PROJET

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DES RISQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS

Juin 2019

TABLE DES MATIÈRES

Préambule

La présente ligne directrice est une indication des attentes de l'Autorité des marchés financiers (l'« Autorité ») à l'égard de l'obligation légale des institutions financières de suivre des pratiques de gestion saine et prudente. Elle porte donc sur l'interprétation, l'exécution et l'application de cette obligation imposée aux institutions financières.

Dans cette optique, l'Autorité privilégie une approche basée sur des principes plutôt que d'édicter des règles précises. Ainsi, du fondement même d'une ligne directrice, l'Autorité confère aux institutions financières la latitude nécessaire leur permettant de déterminer elles-mêmes les stratégies, politiques et procédures pour la mise en œuvre de ces principes de saine gestion et de voir à leur application en regard de la nature, de la taille, de la complexité de leurs activités et de leur profil de risque. À cet égard, la ligne directrice illustre des façons de se conformer aux principes énoncés.

Note de l'Autorité

L'Autorité considère la gouvernance, la gestion intégrée des risques et la conformité (GRC) comme les assises sur lesquelles doivent reposer la gestion saine et prudente et les saines pratiques commerciales d'une institution financière et conséquemment, les bases sur lesquelles l'encadrement prudentiel donné par l'Autorité s'appuie.

La présente ligne directrice s'inscrit dans cette perspective et énonce les attentes de l'Autorité à l'égard des pratiques en matière de gestion des risques liés aux technologies de l'information et des communications (TIC).

Champ d'application

La présente ligne directrice s'applique aux assureurs de personnes, aux assureurs de dommages, aux sociétés de gestion de portefeuille contrôlées par un assureur, aux coopératives de services financiers, aux sociétés de fiducie et aux sociétés d'épargne régis par les lois suivantes :

- *Loi sur les assurances*, RLRQ, c. A-32[1];
- *Loi sur les coopératives de services financiers*, RLRQ, c. 67.3[2];
- *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.01[3].

Enfin, cette ligne directrice s'applique tant à l'institution financière qui opère de façon autonome qu'à celle qui est membre d'un groupe financier.

Dans le cas des coopératives de services financiers et des sociétés mutuelles d'assurance membres d'une fédération, les normes ou politiques adoptées à leur intention par la fédération doivent être cohérentes, voire convergentes, avec les principes de gestion saine et prudente tel qu'il est précisé dans la présente ligne directrice.

1 Art. 325.0.1 et 325.0.2 al.1, par. 3º et al. 2 de la *Loi sur les assurances*.

2 Art. 565.1 et 566 de la *Loi sur les coopératives de services financiers*.

3 Art. 314.1 al.1, par. 3º et al. 2 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*.

Prise d'effet et processus de mise à jour

La *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* est effective à compter du 1er juin 2019.

En regard de l'obligation légale des institutions de suivre des pratiques de gestion saine et prudente, l'Autorité s'attend à ce que chaque institution se soit approprié les principes de cette ligne directrice en élaborant des stratégies, politiques et procédures adaptées à sa nature, sa taille, la complexité de ses activités et son profil de risque.

L'Autorité s'attend à ce que l'institution financière s'approprie les attentes de la présente ligne directrice et qu'elle les mette en œuvre d'ici le 1er juin 2020. Dans la mesure où une institution a déjà mis en place un tel encadrement, l'Autorité pourra en vérifier la conformité avec les exigences prescrites par la loi.

Cette ligne directrice sera actualisée en fonction des développements en matière de gestion du risque des technologies de l'information et des communications et à la lumière des constats effectués dans le cadre des travaux de surveillance menés auprès des institutions financières visées.

Introduction

La progression rapide des innovations technologiques a contribué à transformer les processus et les modèles d'affaires des institutions financières. Ces innovations ont, par contre, introduit des risques significatifs à une époque où les institutions deviennent de plus en plus interconnectées et dépendantes de systèmes hérités[4] et de fournisseurs externes pour mener à bien leurs activités.

L'adoption des innovations technologiques a aussi accentué les risques de perte, de vol, de corruption et d'accès non autorisé aux données. En outre, les institutions sont davantage exposées aux risques de cyberattaques qui sont de plus en plus sophistiquées, fréquentes, ciblées et difficiles à détecter. Les cyberrisques peuvent avoir des conséquences défavorables significatives qui ne devraient pas être sous-estimées, tant au niveau financier et légal que sur les clients et la réputation de l'institution.

Dans ce contexte, la gestion des risques liés aux TIC[5] devrait être complète, robuste et devrait alimenter les disciplines clés telles que la planification stratégique, l'infogérance, la gestion du changement, la sécurité de l'information (incluant la cybersécurité), la continuité des activités et la gestion des données.

Cette ligne directrice expose les attentes de l'Autorité à l'égard de la gestion des risques liés aux TIC. Elle présente la position de l'Autorité, qui évoluera au fur et à mesure que les connaissances de ces sujets se préciseront à travers les activités de supervision et le développement des encadrements internationaux.

Il est important de noter que cette ligne directrice ne prétend pas couvrir tous les aspects de la gestion des risques liés aux TIC. Elle met plutôt l'accent sur les éléments que l'Autorité a jugé pertinents au moment de sa rédaction. Il est de la responsabilité de l'institution de bien comprendre les risques auxquels elle est confrontée et de s'assurer qu'ils soient pris en compte adéquatement en fonction de sa nature, de sa taille, de la complexité de ses activités et de son profil de risque.

---

4 Un système hérité, patrimonial ou *legacy system* en anglais, est un matériel et/ou logiciel continuant d'être utilisé dans une organisation, alors qu'il est supplanté par des systèmes plus modernes. Il fait partie d'un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

5 L'Autorité définit le risque TIC comme étant le risque d'affaires lié à l'utilisation, la propriété, l'opération et l'adoption des TIC. Ce risque comprend notamment les risques de disponibilité et de continuité, de sécurité (incluant la cybersécurité), de changement, d'intégrité des données et d'infogérance.

1. Le cadre de gouvernance des technologies de l'information et des communications

L'Autorité s'attend à ce que l'institution financière identifie, évalue, contrôle, atténue et suive en continu les risques liés aux TIC. Elle devrait établir et maintenir une stratégie et un cadre de gestion spécifique à ces risques qui soient adéquatement développés à partir de sources, de recommandations et de normes reconnues.

En sus des attentes générales formulées par l'Autorité dans la *Ligne directrice sur la gouvernance*, l'Autorité précise ci-après ses attentes en matière de gouvernance liée aux TIC.

Le conseil d'administration[6] doit s'assurer de l'établissement et du maintien d'un cadre de gouvernance des TIC ainsi que d'une définition claire des rôles et responsabilités nécessaires à l'atteinte des objectifs de l'institution en la matière. À cet effet, il devrait notamment :

- s'assurer d'échanger continuellement avec les parties intéressées afin de documenter sa compréhension des besoins et porter un jugement sur la conception actuelle et future de la gouvernance des TIC;
- s'assurer de la mise en place du cadre de gouvernance des TI selon les préceptes[7] (section 1.5), les modèles de prise de décision et les niveaux d'autorité convenus;
- définir l'information requise pour la prise de décision éclairée (section 1.7);
- suivre l'efficacité et la performance de la gouvernance des TIC;
- évaluer dans quelle mesure la gouvernance des TIC et les mécanismes déployés (incluant les structures, principes de conception du cadre et processus) opèrent efficacement et produisent une surveillance appropriée des TIC.

Il doit de plus s'assurer que l'appétit (section 2.2) et le niveau de tolérance pour le risque lié aux TIC soient compris, articulés et communiqués et que le risque de l'utilisation des TIC soit identifié et géré. À cet effet, il devrait notamment :

- examiner et juger de l'effet courant et futur de l'utilisation des TIC dans l'institution;
- s'assurer de l'établissement d'une gestion de risque afin de fournir une assurance raisonnable que les pratiques de gestion du risque TIC n'excèdent pas l'appétit;
- s'assurer du suivi des métriques et objectifs clés des processus de gestion de risque lié aux TIC.

