Bureau du surintendant des institutions financières Canada
Office of the Superintendent of Financial Institutions Canada

NOTE D'INFORMATION

Date : Le 27 octobre 2013

Destinataires : Institutions financières fédérales

Objet : Conseils sur l'auto-évaluation en matière de cybersécurité

Les cyberattaques sont de plus en plus fréquentes et complexes, et elles relèvent le profil de risque de nombreux organismes de par le monde. Par conséquent, ces organismes, dont des institutions financières, les fournisseurs d'infrastructures essentielles, les organismes de réglementation de même que les médias et le grand public ont accordé récemment beaucoup d'attention au niveau général de préparation aux attaques de cette nature.

La cybersécurité gagne en importance en raison de divers facteurs, par exemple le recours continu de plus en plus grand à la technologie, l'interconnectivité du secteur financier et le rôle essentiel que les institutions financières fédérales (IFF) jouent dans l'ensemble de l'économie. Le BSIF s'attend donc à ce que la haute direction d'une IFF confirme que les politiques et les pratiques de gestion des cyberrisques demeurent appropriées et efficaces, eu égard à l'évolution des circonstances et des risques mêmes.

Le BSIF reconnaît que bien des IFF ont peut-être déjà évalué leur état de préparation ou qu'elles s'apprêtent peut-être à le faire. À la lumière de ces faits, le BSIF est d'avis que des conseils sur l'auto-évaluation pourraient être utiles à bon nombre d'entre elles, et il leur fait donc parvenir le guide ci-annexé.

Les IFF sont encouragées à remplir ce formulaire ou à se servir d'outils semblables pour évaluer leur état actuel de préparation, puis concevoir et tenir à jour des pratiques efficaces de cybersécurité. Le BSIF n'a pas l'intention, pour le moment, d'établir des consignes précises de contrôle et de gestion du cyberrisque. Néanmoins, et dans l'esprit de l'importance accordée à la cybersécurité dans le document intitulé *Plan et priorités pour 2013-2016*, le BSIF pourrait demander aux institutions de remplir le formulaire ci-joint ou insister autrement sur les pratiques de cybersécurité au moment des évaluations de surveillance.

Les questions à ce sujet peuvent être adressées à Mohamad Al-Bustami, directeur général, Division des risques liés à la technologie, à 416-973-2088, ou TRD@osfi-bsif.gc.ca.

Le surintendant auxiliaire,

Mark Zelmer

BSIF
OSFI

255, rue Albert
Ottawa, Canada
K1A 0H2

www.osfi-bsif.gc.ca

Canada

Annexe – Conseils sur l'auto-évaluation en matière de cybersécurité

Le présent formulaire d'auto-évaluation définit les attributs et les particularités souhaitables des pratiques de cybersécurité dont l'IFF pourrait tenir compte lorsqu'elle juge de l'adéquation de son cadre de cybersécurité et décide des améliorations à y apporter. Dans le cadre de cet exercice, l'IFF est invitée à décrire l'état actuel plutôt que l'état visé de ses pratiques de cybersécurité, dans l'optique de l'ensemble de l'entreprise. Si l'IFF applique des pratiques utiles que le formulaire ne mentionne pas, elle devrait les énumérer et décrire les résultats de leur évaluation.

Le BSIF recommande aux IFF de coter leur degré actuel de maturité sur une échelle de 1 à 4 et de bien justifier toutes les cotes attribuées. Voici la définition proposée de chacune.

4 – Mise en œuvre intégrale	L'IFF a mis en œuvre les principes à l'échelle de l'entreprise en tout. Des éléments de preuve appuient l'évaluation. Aucune question en suspens n'a été constatée (p. ex., par les responsables de l'auto-évaluation ou par des groupes comme l'équipe de la gestion du risque opérationnel, les auditeurs internes, les surveillants ou des tiers autres).
3 – Mise en œuvre en grande partie	L'IFF a mis en œuvre les principes à l'échelle de l'entreprise dans une large mesure, mais pas intégralement, ou certaines questions en suspens mineures ont été constatées (p. ex., par les responsables de l'auto-évaluation ou par des groupes comme l'équipe de la gestion du risque opérationnel, les auditeurs internes, les surveillants ou des tiers autres).
2 – Mise en œuvre partielle	L'IFF a mis en œuvre les principes partiellement, il lui reste à en réaliser des aspects importants et certaines questions en suspens ont été constatées (p. ex., par les responsables de l'auto-évaluation ou par des groupes comme l'équipe de la gestion du risque opérationnel, les auditeurs internes, les surveillants ou des tiers autres).
1 – Aucune mise en œuvre	L'IFF n'a pas mis en œuvre cette pratique.
S.O.	Si l'IFF détermine que les cotes de 1 à 4 ne s'appliquent pas, elle est invitée à bien justifier sa décision.

