez des questions sur la Ligne directrice B-13 ou sur la conception de programmes et politiques de cybersécurité, communiquez avec un membre du groupe Protection de la vie privée et des données.

[1] [ps2id id='1' target='/]"Gestion du risque lié aux technologies et du cyberrisque. En ligne. Bureau du surintendant des institutions financières (dernière modification le 13 juillet 2022).
[2] [ps2id id='2' target='/]"Signalement des incidents liés à la technologie et à la cybersécurité. En ligne. Bureau du surintendant des institutions financières (dernière modification le 3 septembre 2021).

[3] [ps2id id='3' target='/]“Autoévaluation en matière de cybersécurité. En ligne. Bureau du surintendant des institutions financières (dernière modification le 16 août 2021).
[4] [ps2id id='4' target='/]"Réponses du BSIF aux commentaires reçus dans le cadre de la consultation sur la version à l’étude de la ligne directrice B-13 – Gestion du risque lié aux technologies et du cyberrisque. En ligne. Bureau du surintendant des institutions financières (dernière modification le 9 juin 2022).
[5] [ps2id id='5' target='/]“Lignes directrices sur la sécurité de l’information. En ligne. British Columbia Financial Services Authority (dernière modification le 18 février 2021).
[6] [ps2id id='6' target='/]“Questionnaire d’autoévaluation en matière de cybersécurité. En ligne. Financial and Consumer Affairs Authority of Saskatchewan.

par Darcy Ammerman, Robbie Grant et ZiJian Yang (étudiant d’été en droit)

Mise en garde