---

6 Lorsqu'il est fait mention du conseil d'administration, il peut s'agir d'un comité de ce dernier formé, par exemple, à des fins d'examen de points particuliers.

7 Conduite à suivre, règle (ou un ensemble de règles) à observer, généralement formulée par une autorité incontestée dans un domaine précis.

Le conseil doit s'assurer que des ressources suffisantes et adéquates (section 1.1), liées aux TIC (individus, processus et technologies) soient disponibles pour supporter les objectifs d'entreprise.

Il doit aussi s'assurer que la mesure et la reddition de la performance et la conformité des TIC soient transparentes et que les parties intéressées approuvent les objectifs, les métriques et les actions correctives. À cet effet, il devrait :

- examiner et évaluer les besoins courants et futurs à l'égard de l'utilisation des TIC pour la communication et la reddition aux parties intéressées;
- établir des principes pour les communications et s'assurer de l'établissement de mécanismes contribuant au rehaussement de la qualité et l'exhaustivité de l'information (section 1.7).

1.1 Compétences

L'Autorité s'attend à ce que le conseil d'administration s'assure que ses membres et les instances décisionnelles[8] aient la connaissance et la compréhension requise de l'utilisation, des directions et des tendances des TIC, de même que l'autorité nécessaire pour exercer leurs responsabilités.

Une gouvernance efficace et efficiente qui inclut les technologies de l'information et des communications et les innovations liées à l'exploitation des TIC requiert un niveau approprié d'expertise, de qualifications professionnelles, de connaissances ou d'expériences pertinentes.

L'évaluation initiale de même que le maintien de ces attributs devraient se faire par le biais d'une politique d'évaluation des critères de compétence applicable aux membres des instances décisionnelles de l'institution. Cette politique d'évaluation devrait être appliquée sur une base périodique aux personnes nommées aux postes stratégiques liés à la gouvernance et la gestion des risques liées aux TIC afin de s'assurer du maintien des critères déterminés.

Au chapitre de la compétence, il importe de préciser que dans le cas des membres du conseil d'administration, le niveau approprié d'expertise, de qualifications professionnelles, de connaissance ou d'expérience pourrait être atteint de façon collective, c'est-à-dire par la complémentarité des attributs propres aux personnes qui y siègent.

En raison de la nature dynamique du risque TIC, l'institution financière pourrait considérer une actualisation périodique plus fréquente de sa grille d'aptitudes et de connaissances

[8] Par souci d'allègement du texte, l'expression générique « instances décisionnelles » sera utilisée pour faire référence aux membres du conseil d'administration, aux membres de la haute direction ainsi qu'aux responsables des fonctions de supervision.

relatives aux technologies de l'information utilisée pour l'évaluation de la compétence des personnes membres des instances décisionnelles.

Dans cette perspective, l'institution devrait recenser périodiquement l'ensemble des compétences courantes à l'égard des TIC, présentes au sein de l'institution ainsi que celles requises à la réalisation des stratégies et à l'atteinte des objectifs. Les parties intéressées à la gestion des risques TIC occupent plusieurs rôles qui requièrent des ensembles distincts de compétences dont les objectifs se rapportent à des niveaux variables d'éducation, de qualification, d'expérience, de connaissances et d'aptitudes techniques et/ou comportementales. De plus, ces compétences évoluent selon différents cycles de vie.

Afin de comprendre les vulnérabilités des systèmes TIC et les menaces, il est nécessaire d'avoir une connaissance de base des éléments constitutifs d'un système TIC et de la façon dont ils sont connectés physiquement et logiquement entre eux. Aussi, l'expertise dans les sources de menaces, les scénarios de menaces, les vulnérabilités et l'impact sur les affaires est essentielle. Elle fait référence à la nature et la composition de base du risque lié aux TIC et l'amélioration continue requise pour traiter la nature dynamique des menaces, des vulnérabilités et des impacts.

Afin de minimiser le risque qu'il n'y ait pas suffisamment d'expérience TIC aux postes d'administrateurs et de président-directeur général, le conseil d'administration devrait développer un processus formel d'acquisition de compétences qui traite des enjeux stratégiques liés aux TIC.

La gestion d'une institution financière implique une connaissance poussée de celle-ci, de l'environnement dans lequel elle opère, de sa culture, de son ou ses secteurs d'activités ainsi que de son profil de risque. Cette connaissance porte aussi sur des domaines tels que les implications, les opportunités et les menaces entourant les TIC et les innovations qui y sont liées. Dans cette optique, afin que le conseil d'administration soit en mesure de comprendre et d'influencer les compromis entre la flexibilité, la stabilité et la performance opérationnelle recherchée dans le développement de systèmes TIC supportant l'architecture d'entreprise, il apparaît essentiel que l'institution financière mette de l'avant des mécanismes formels pour la création et le maintien d'une documentation de l'environnement des TIC (section 1.6).

1.2 Rôles et responsabilités

L'Autorité s'attend à ce que l'institution financière établisse et documente clairement les rôles et les responsabilités des parties intéressées à la gouvernance des TIC afin de bien camper l'imputabilité et la responsabilité des différentes tâches.

Cette documentation devrait permettre aussi d'identifier les parties intéressées devant être consultées et informées lors de l'élaboration et la mise en œuvre des pratiques de gouvernance TIC afin de favoriser la transparence et la collaboration au sein de la culture d'entreprise.

Le conseil d'administration

L'Autorité s'attend que le mandat du conseil d'administration fasse notamment mention des rôles et des responsabilités propres aux TIC et aux innovations liées aux TIC attribuées aux membres qui le composent. En regard des rôles et responsabilités qui lui sont habituellement dévolus, le conseil d'administration devrait notamment :

- veiller à ce que l'institution financière agisse en conformité avec les lois, règlements et normes applicables, dont la *Loi sur la protection des renseignements personnels dans le secteur privé* et la *Loi concernant le cadre juridique des technologies de l'information*;
- veiller à ce que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement organisationnel éthique. L'exploitation des données massives rendues possibles à l'aide des nouvelles technologies pourrait accroître les risques de comportement non éthique dans les institutions.

Il importe d'assurer que le conseil d'administration ait une compréhension claire de l'importance stratégique des TIC de même que des risques liés à l'utilisation des TIC et de ses données.

À l'égard des responsabilités pour la gestion des risques TIC, le conseil d'administration devrait notamment considérer les actions suivantes :

- examiner les encadrements liés aux TIC, incluant les éléments de reddition de compte, afin d'évaluer leur pertinence et exhaustivité;
- examiner les hypothèses et les analyses étayant la détermination des risques principaux liés aux TIC ;
- examiner les catégories de risques liés aux TIC auxquels fait face l'institution, les interrelations entre les risques, leur probabilité d'occurrence, leur impact potentiel et les mesures d'atténuation et plans d'action, le cas échéant.

En matière de sécurité de l'information de l'institution financière, le conseil d'administration devrait s'assurer que :

- l'institution maintienne une sécurité qui soit proportionnelle à l'ampleur et l'étendue des menaces qui pèsent sur ses actifs informationnels et qui permet le bon fonctionnement de l'institution;
- les contrôles déployés pour protéger les actifs informationnels soient proportionnels à la criticité et la sensibilité de ses actifs;
- l'institution entreprenne des régimes d'essais systématiques et obtienne des assurances à l'égard de l'efficacité de ses contrôles;
- les rôles et responsabilités des instances décisionnelles (incluant les comités, groupes de travail et forums) et autres individus clés responsables de la prise de décision, approbation, surveillance et opérations des fonctions de sécurité de l'information soient clairement définis.

L'autoévaluation pratiquée par le conseil d'administration de façon courante sur l'ensemble de son mandat devrait également porter sur la connaissance et la compréhension des risques TIC de l'institution.