Vous trouverez ci-après le formulaire d'auto-évaluation:

1. Organisation et ressources

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
1.1	L'IFF a établi clairement qui doit rendre compte des résultats et des ressources financières du programme de cybersécurité et qui en a la charge[1].			
1.2	L'IFF a assigné des responsabilités et des rôles particuliers en matière de gestion de la cybersécurité, et des pouvoirs opérationnels suffisants ont été délégués aux personnes concernées.			
1.3	L'IFF dispose d'un groupe de spécialistes en cybersécurité gérés centralement qui ont pour tâche de recueillir des renseignements sur les menaces, de gérer les menaces et d'intervenir en cas d'incidents.			
1.4	L'IFF dispose de capacités d'identification et d'intervention en tout temps pour gérer la cybersécurité.			
1.5	L'IFF dispose d'un effectif suffisant et spécialisé pour gérer la cybersécurité.			
1.6	Les spécialistes de la cybersécurité font l'objet d'une vérification des antécédents et d'une enquête de sécurité approfondies.			
1.7	L'IFF a un plan officiel de formation technique continue des spécialistes de la cybersécurité.			
1.8	Une formation sur la cybersécurité est offerte aux nouveaux employés et aux employés en poste.			
1.9	Des séances de sensibilisation à la cybersécurité sont offertes à tous les employés.			

[1] Cadre de cybersécurité : Série complète de ressources organisationnelles, notamment politiques, personnel, processus, pratiques et technologies utilisées pour évaluer les cyberrisques et les cyberattaques et les atténuer.

2. Évaluation du cyberrisque et du contrôle

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
2.1	L'IFF dispose d'un processus d'évaluation périodique et complet du cyberrisque qui tient compte des personnes (soit les employés, les clients et d'autres parties de l'extérieur), des processus, des données et de la technologie, dans l'ensemble de ses secteurs d'activité et régions.			
2.2	L'IFF évalue les éventuelles expositions au cyberrisque découlant de ses ententes d'impartition réputées importantes aux termes de la ligne directrice B-10 du BSIF et prend des mesures pour les atténuer.			
2.3	L'IFF évalue les éventuelles expositions au cyberrisque découlant de ses fournisseurs de services de TI essentiels et prend des mesures pour les atténuer.			
2.4	Les processus de gestion du changement, d'évaluation du risque et de diligence raisonnable de l'IFF tiennent compte du cyberrisque.			
2.5	L'IFF effectue périodiquement des examens de la vulnérabilité du matériel et des logiciels et des tests sur les clients, les serveurs et l'infrastructure réseau pour déceler les lacunes du contrôle de la sécurité.			
2.6	L'IFF effectue périodiquement des tests de pénétration aux limites du réseau pour déceler les lacunes du contrôle de la sécurité (p. ex., points d'entrée et de sortie du réseau ouverts).			
2.7	L'IFF effectue périodiquement des tests en collaboration avec ses services tiers d'atténuation du cyberrisque.			
2.8	L'IFF effectue périodiquement des exercices de simulation de cyberattaques (y compris déni de service distribué) et de reprise des activités.			
2.9	L'IFF tient compte dans son évaluation des risques de l'incidence d'une interruption prolongée du service Internet à l'échelle du Canada.			

3. Connaissance situationnelle

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
3.1	L'IFF tient une base de connaissances panorganisationnelle à jour de ses utilisateurs, dispositifs et applications de même que des rapports entre eux, ce qui comprend, sans toutefois s'y limiter : • l'inventaire des actifs (logiciels et matériel); • des schémas du réseau (indiquant notamment les limites, le trafic et le flux de données); • des données sur l'utilisation et le fonctionnement du réseau.			
3.2	L'IFF tient centralement des données historiques sur les événements liés à la sécurité.			
3.3	L'IFF normalise et regroupe les données sur les événements liés à la sécurité et établit des corrélations entre elles.			
3.4	L'IFF effectue une analyse automatisée des événements liés à la sécurité pour prévoir les éventuelles cyberattaques dont les attaques par déni de service distribué.			
3.5	L'IFF ajoute à une analyse automatisée des événements liés à la sécurité d'autres analyses spécialisées de ces événements pour prévoir les éventuelles cyberattaques.			
3.6	L'IFF surveille et suit les incidents liés à la cybersécurité dans le secteur des services financiers et de manière plus globale, selon le cas, en participant aux programmes sectoriels (p. ex., ceux du Centre canadien de réponse aux incidents cybernétiques).			
3.7	L'IFF est abonnée aux services de renseignements sectoriels sur la cybersécurité.			

4. Gestion du risque de menace et de vulnérabilité

Point	Critères	Cote*	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
Détection/prévention de la perte de données				
4.1	L'IFF a instauré des outils pour : • empêcher que des données protégées quittent l'entreprise; • surveiller le trafic sortant à risque élevé afin de déterminer si des données protégées quittent l'entreprise (p. ex., par région, taille, volume, type de données); • protéger les données stockées dans les mémoires en ligne et hors ligne (p. ex., ordinateurs de bureau, ordinateurs portatifs, dispositifs mobiles, dispositifs amovibles et supports amovibles); • protéger les données inactives et actives.			
4.2	L'IFF a instauré les mécanismes de contrôle susmentionnés à l'échelle de l'entreprise.			
Détection et atténuation des cyberincidents				
4.3	L'IFF a instauré les outils de sécurité qui suivent, et elle veille à ce qu'ils soient d'actualité, automatiquement mis à jour et appliqués à l'ensemble de l'entreprise : • systèmes de détection des intrusions et de protection contre les intrusions; • pare-feux des applications Web; • anti-virus; • anti-espiogiciels; • anti-pourriel; • protection contre les attaques par déni de service distribué (DDoS); • autre (veuillez décrire).			
4.4	L'IFF a instauré les outils de sécurité susmentionnés en se servant de techniques avancées de détection (p. ex., axées sur le comportement et/ou axées sur la réputation).			

Sécurité des logiciels				
4.5	L'IFF dispose d'un processus permettant d'obtenir, de tester et de déployer automatiquement des correctifs de sécurité et des mises à jour en temps opportun selon la criticité.			
4.6	L'IFF considère et atténue le cyberrisque présenté par des logiciels pour lesquels il est impossible d'obtenir du soutien.			
4.7	L'IFF dispose d'un processus de confirmation de la réussite du déploiement complet des correctifs de sécurité et de rectification des échecs de mise à jour.			
4.8	Les logiciels de l'IFF développés en interne ou en externe sont assujettis à des normes de conception, de codage et de mise à l'essai de systèmes protégés qui intègrent de bons contrôles de la cybersécurité.			
4.9	L'IFF instaure les mécanismes de contrôle susmentionnés à l'échelle de l'entreprise.			
Infrastructure réseau				
4.10	L'IFF a instauré un mécanisme de surveillance et de protection de la limite réseau.			
4.11	L'IFF répartit son réseau d'entreprise en de nombreuses zones de confiance distinctes.			
4.12	L'infrastructure réseau de l'IFF comporte de nombreuses couches de défense (p. ex., en nuage, PPI et sur place) pour contrer les attaques par déni de service distribué (DDoS).			
4.13	L'IFF est en mesure d'isoler ou de circonscrire rapidement les établissements compromis, ou de mettre fin rapidement à leurs activités.			
4.14	L'IFF a instauré des processus et des outils pour sécuriser les dispositifs mobiles et les réseaux sans fil.			
4.15	L'IFF instaure les mécanismes de contrôle susmentionnés à l'échelle de l'entreprise.			