Le conseil d'administration devrait régulièrement s'assurer de l'évaluation de la conformité de l'institution à son cadre de gouvernance des TIC. Aussi, il devrait s'assurer que la fonction de conformité[9] rende compte des résultats significatifs découlant de la vigie à l'égard des TIC et des lois, projets de lois ou règlements nationaux et internationaux les encadrant, et revoir les risques émergents de non-conformité liés à ses activités.

D'autre part, il est attendu que le comité d'audit s'assure aussi de l'efficacité des processus de gouvernance, de gestion de risques et de contrôles internes liés aux TIC.

Plusieurs tâches de gestion des TIC requièrent des prises de position et des décisions provenant des secteurs d'affaires. Aussi, différents aspects de la gouvernance des TIC peuvent être entrepris par la direction si les responsabilités et l'autorité appropriées leur ont été assignées par le conseil d'administration.

La haute direction

Les membres de la haute direction sont responsables de l'atteinte des objectifs stratégiques organisationnels. Ils sont responsables de l'évaluation des risques TIC et de la mise en œuvre du système de contrôle interne approprié. D'une manière générale, la haute direction exerce l'ensemble des fonctions liées à la gestion des TIC et au bon fonctionnement de l'institution d'une manière qui soit cohérente avec la stratégie, l'appétit et les niveaux de tolérance aux risques liés aux TIC et les différentes politiques approuvées par le conseil d'administration.

En sus des rôles et responsabilités qui leur sont généralement dévolus, la haute direction devrait notamment :

- produire une vue holistique de l'environnement TIC et affaires, la vision future et les initiatives requises pour y migrer (Section 1.6);
- s'assurer de la disponibilité de connaissances pertinentes, courantes et fiables pour supporter les processus et faciliter la prise de décision liée aux TIC ainsi que de l'identification, du rassemblement, de l'organisation, du maintien, de l'utilisation et de l'évaluation du degré de désuétude desdites connaissances;
- s'assurer de recueillir et évaluer les indicateurs et les objectifs TIC et d'affaires en plus de s'assurer que les processus sont conformes aux objectifs et indicateurs définis et que les rapports sont produits en temps opportun et de manière systématique;

[9] Lorsqu'il est fait mention de la fonction de conformité, il peut s'agir de toute autre fonction de supervision indépendante de la deuxième ligne de défense.

- surveiller et évaluer en continu, en collaboration avec les fonctions de conformité et d'audit interne[10], l'environnement de contrôle (les autoévaluations, les revues d'assurance, l'identification des déficiences dans les contrôles, la conformité des processus supportés par les TIC aux lois, règlements et obligations contractuelles, etc.);
- s'assurer de créer un environnement propice à maintenir la sensibilisation aux TIC, à identifier les opportunités liées aux TIC existantes et émergentes et à influencer la planification stratégique et les décisions d'architecture d'entreprise;
- gérer la relation entre les services informatiques et les unités d'affaires de manière formelle et transparente et en utilisant un langage commun pour assurer l'atteinte conjointe des objectifs stratégiques;
- s'assurer de l'établissement d'une vision pour l'architecture d'entreprise comprenant les processus, informations, données et couches d'architectures d'applications et de technologies;
- s'assurer de la réalisation des stratégies TIC et d'affaires par la création de modèles et de pratiques qui décrivent les architectures courantes et visées.

Dans le cadre de la gestion intégrée des risques liés aux TIC, la haute direction de l'institution financière devrait notamment :

- aligner la gestion des risques TIC aux objectifs de création et de préservation de valeur de l'institution ainsi qu'aux processus d'affaires ou secteurs particuliers où ces risques sont les plus susceptibles de se matérialiser;
- évaluer et s'assurer de tenir compte de l'incidence potentielle des risques TIC identifiés sur les stratégies, la conformité de l'institution et l'intégrité de l'information financière.

Le chef de la gestion des risques[11] est responsable du développement, de l'implantation et de la coordination de la stratégie de gestion des risques liés aux TIC. Dans cette optique, Il devrait être en mesure de synthétiser, vulgariser et de communiquer efficacement l'information liée aux TIC auprès de divers auditoires.

1.3 Rôles des lignes de défense

Les directions opérationnelles constituent la première ligne de défense responsable de la gestion quotidienne des risques liés aux TIC. Ils doivent détecter et signaler les expositions inhabituelles aux risques en tenant compte des niveaux de tolérance aux risques liés aux TIC de l'institution et des politiques, limites et contrôles en la matière.

---

10 Lorsqu'il est fait mention de la fonction d'audit interne, il peut s'agir de toute autre fonction d'évaluation indépendante désignant la troisième ligne de défense.

11 À défaut de l'existence d'un tel poste, d'une personne détenant un niveau d'autorité suffisant pour assurer son indépendance et disposant des pouvoirs et des ressources nécessaires, en fonction de la nature, de la taille et de la complexité de l'institution, afin d'accomplir son mandat adéquatement cette responsabilité devrait être confiée à un membre de la haute direction.

La fonction de gestion des risques liés aux TIC

La fonction de gestion des risques de l'institution financière devrait prendre en charge tout autant les dimensions opérationnelles que stratégiques des risques et innovations liés aux TIC.

Cette fonction devrait assurer un suivi rigoureux des risques importants ainsi qu'une veille des risques émergents liés aux TIC de façon intégrée et en continu.

Les préceptes de la gestion des risques liés aux TIC sont abordés à la section 2.

La fonction de conformité

La fonction de conformité devrait établir des politiques et des procédures de gestion de la conformité à l'égard des exigences légales, réglementaires et normatives encadrant l'utilisation, la propriété, l'opération et l'adoption des TIC dans l'ensemble de ses activités de l'institution et d'en assurer la mise à jour périodique. L'Autorité considère d'ailleurs que le cadre et ses principes devraient s'arrimer au cadre global de la gestion des risques.

L'audit interne

La fonction d'audit interne indépendante devrait être en mesure de fournir une assurance objective quant à l'efficacité de la gouvernance des TIC, des processus de gestion des risques liés aux TIC et de la conformité et des mécanismes de contrôle interne et leur adéquation avec les activités de l'institution financière.

Selon une approche axée sur les risques, cette assurance, balisée par les normes en la matière, devrait notamment couvrir l'efficience et l'efficacité des opérations TIC, la protection des actifs informationnels, la fiabilité et l'intégrité des processus de divulgation et la conformité aux lois, règlements, normes, procédures et contrats pour l'ensemble de l'institution financière.

Les activités d'audit interne de l'institution devraient comprendre la revue de la conception et de l'efficacité des contrôles de sécurité de l'information, incluant ceux maintenus par les parties externes. L'audit interne devrait aussi évaluer l'assurance des contrôles de sécurité de l'information lorsqu'elle est produite par une partie externe et qu'elle a le potentiel de nuire à l'institution, à sa clientèle ou à d'autres parties intéressées.

1.4 Structures de gouvernance des TIC

L'Autorité s'attend à ce que l'institution évalue régulièrement les structures, rôles et fonctions de support afin de permettre le développement et l'amélioration continue de sa gouvernance des TIC.

Dans cette perspective, l'institution financière devrait s'assurer :

- que les parties intéressées à la gouvernance des TIC ainsi que leurs rôles et responsabilités (section 1.2) soient revus et clairement identifiés;

- que l'autorité, les droits et les frontières relatives à la prise de décision soient établis et arrimés entre les différentes structures et rôles choisis et que des procédures d'escalade soient mises en place en cas de problèmes dans la prise de décision;
- que la structure au niveau du conseil d'administration[12] permette de se concentrer adéquatement sur l'ensemble des enjeux de l'institution liés aux TIC;
- de l'assignation d'un responsable à la haute direction, tel un chef des technologies ou de l'information[13], ou autre, pour la présentation au conseil d'administration des propositions technologiques et des statuts de la mise en œuvre des stratégies et encadrements liés aux TIC;
- de la surveillance par un responsable à la haute direction, tel un chef de la sécurité de l'information[14], ou autre, du déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques de l'institution;
- de la surveillance par un responsable à la haute direction, tel un chef des données[15], ou autre, de l'encadrement approuvé par le conseil d'administration à l'égard de la collecte, l'emmagasinage et l'utilisation des données à travers l'institution;
- de la gestion par un comité exécutif des enjeux opérationnels liés à la mise en œuvre des stratégies et encadrements approuvés par le conseil d'administration liés aux TIC;
- de l'assignation, parmi la haute direction, de propriétaires pour l'ensemble des différents risques TIC présents dans l'institution.

L'institution financière devrait de plus s'assurer :

- de la gestion par un comité, tel un comité des risques ou un comité technologique exécutif[16], constitué de membres de la haute direction, de la surveillance et la gestion des risques stratégiques liés aux TIC à travers l'institution;
- de l'assignation d'un responsable à la haute direction pour la mise en œuvre de l'encadrement touchant la gestion des coûts et bénéfices liés aux TIC;
- de l'assignation de responsables parmi les différents secteurs de l'institution pour identifier, évaluer et rapporter les risques liés aux TIC;
- de l'assignation de gestionnaires responsables pour l'exécution des programmes de changement identifiés dans les plans stratégiques;
- de s'assurer de l'établissement d'une vision pour l'architecture d'entreprise comprenant les processus, informations, données et couches d'architectures

12 L'absence d'une structure adéquate expose l'institution à des risques stratégiques technologiques significatifs.

13 Ce poste porte parfois aussi le nom de *Chief Technology Officer* (CTO) ou *Chief Information Officer* (CIO).

14 Ce poste porte parfois aussi le nom de *Chief Information Security Officer* (CISO).

15 Ce poste porte parfois aussi le nom de *Chief Data Officer* (CDO).

16 Ce comité porte parfois le nom de Comité directeur technologique ou d'*IT Steering Committee*.

d'applications et de technologies en effectuant le pont entre le conseil d'administration et la haute direction;

- de la surveillance par un responsable du développement de l'architecture technologique de l'institution et de son intégration à l'architecture d'entreprise.

Les rôles d'ingénierie et d'architecture dans le développement d'une sécurité de l'information adéquate pour les systèmes TIC de l'institution devraient être accompagnés d'une ségrégation adéquate entre la sécurité opérationnelle et la gestion des risques.

D'autres rôles définis à travers l'institution peuvent avoir un effet sur la gouvernance et la gestion des risques TIC. Ils ne sont pas directement liés à la gestion des risques TIC, mais ils sont des parties intéressées de ce processus. Il peut s'agir, par exemple, des propriétaires des processus d'affaires et TIC, du responsable de la continuité des affaires, du responsable des ressources humaines et l'approvisionnement.

Le conseil d'administration et la haute direction sont les mieux placés pour s'assurer que les lignes de défense propres aux TIC sont bien représentées dans le système de gestion des risques et les processus de contrôle. Ils ont la responsabilité et l'imputabilité collectives d'établir les objectifs d'affaires (incluant les objectifs liés aux TIC qui en découlent) de l'institution. Ils sont aussi responsables de définir les stratégies, d'établir les structures requises pour la meilleure gestion des risques liés aux TIC et de communiquer le ton établi au sommet de l'institution notamment en prônant la transparence et la collaboration entre les parties intéressées à la gouvernance des TIC.

1.5 Préceptes et propriétés du cadre de gouvernance des TIC

Préceptes

L'Autorité s'attend à ce que l'institution financière identifie les préceptes fondamentaux d'une saine gouvernance des TIC applicables à son environnement et les actions requises au développement et déploiement de l'ensemble d'entre eux.

Une saine gouvernance des TIC repose sur la définition et l'utilisation des préceptes fondamentaux pouvant aider le conseil d'administration à comprendre, remplir et communiquer les obligations légales, réglementaires et éthiques à l'égard de l'utilisation des TIC au sein de l'institution financière.

Ces préceptes fondamentaux d'une saine gouvernance des TIC expriment les comportements souhaités afin de guider la prise de décision. Les énoncés de ces préceptes font référence à ce qui devrait se produire sans prescrire le comment ni le moment. Ils devraient être rédigés d'une façon assimilable par l'ensemble des lecteurs visés, incluant le conseil d'administration et la haute direction.

Les préceptes fondamentaux suivants devraient être considérés pour une saine gouvernance des TIC :

- Responsabilité : Les individus et les groupes au sein de l'institution comprennent et acceptent leurs responsabilités à l'égard de la demande et l'utilisation des TIC et l'utilisation des données.

- Acquisition : L'acquisition des TIC est justifiée, basée sur des analyses continues et pertinentes dans le cadre d'un processus décisionnel clair et transparent. Les décisions sont basées sur un équilibre approprié entre les bénéfices, les coûts, les opportunités et les risques à court, moyen et long terme.

- Performance : Les TIC sont adaptées aux besoins de support actuels et futurs de l'institution en fournissant la qualité et les niveaux de services requis.

- Conformité : L'utilisation des TIC est conforme aux lois et règlements. Les encadrements et les pratiques sont clairement définis, déployés et appliqués.

- Comportement humain : Les encadrements, pratiques et décisions liées aux TIC démontrent le respect des comportements humains et l'évolution de ces comportements pour l'ensemble des individus impliqués dans les activités.

Il est de la responsabilité de chaque institution d'identifier les actions requises pour le déploiement de ces préceptes en fonction de sa nature et des analyses de risques et opportunités liées aux TIC. Plusieurs actions devraient aussi être considérées pour l'élaboration de ces préceptes à l'égard de la gouvernance des TIC et des données. Notamment, le conseil d'administration devrait :

- s'assurer que les responsabilités couvrent le cycle de vie des données;
- s'assurer de l'évaluation de la compétence des individus clés responsables de la prise de décision à l'égard des TIC;
- évaluer les TIC et leurs activités, lors de l'étude des plans et politiques, afin de s'assurer qu'elles sont alignées aux objectifs de l'institution, qu'elles considèrent les bonnes pratiques et qu'elles répondent aux besoins des parties intéressées clés;
- s'assurer que l'institution et ses fournisseurs développent une compréhension commune du processus d'acquisition des TIC;
- évaluer les plans de l'institution pour assurer que les TIC supporteront les processus d'affaires avec la capacité requise;
- évaluer la mesure dans laquelle les TIC répondent aux obligations réglementaires, légales, contractuelles ainsi qu'aux standards et normes professionnelles et internationales.
- évaluer régulièrement la conformité de l'institution à son cadre de gouvernance des TIC, tel que le suivi approprié aux encadrements sur l'exactitude des données et l'efficacité des TIC;

- évaluer les activités liées aux TIC et s'assurer que les comportements humains sont identifiés et considérés adéquatement, qu'ils demeurent pertinents et qu'une attention appropriée leur soit apportée.

De plus, de manière plus spécifique, les préceptes fondamentaux suivants contribuent à une saine gouvernance de la sécurité de l'information et devraient être pris en considération, soit :

- s'assurer d'établir la sécurité de l'information à travers toutes les activités de l'institution incluant l'information traitée chez les parties externes au périmètre de l'institution;
- adopter une approche basée sur l'appétit pour le risque de l'institution incluant la perte de compétitivité, la conformité, les interruptions opérationnelles, l'impact sur la réputation et les pertes financières;
- assurer la conformité avec les exigences internes et externes par le biais d'audits de sécurité indépendants;
- cultiver un environnement favorable à la sécurité en coordonnant les activités des parties intéressées afin d'obtenir une direction cohérente pour la sécurité de l'information et supporter la livraison des programmes d'éducation, de formation et de sensibilisation en sécurité;
- revoir la performance de la sécurité en termes d'impacts sur l'institution et non seulement sur la base de l'efficacité des contrôles de sécurité.