Gestion et configuration standard de la sécurité				
4.16	L'IFF produit des images de systèmes d'exploitation normalisées pour les dispositifs client, serveur et réseau.			
4.17	L'IFF applique un processus officiel de gestion du changement pour gérer la configuration de la sécurité de l'ensemble du matériel et des logiciels de ses réseaux.			
4.18	L'IFF énonce par écrit, instaure et fait appliquer des normes de configuration de sécurité pour l'ensemble du matériel et des logiciels du réseau.			
4.19	L'IFF limite l'utilisation de logiciels et de matériel non autorisés ou non enregistrés, ce qui comprend les dispositifs mobiles, au moyen de politiques et d'outils automatisés.			
4.20	L'IFF instaure les mécanismes de contrôle susmentionnés à l'échelle de l'entreprise.			
Contrôle et gestion de l'accès réseau				
4.21	L'IFF est en mesure de déceler et de bloquer automatiquement l'accès non autorisé au réseau (p. ex., accès câblé, sans fil et à distance).			
4.22	L'IFF applique de solides mécanismes d'authentification pour gérer les identités des utilisateurs et leur accès au réseau.			
4.23	L'IFF contrôle et gère rigoureusement l'utilisation des privilèges administratifs.			
4.24	L'IFF instaure les mécanismes de contrôle susmentionnés à l'échelle de l'entreprise.			
Gestion des tiers				
4.25	L'IFF tient compte du risque lié à la cybersécurité dans le cadre de son processus de diligence raisonnable visant les ententes d'impartition importantes et les fournisseurs de services de TI essentiels, y compris les ententes de sous-traitance connexes.			
4.26	Les contrats visant toutes les ententes d'impartition importantes et tous les fournisseurs de services de TI essentiels prévoient la protection de l'information de l'IFF.			
4.27	L'IFF a instauré un processus de surveillance du niveau de préparation au cyberrisque présenté par les ententes d'impartition importantes et les fournisseurs de services de TI essentiels.			

4.28	L'IFF a instauré des processus qui signalent rapidement un cyberincident impliquant les fournisseurs de services avec lesquels elle a conclu au moins une entente d'impartition importante et les fournisseurs de service de TI essentiel.			
Clientèle				
4.29	Des séances de sensibilisation à la cybersécurité et d'information à ce sujet sont offertes à la clientèle.			
4.30	L'IFF a pris des mesures additionnelles pour protéger sa clientèle.			

5. Gestion des incidents liés à la cybersécurité

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
5.1	La conception du cadre de gestion des incidents de l'IFF permet de réagir rapidement aux cyberincidents importants.			
5.2	Une structure « de commandement et de contrôle » efficace dotée de pouvoir délégué de dépenser suffisants a été établie dans le cadre de gestion des incidents afin de favoriser une intervention rapide peu importe l'ampleur des incidents de cybersécurité.			
5.3	L'IFF a instauré des procédures écrites de contrôle et d'analyse des incidents de cybersécurité et d'intervention, le cas échéant.			
5.4	La conception du processus de gestion du changement de l'IFF permet d'intervenir promptement et de prendre des mesures d'atténuation rapides dans le cas d'incidents de cybersécurité.			
5.5	Le cadre de gestion des incidents de l'IFF comporte des critères de signalement progressif aux paliers supérieurs qui cadrent avec la taxonomie de la cybersécurité.			
5.6	L'IFF a un plan de communication interne pour traiter des incidents de cybersécurité qui comprend des protocoles de communication pour les principaux intervenants internes (p. ex., unités opérationnelles pertinentes / centres d'appels, haute direction, gestion des risques et conseil d'administration).			
5.7	L'IFF a un plan de communication externe pour traiter des incidents de cybersécurité qui comprend des protocoles de communication et des communications provisoires formulées au préalable pour les principaux intervenants externes (c.-à-d., clientèle, médias, fournisseurs de services essentiels, etc.).			

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
5.8	La conception du processus de gestion des incidents de cybersécurité de l'IFF est telle que les tâches suivantes doivent être menées à bien avant qu'un incident puisse être clos officiellement : • reprise des activités après l'interruption des services causée par des cyberincidents; • confirmation de l'intégrité des systèmes après des cyberincidents; • recouvrement des données perdues ou corrompues à cause de cyberincidents.			
5.9	L'IFF a instauré un processus d'examen postérieur à un incident qui : • est exécuté dans le cas d'incidents importants de cybersécurité; • comprend des enquêtes judiciaires contre la cybercriminalité; • établit la chronologie des événements préalables et postérieurs à l'incident de cybersécurité et ceux qui se produisent pendant l'incident; • identifie la cause profonde et signale les lacunes du contrôle; • évalue les éventuels échecs du processus de gestion des incidents; • établit un plan d'action pour corriger les lacunes constatées.			