Enfin, certains préceptes additionnels guidant la mise en place d'une architecture d'entreprise pour l'utilisation des ressources TIC au sein de l'institution devraient aussi être considérés et définis. Parmi eux, l'agilité permettant une adaptation rapide à des besoins changeants et l'ouverture face à l'exploitation des standards internationaux.

Propriétés

Il est du ressort de l'institution de définir la forme de son cadre de gouvernance des TIC en fonction de sa nature, sa taille, la complexité de ses activités et son profil de risque.

Par contre, certains éléments clés devraient être considérés, comprenant :

- l'intégration de la capacité actuelle et future des TIC dans les processus de planification d'affaires pour assurer que les plans stratégiques TIC répondent aux stratégies d'affaires;
- la mise en place et la reconnaissance de mécanismes pour assurer que les individus portant des responsabilités aient aussi le devoir d'en rendre compte.

Le cadre de gouvernance d'une institution financière devrait également refléter les changements qui s'opèrent au fil du temps. La qualité des pratiques de gouvernance est un facteur important au maintien de la confiance des marchés. À cet égard, celles-ci devraient évoluer de façon à refléter les nouvelles façons de faire, notamment en lien avec les technologies, et les meilleures pratiques de l'industrie. Ainsi, le cadre de gouvernance des TIC devrait tenir compte des bonnes pratiques reconnues par les cadres de

gouvernance et gestion des données professionnels et internationaux existants[17] et de gouvernance de la sécurité de l'information (incluant la cybersécurité) et s'aligner avec les objectifs d'affaires de l'institution.

Les divers éléments de l'encadrement des TIC devraient considérer et arrimer entre eux toutes dispositions inhérentes et utiles à la gestion des risques technologiques, dont notamment celles portant sur :

- la gestion des risques liés aux TIC;
- la sécurité de l'information;
- la gestion de crise;
- l'infogérance;
- la continuité des activités;
- la gestion des programmes/projets/changements;
- les ressources humaines;
- l'éthique;
- la propriété intellectuelle;
- la protection des renseignements personnels.

De plus, en raison des changements rapides dans les environnements opérationnels et de sécurité des TIC, l'institution devrait revoir et mettre à jour régulièrement son encadrement et s'assurer que les changements soient pris en charge par les processus de conformité vérifiant leur application et gérant tout écart de conformité.

1.6 Documentation de l'environnement des TIC

L'Autorité s'attend à ce que l'institution documente en continu son environnement technologique pour consultation par les parties intéressées à la gouvernance des TIC.

La documentation favoriserait l'établissement et le maintien d'une compréhension claire de l'importance stratégique et des risques liés à l'utilisation des TIC et des données de l'institution et contribuerait à la prise de décision.

Ainsi, elle pourrait regrouper des informations qui reflètent l'état de la stratégie TIC, l'architecture actuelle et ciblée, les objectifs et risques TIC stratégiques, les plans et leurs états courants, les énoncés d'impact des risques liés aux TIC et les processus et structures existantes pour leur gestion, sa méthodologie de développement et les processus d'opérations.

[17] Parmi eux, il y a notamment ceux produits par les organisations NIST, Cobit, ITIL et ISO.

L'Autorité s'attend à ce que l'institution financière maintienne une connaissance de ses systèmes, ses actifs, ses données, de leur circulation dans l'institution ainsi que de ses capacités. Le regroupement, et surtout le maintien de cette documentation, devrait contribuer au développement optimal des stratégies technologiques et d'affaires. L'incapacité de créer une base solide d'informations pour la prise de décision stratégique est en soi un risque de gouvernance stratégique.

Cette documentation ne devrait jamais être statique, mais plutôt changer dans le temps. Tout comme les affaires, les TIC de l'institution sont en perpétuel changement et évoluent au rythme des acquisitions, des mises à jour et des changements externes tels que les cyberrisques.

Cette documentation devrait contenir suffisamment d'informations agrégées pour faciliter la prise de décision concernant la stratégie TIC.

Les encadrements de l'institution devraient préciser les rôles et les responsabilités des instances décisionnelles et des unités opérationnelles à l'égard de l'établissement, du maintien et de la consultation de cette documentation.

Bien que la documentation puisse être préparée et maintenue par diverses composantes de l'institution, les éléments clés devraient toutefois être autorisés par la haute direction et approuvés par le conseil d'administration et constituer une source autoritaire pour la prise de décision et particulièrement, les décisions stratégiques.

Parmi les documents stratégiques qui sont issus des meilleures pratiques, l'institution pourrait considérer notamment :

- la description des contextes auxquels fait face l'institution, les lignes d'affaires et les fonctions de support;
- les composantes de la stratégie TIC, son plan stratégique et son statut;
- la description des risques TIC sur les stratégies d'affaires;
- l'architecture stratégique actuelle et visée des TIC;
- les modèles et processus d'opérations des TIC.

1.7 Information pour la prise de décision

L'information est un outil pour la gouvernance avec lequel les parties intéressées assument leurs rôles, accomplissent leurs tâches et interagissent entre elles. Plusieurs catégories de rôles nécessaires à la gouvernance des TIC consomment, utilisent, produisent ou protègent de l'information à la fois générale ou spécifique. Ces informations peuvent prendre une forme physique, empirique, sémantique, pragmatique et même sociale. Leur utilisation varie selon le cycle de vie de l'information. Parmi les différents éléments d'information soutenant une saine gouvernance et gestion des risques liés aux TIC que l'institution devrait considérer dans ses pratiques, il y a notamment :

- le profil de risque;
- la taxonomie et le registre (ou univers) des risques;

- la matrice des risques et contrôles (incluant scénario et évaluation de risque);
- le rapport de risque;
- l'architecture d'entreprise définissant les différents points de vue (ou perspectives) permettant de répondre aux besoins des différentes parties intéressées et ses documents décrivant les éléments constitutifs des services (applications, technologies, infrastructures et autres).

2. L'identification et la gestion des risques liés aux technologies

L'Autorité s'attend à ce que l'institution financière identifie, évalue et mitige les risques TIC à l'intérieur des seuils de tolérance établis.

La gestion des risques TIC devrait faire partie intégrante de la gestion intégrée des risques de l'institution.

À cette fin, des mécanismes devrait être mis en œuvre afin de :

- collecter des données pertinentes à l'identification, l'analyse et la reddition des risques TIC;
- développer des informations utiles pour supporter la prise de décision;
- maintenir un registre des risques TIC connus, leurs attributs et activités de contrôles;
- produire de l'information sur l'état courant du risque en temps opportun pour les parties intéressées;
- gérer les opportunités de réduire le risque à un niveau acceptable comme un portefeuille;
- répondre en temps opportun à l'aide de mesures efficaces pour limiter l'amplitude des pertes liées aux évènements impliquant les TIC.

2.1 Les types de risques liés aux technologies

L'Autorité s'attend à ce que l'institution mette en place une taxonomie[18] qui lui est propre afin de s'assurer que tous les types de risques liés aux TIC soient considérés, permettant ainsi d'en faciliter l'agrégation et de contribuer à l'établissement d'une vue holistique.

Régulièrement, le risque lié aux TIC est considéré comme une composante du risque opérationnel. Toutefois, même les risques stratégiques et de réputation peuvent comporter une composante liée aux TIC, particulièrement lorsque celles-ci permettent la réalisation d'initiatives d'affaires. C'est aussi le cas pour le risque de crédit, où une faible sécurité des TIC peut mener à des cotes de crédit erronées.

La gestion des risques technologiques devrait avoir un caractère prospectif et prendre en considération tant les dimensions opérationnelles que stratégiques des risques technologiques omniprésents dans l'ensemble des processus des institutions financières.

[18] L'Autorité reconnaît qu'il n'y a pas de taxonomie universelle pour les risques. D'ailleurs, il n'existe pas de taxonomie définitive des risques dans la réglementation financière autre que la classification générique recommandée par l'Accord de Bâle II pour les institutions de dépôt.

Notamment, au-delà des risques opérationnels liés aux technologies, les risques stratégiques suivants, qui peuvent entraver l'atteinte des stratégies d'entreprises par les conseils d'administration, devraient être pris en considération :

- Le risque de positionnement technologique
    - Le risque qu'au moment de la définition de la stratégie, la position technologique visée au sein de l'industrie ne soit pas enchâssée adéquatement dans la stratégie d'affaires, ne soit pas viable (en termes de modèle d'affaires et modèle technologique et d'objectifs stratégiques) ou ne soit pas réalisable (en termes de plan d'exécution stratégique TI).
- Le risque d'exécution technologique
    - Le risque que, dans l'exécution de sa stratégie et de son plan stratégique, le conseil d'administration n'atteigne pas les objectifs TI stratégiques désirés ainsi que les objectifs d'affaires associés.
- Le risque de gouvernance technologique
    - Le risque que le conseil d'administration ne parvienne pas à mettre en place les éléments nécessaires (politiques, processus, etc.) pour gouverner le développement et l'exécution de sa stratégie TI.

La taxonomie de l'institution devrait être adaptée à sa situation afin d'en faciliter l'agrégation et de contribuer à l'établissement d'un portrait complet. Ainsi, cette taxonomie devrait présenter un caractère exhaustif des risques liés aux TIC permettant aux responsables de l'identification des risques d'envisager tous les types de risques susceptibles d'avoir des répercussions sur les objectifs de l'institution.

L'institution devrait considérer le risque technologique de manière holistique en considérant tout autant les risques courants que les risques de ne pas répondre adéquatement aux changements ou à l'arrivée de technologies nouvelles ou émergentes afin d'accroître son agilité et sa capacité de répondre au changement avec le temps.

Dans l'élaboration de sa taxonomie de risques, l'institution devrait tenter d'établir un nombre raisonnable de catégories qui permettent à la fois de regrouper adéquatement les risques sans pour autant affaiblir le caractère particulier de chaque catégorie. Dans l'éventualité où une institution dispose déjà d'une taxonomie des risques dans un secteur fonctionnel donné, par exemple l'audit interne, il serait souhaitable d'en tenir compte dans l'élaboration d'une taxonomie des risques organisationnels, car elle peut contenir des catégories dont l'application à l'échelle de l'institution est éprouvée. Une fois développée, cette taxonomie devrait être communiquée à l'ensemble de l'institution afin d'assurer une utilisation cohérente dans l'identification et l'agrégation des risques TIC.

2.2 Tolérance pour le risque TIC

L'Autorité s'attend à ce que l'institution financière établisse et maintienne un énoncé global décrivant qualitativement et quantitativement son niveau de tolérance pour le risque TIC. Elle s'attend également à ce que l'institution définisse clairement ses niveaux de tolérance aux risques les plus importants et s'assure de les intégrer dans ses opérations, en lien avec ses politiques et procédures de gestion de risques.

L'appétit pour le risque est en lien étroit avec la stratégie d'affaires de l'institution. L'énoncé de l'appétit pour le risque devrait comporter des informations d'ordre qualitatif permettant de situer les risques TIC ciblés ainsi que le comportement désiré de l'institution selon une variété de scénarios. L'énoncé devrait également comporter quelques objectifs ou limites d'ordre quantitatif, exprimés en fonction des revenus, du capital ou de toute autre mesure jugée pertinente.

Tel que souligné précédemment, le conseil d'administration et la haute direction sont les mieux placés pour diffuser le ton établi au sommet. Ils devraient communiquer régulièrement le niveau de tolérance établi pour le risque TIC afin de faciliter son intégration dans les opérations et encourager l'innovation technologique.

L'autorité s'attend à l'évaluation de l'adéquation des ressources avec l'appétit pour le risque par des exercices de simulation de crise pour l'ensemble des risques matériels et probables, classifiés selon leur probabilité et leur impact (p. ex. : les risques TIC, dont le cyberrisque).

2.3 Attributs du cadre de gestion des risques liés aux technologies

L'Autorité s'attend à ce que l'institution effectue une gestion intégrée de ses risques TIC soutenue par une solide structure de gouvernance, des stratégies, politiques et procédures lui permettant d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et de suivre adéquatement les risques importants.

L'Autorité considère en outre que l'institution financière devrait tendre vers une gestion intégrée de ses risques TIC par opposition à une approche où les risques sont considérés séparément. Ainsi, les risques jugés moins importants, mais qui pourraient le devenir une fois combinés, devront aussi être pris en compte. Une approche holistique où l'interrelation et l'interdépendance entre les risques sont considérés permettrait de mettre en lumière des aspects importants susceptibles d'influencer le niveau des risques réellement assumés par l'institution. Par exemple, certains risques liés à une ségrégation inadéquate des accès logiques aux systèmes informatiques, et qui sont la conséquence de lacunes de gouvernance en sécurité de l'information, apparaissent plus clairement lorsqu'ils sont consolidés à l'échelle de l'institution.

Cette façon de faire permet également de mieux prendre en compte les risques plus difficilement quantifiables sur la base des méthodes habituellement utilisées. Certains

risques opérationnels, le risque stratégique et le risque de réputation sont de bons exemples de tels risques.

Par ailleurs, un cadre de gestion intégrée des risques accroît l'efficacité du traitement des impacts en cascade pour les risques à conséquences multiples. Les risques liés à l'utilisation des technologies, compte tenu de leurs nombreuses ramifications, constituent de bons exemples : interruption des opérations, pertes de données, vols d'identités, cyber attaques, atteinte à la réputation, poursuites judiciaires, etc. Dans cette optique, les stratégies, ressources, technologies et connaissances doivent être alignées pour assurer une gestion adéquate et complète de ces risques à travers toute l'institution.

L'institution devrait être en mesure de saisir l'impact du risque technologique sur les opérations, incluant la mission, les fonctions ou la réputation, ainsi que sur les actifs et individus. En conséquence, l'institution devrait avoir une approche intégrée pour identifier, évaluer, contrôler et gérer le risque technologique. Cette approche devrait être appliquée à l'échelle de l'institution et devrait permettre notamment :

- d'assurer un suivi adéquat et en temps opportun des activités de mitigation des risques présents au registre de risques des TIC. Le registre de risque lié aux TIC, mis à jour régulièrement de manière prospective et non rétrograde, pourrait par exemple, comporter une liste des attributs des risques liés aux TIC connus et potentiels susceptibles d'affecter l'institution et produire en temps opportun l'information utile pour fins de réduction des risques pour l'ensemble des parties intéressés;
- d'assurer un alignement de l'ensemble des outils d'évaluation des risques utilisés afin de ne pas entraver la production d'une vue holistique des risques liés aux TIC à travers l'institution;
- d'utiliser un processus de gestion des actifs informationnels[19] exhaustif afin de permettre de leur associer les risques de manière holistique;
- d'exploiter un cadre de classification[20] des données et des actifs informationnels, incluant ceux qui sont gérés par des parties externes, et des procédures établies et déployées et permettant d'établir des vues holistiques des systèmes clés;
- d'utiliser des processus de gestion d'incidents, dotés d'objectifs de reprise et recouvrement adéquats et permettant la proactivité dans la gestion des risques.

L'institution devrait réaliser des évaluations des risques liés aux TIC à des intervalles planifiés ou lorsque des changements significatifs sont prévus ou ont lieu en tenant

---

19 Les vulnérabilités des actifs de l'institution devraient être recensées et documentées. Il en est de même des menaces internes et externes et des probabilités et impacts d'affaires potentiels afin de déterminer le niveau de risque et établir les plans d'action adéquats. Aussi, la conduite de ces activités devrait bénéficier de toutes les informations disponibles, notamment l'intelligence existante sur les cybermenaces.

20 Cette classification devrait refléter la mesure dans laquelle un incident de sécurité de l'information affectant un actif informationnel a le potentiel de nuire, à l'institution, à sa clientèle ou à d'autres parties intéressées.

compte de critères établis. L'évaluation des risques liés aux TIC devrait s'inscrire dans un processus systématique et cyclique permanent[21].