6. Gouvernance de la cybersécurité

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
Politique et stratégie de cybersécurité				
6.1	L'IFF a établi une politique de cybersécurité à l'échelle de l'entreprise[2], et a instauré des procédures à l'appui qui énoncent les démarches qu'elle fera pour identifier et gérer les cyberrisques.			
6.2	La politique de cybersécurité définit clairement les rôles et les responsabilités de chacune des trois lignes de défense et des autres parties prenantes.			
6.3	La politique de cybersécurité s'applique à tous les groupes et entités opérationnels de l'IFF, ce qui comprend les filiales, les coentreprises et les régions.			
6.4	L'IFF a défini une taxonomie commune et uniforme du cyberrisque.			
6.5	La politique de cybersécurité de l'IFF est liée à d'autres politiques pertinentes de gestion du risque, notamment celles qui portent sur la sécurité de l'information, la gestion de la continuité des activités, l'impartition, les nouvelles initiatives, la gestion du changement, etc.			
6.6	L'IFF a établi une stratégie de cybersécurité conforme à sa stratégie d'affaires.			
6.7	L'IFF dispose d'un plan stratégique et tactique de mise en œuvre de la cybersécurité qui décrit les principales initiatives et les échéanciers.			
Deuxième ligne de défense (p. ex., gestion du risque))				
6.8	Des évaluations du risque et des contrôles (ERC) traitent du cyberrisque et des contrôles d'atténuation.			
6.9	Des principaux indicateurs de risque et de rendement ainsi que des seuils ont été établis pour les principaux risques inhérents à la cybersécurité et aux contrôles de l'IFF.			
6.10	L'IFF s'est servie de l'analyse de scénario pour simuler une cyberattaque importante et considérer des mesures d'atténuation de même que pour déceler les éventuelles lacunes du contrôle.			

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
6.11	La deuxième ligne de défense évalue efficacement le cyberrisque dans le cadre du processus de gestion du changement de l'IFF.			
6.12	Les responsabilités de la deuxième ligne de défense en matière d'évaluation de la cybersécurité ont été attribuées à un groupe de contrôle indépendant possédant une expertise en cyberrisque.			
6.13	La deuxième ligne de défense effectue régulièrement une analyse critique indépendante des diverses évaluations du cyberrisque menées par la première ligne de défense (p. ex., évaluation des risques dans les cadres des AERC, analyse de scénario, processus de gestion du changement, PIR et évaluations des menaces et des risques).			
6.14	La deuxième ligne de défense veille à ce que des mesures d'atténuation efficaces soient prises à l'égard d'incidents de cybersécurité et les soumet à une analyse critique.			
6.15	Les énoncés sur la propension à prendre des risques et la tolérance au risque opérationnel de l'IFF tiennent compte du cyberrisque.			
6.16	L'IFF a envisagé de contracter une assurance contre le cyberrisque qui procure des mesures d'atténuation financière des cyberincidents et de leurs incidences.			
Audit interne – troisième ligne de défense				
6.17	La portée des audits internes englobe tous les aspects du présent questionnaire qui ont trait à la cybersécurité.			
6.18	La fréquence des audits de cybersécurité est établie en fonction du risque de cyberattaques et est conforme à ce dernier.			
6.19	Le service d'audit interne a évalué à la fois la conception et l'efficacité du cadre de cybersécurité ou prévoit le faire.			
6.20	Le service d'audit interne dispose d'assez de ressources et d'expertise pour auditer la mise en œuvre du cadre de cybersécurité.			

[2] Politique de cybersécurité : Ensemble de principes écrits et autorisés qui expliquent comment le programme de cybersécurité sera régi et exécuté.

Point	Critères	Cote	Justification et description de la cote (Conception et efficacité du contrôle)	Plan d'action et date cible de la mise en œuvre intégrale
Supervision par la haute direction				
6.21	Un comité spécial de la haute direction a été mis sur pied et chargé du dossier du cyberrisque ou un autre comité de la haute direction peut consacrer suffisamment de temps aux discussions sur la mise en œuvre du cadre ou de la politique de cybersécurité.			
6.22	La haute direction offre des ressources et un financement suffisants pour soutenir la mise en œuvre du cadre de cybersécurité de l'IFF.			
6.23	Des processus ont été instaurés afin de signaler les dépassements des limites et des seuils à des paliers successivement plus élevés de la haute direction dans le cas des cyberincidents significatifs ou graves.			
6.24	Le cadre de contrôle interne[3] de l'IFF englobe le cadre de cybersécurité et le son plan de mise en œuvre, ce qui comprend l'adéquation des contrôles d'atténuation en vigueur.			
Analyse comparative externe				
6.25	L'IFF a exécuté un examen comparatif externe relatif à son cadre de cybersécurité.			

[3] Voir la ligne directrice *Gouvernance d'entreprise* pour obtenir des précisions à ce sujet.