L'institution devrait démontrer qu'elle a évalué les risques associés à l'entretien continu de ses systèmes hérités et que des contrôles adéquats sont déployés pour gérer efficacement les risques de ces technologies. Si ces systèmes hérités supportent des opérations critiques, l'institution devrait avoir en place une stratégie pour gérer l'infrastructure vieillissante incluant l'évaluation d'investissements additionnels ou la transition dans le temps vers des technologies de nouvelle génération.

Toutes les composantes matérielles et logicielles du modèle TIC de l'institution ont une durée de vie utile, et le conseil d'administration devrait être au fait des risques du non-renouvellement dans un délai raisonnable de ces systèmes.

Aussi, l'institution devrait notifier l'Autorité lorsqu'elle devient consciente qu'un incident lié aux TIC pourrait avoir un impact significatif et dommageable sur sa capacité à fournir des services adéquats à ses clients, sur sa réputation ou sur sa condition financière.

En plus de l'évaluation du risque technologique de ses activités, de ses produits et de ses services (incluant particulièrement l'évaluation du cyberrisque), l'institution devrait considérer l'impact qu'il représente sur ses partenaires, fournisseurs, clients, voire même, sur les autres participants du secteur financier.

Parmi ses pratiques de gestion, l'institution financière devrait soumettre ses contrôles à des revues indépendantes périodiques et, selon sa nature, sa taille et la complexité de ses activités, à des tests d'intrusions[22]. À l'égard de la sécurité de l'information, l'efficacité des contrôles devrait être testée à l'aide d'un programme systématique proportionnel au rythme de changement des menaces et vulnérabilités, à la criticité et la sensibilité des actifs informationnels, aux conséquences d'un incident de sécurité de l'information et à la matérialité et la fréquence des changements à ses actifs informationnels.

Les détails des constats majeurs issus des revues devraient faire l'objet d'une reddition auprès du conseil d'administration et les lacunes identifiées, être corrigées dans un délai convenable.

Dans l'évaluation des risques de la sécurité de l'information, l'institution devrait notamment :

- identifier les risques de sécurité de l'information liés à la perte de confidentialité, d'intégrité et de disponibilité des informations et identifier les propriétaires des risques;

---

21 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES. *Gestion du risque numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et document d'accompagnement*, 2015.

22 Les tests d'intrusions et les évaluations de vulnérabilités produisent une image d'un système informatique dans un état et à un moment spécifique. Cette image est limitée aux portions du système qui est testé durant les tentatives d'intrusion. Dans cette perspective, les tests d'intrusion et les évaluations de vulnérabilités ne sont pas des substituts pour l'évaluation des risques TIC.

- établir et tenir à jour les critères de risque de sécurité de l'information incluant les critères d'acceptation des risques et les critères de réalisation des évaluations des risques de sécurité de l'information.

De plus, dans le traitement des risques de sécurité de l'information, l'institution devrait notamment :

- déterminer toutes les mesures nécessaires à la mise en œuvre des options de traitement des risques de sécurité de l'information choisies;
- comparer les mesures déterminées avec les meilleures pratiques existantes et vérifier qu'aucune mesure nécessaire n'a été omise;
- produire une déclaration d'applicabilité contenant les mesures nécessaires et la justification de leur insertion, le fait qu'elles soient mises en œuvre ou non et la justification de l'exclusion de mesures;

L'institution financière devrait maintenir activement la sécurité de son information en considérant les changements aux menaces et vulnérabilités incluant celles résultant des changements à ses actifs informationnels, le stade auquel ils sont dans leur cycle de vie[23] et son environnement d'affaires.

L'institution devrait conserver des informations documentées sur les processus d'évaluation et de traitement des risques de sécurité de l'information.

Dans l'évaluation des risques et des contrôles, les mécanismes de protection peuvent inclure l'évitement ou l'élimination du risque en ne s'engageant pas dans une activité identifiée. Ils peuvent aussi inclure l'atténuation du risque à travers les contrôles ou le partage ou transfert du risque. Notamment, l'institution pourrait considérer prendre une couverture d'assurance pour différents risques incluant les coûts de recouvrement et de rétablissement.

L'institution devrait de plus procéder à l'évaluation en continu du cadre de gestion des risques TIC à partir d'objectifs d'évaluation clairs, d'attentes et de méthodologies établies et diffusées aux parties intéressées et de comptes rendus comportant des conclusions claires et des actions correctives concrètes. Cette façon de faire implique également une documentation agrégée et synthétisée des constats et des décisions (sections 1.6 et 1.7) émanant de l'application du cadre de gestion des risques TIC et des exercices de simulations de crise (p. ex. : les ajustements apportés à l'énoncé de l'appétit pour le risque TIC et au plan stratégique). L'Autorité pourrait, si elle le juge opportun, fournir des attentes plus précises en matière de documentation nécessaire pour supporter le cadre de gestion du risque TIC.

[23] Ceci fait référence au processus traitant de la planification et conception des actifs informationnels jusqu'à leur déclassement et élimination.

2.4 L'agrégation des risques liés aux technologies

La gestion des risques liés aux TIC ne peut atteindre son plein potentiel que dans la mesure où le risque est géré à travers l'institution. La vue agrégée des risques liés aux TIC, au-delà des enjeux techniques, est essentielle afin de prévenir un faux sentiment de sécurité ou d'urgence de même qu'à une définition optimale de la tolérance au risque TIC.

Afin de contribuer à une saine agrégation des risques TIC, l'institution devrait notamment :

- s'assurer de l'utilisation d'une terminologie TIC claire et constante dans l'ensemble de l'institution;
- exploiter des données qualitatives et quantitatives ainsi que des échelles compatibles afin d'évaluer la fréquence et l'impact des risques;
- identifier les dépendances entre les risques recensés, compilés et communiqués dans la reddition afin de prévenir l'apparition de risques plus importants;
- d'assurer de l'utilisation d'approches harmonisées, constantes, convenues et communiquées auprès de toutes les parties intéressées, pour l'évaluation de la fréquence et de l'impact des scénarios de risques liés aux TIC;
- utiliser une taxonomie constante pour la description des risques (section 2.1).

Les risques liés aux TIC peuvent être agrégés selon de multiples dimensions (unités organisationnelles, types de risques liés aux TIC, processus, etc.). Ils devraient être agrégés au niveau de l'institution pour être considérés en combinaison avec tous les autres risques qui doivent être gérés.

2.5 L'impact d'affaires des risques liés aux technologies

L'Autorité s'attend à ce que l'institution utilise des méthodes permettant de faire le lien entre les scénarios de risques liés aux TIC et leurs impacts potentiels sur les affaires afin que l'ensemble des parties intéressées comprennent les effets des évènements indésirables liés aux technologies de l'information et des communications.

L'Autorité ne prescrit aucune méthode pour convertir les risques liés aux TIC en termes d'affaires appropriés. L'institution devrait choisir les méthodes en fonction des notions financières, de confidentialité, d'intégrité, de clientèle, d'avantages compétitifs et de réputation appropriées.

Les évaluations des risques liés aux TIC requièrent que les résultats produits soient exprimés en des termes d'affaires clairs et non ambigus. Aussi, une gestion efficace des risques liés aux TIC requiert une compréhension mutuelle, entre les secteurs d'affaires et technologiques, des risques qui devraient être gérés et leurs raisons sous-jacentes. Les parties intéressées à la gestion des risques liés aux TIC devraient avoir la capacité de comprendre et d'exprimer la manière dont des évènements ou incidents défavorables pourraient agir sur les objectifs d'affaires de l'institution.

3. Les pratiques de gestion des risques liés aux technologies

L'Autorité s'attend à ce que l'institution financière considère l'ensemble des pratiques de gestion des risques liés aux TIC qui ont fait leurs preuves dans l'établissement de sa gouvernance et de sa gestion des risques liés aux TIC.

Chacune des pratiques abordées dans cette section, tirées des meilleures pratiques en la matière, concourt à l'établissement d'une approche holistique de gouvernance des TIC. Ces pratiques pourraient également contribuer à développer une compréhension organisationnelle des systèmes, des actifs informationnels, des données et des capacités nécessaires à la gestion des risques liés aux TIC. De même, elles pourraient contribuer à la protection, à la détection, à la réponse et au recouvrement dans la gestion des risques liés aux TIC.

Dans la mise en place de pratiques robustes de gestion des risques à travers l'institution, cette dernière devrait aussi tenir compte de la participation des parties intéressées externes afin de voir à ce que l'information juste et pertinente à la gestion des risques soit distribuée et utilisée avant l'apparition d'incidents de sécurité.

3.1 Les pratiques d'identification

L'Autorité s'attend à ce que l'institution financière mette en place des mécanismes afin de mieux comprendre le contexte d'affaires, les ressources qui supportent les fonctions critiques et les risques liés aux TIC afin de permettre de cibler et prioriser les efforts selon les besoins d'affaires et les stratégies de gestion de risques.

Parmi ces mécanismes, il y a notamment la gestion des actifs, l'environnement d'affaires, la gouvernance des TIC, l'évaluation du risque TIC et la stratégie de gestion du risque TIC.

L'institution devrait s'assurer que les données, le personnel, les systèmes TIC (incluant ses diverses composantes matérielles et logicielles) et les locaux contribuant à l'atteinte des objectifs d'affaires, soient identifiés et gérés en assurant une cohérence à leur importance relative face aux objectifs d'affaires et stratégies de risques de l'institution.

Les rôles, les responsabilités et la gestion des risques TIC par l'ensemble des parties intéressées devraient tenir compte de la mission, des objectifs, des priorités et des activités (incluant leurs interdépendances, fonctions critiques et besoins de résilience requis pour la livraison des services critiques) de l'institution.

La gouvernance établie pour la gestion de l'ensemble des risques (stratégique, légaux, réglementaires, opérationnels, etc.), l'impact du risque TIC sur les opérations, l'image ou la réputation et la stratégie (priorités, contraintes, niveaux de tolérance et hypothèses établies) devraient être compris et considérés dans la gestion des risques TIC de l'institution.

3.2 Les pratiques de protection

L'Autorité s'attend à ce que l'institution financière mette en place des mécanismes de protection permettant d'assurer la livraison de ses services critiques.

Parmi ces mécanismes, il y a notamment la gestion des identités et des accès, la formation et sensibilisation, la sécurité des données, les procédures et processus de protection de l'information et les technologies protectrices.

L'institution devrait s'assurer que l'accès physique et logique aux actifs informationnels et aux ressources associées est limité aux utilisateurs, processus ou appareils autorisés ainsi qu'aux activités et transactions autorisées. L'institution devrait s'assurer de plus que :

- le personnel et les partenaires de l'institution reçoivent une formation à la sensibilisation à la sécurité de l'information et soit adéquatement formés pour s'acquitter de leurs tâches et responsabilités liées à la sécurité de l'information, conformément aux encadrements établis;
- les informations et les enregistrements (données) soient gérés conformément à la stratégie de gestion des risques de l'institution afin de protéger la confidentialité, l'intégrité et la disponibilité des informations;
- les encadrements de sécurité (qui traitent du but, de la portée, des rôles, des responsabilités, de l'engagement de la direction et de la coordination entre les entités organisationnelles) et les processus et les procédures qui en découlent soient maintenus et utilisés pour gérer les systèmes d'information et les actifs;
- la maintenance et la réparation des composants des systèmes TIC soient effectuées conformément aux encadrements et procédures établies;
- les solutions de sécurité technique soient gérées pour assurer la sécurité et la résilience des systèmes et des actifs, conformément aux encadrements, procédures et accords connexes.

3.3 Les pratiques de détection

L'Autorité s'attend à ce que l'institution financière mette en place des activités pour identifier l'apparition d'évènements pouvant matérialiser des risques liés aux TIC.

Ces activités contribuent à la découverte en temps opportun d'évènements potentiellement indésirables. Parmi elles, il y a notamment la détection d'évènements et d'anomalies, la surveillance en continu de la sécurité et la mise à l'essai des processus de détection.

L'institution devrait notamment s'assurer que :

- une activité anormale soit détectée en temps opportun et l'impact potentiel des évènements est compris;

- les systèmes TIC et les actifs informationnels soient surveillés à intervalles réguliers afin d'identifier les évènements de cybersécurité et de vérifier l'efficacité des mesures de protection;
- les processus et les procédures de détection soient maintenus et testés pour assurer une connaissance adéquate et opportune des évènements anormaux.

3.4 Les pratiques de réponse et de recouvrement en cas d'incident

L'Autorité s'attend à ce que l'institution financière mette en place les activités appropriées afin de prendre action suite à la détection d'un incident de cybersécurité, maintenir les plans assurant la résilience et rétablir les services affectés par un incident de cybersécurité.

Ces activités supportent la capacité de l'institution à contenir les impacts d'un incident de sécurité potentiel et accélèrent le retour aux opérations normales. Parmi elles, il y a notamment la planification des plans de réponse et de recouvrement, les communications, l'analyse, la mitigation et l'amélioration continue.

L'institution doit s'assurer notamment que :

- les processus et procédures de réponse et de récupération sont exécutés et maintenus afin d'assurer la réponse aux incidents de cybersécurité détectés et la restauration des systèmes ou des actifs;
- les activités de réponse sont coordonnées avec les parties intéressées internes et externes (p. ex., le soutien externe des forces de l'ordre);
- les activités de restauration sont coordonnées avec les parties internes et externes (p. ex., les centres de coordination, les fournisseurs d'accès Internet, les victimes et les fournisseurs);
- l'analyse est menée pour assurer une réponse efficace et soutenir les activités de rétablissement;
- des activités sont effectuées pour empêcher l'expansion d'un évènement, en atténuer les effets et résoudre l'incident;
- les activités de réponse organisationnelle sont améliorées en intégrant les leçons tirées des activités de détection/réponse actuelles et précédentes;
- la planification et les processus de rétablissement sont améliorés en intégrant les leçons apprises dans les activités futures.

3.5 Autres pratiques

Les opérations liées aux technologies

Les innovations technologiques, telles que l'infonuagique, l'Internet des objets et les mégadonnées, ont un impact significatif sur la fonction des opérations TIC, notamment au niveau des processus qui doivent être adaptés, dont la gestion des capacités et la gestion

de la sécurité, et des connaissances qui devraient être bonifiées pour opérer dans de nouveaux systèmes TIC.

Dans ce contexte, il importe que le conseil d'administration reconnaisse le rôle clé des opérations TIC dans le succès du plan stratégique TIC et que le personnel des opérations TIC ait l'information et les outils requis pour détecter tout problème qui pourrait être introduit dans les opérations des centres de traitement, des réseaux, des infrastructures de sécurité de l'information et dans le support aux utilisateurs.

Ces outils et informations devraient contribuer notamment :

- à l'identification des risques (inventaire du matériel de traitement de l'information, ressources, emplacements, etc.);
- à l'évaluation des risques (priorisation des efforts de mitigation des risques TIC);
- au déploiement des contrôles de mitigation (politiques, directives, standards, procédures, contrôles, sécurité physique et logique, gestion des données, du personnel et des changements, distribution et transmission d'information, sauvegardes, support utilisateurs, etc.);
- au suivi et à la reddition des risques (suivi de la performance, planification de la capacité, autoévaluation des contrôles).

Malgré que l'exploitation des innovations technologiques, et des complexités qu'elle entraîne puisse être facilitée par l'utilisation de plusieurs sources d'information, le conseil d'administration devrait prendre conscience que ces innovations nécessitent une gestion étroite afin de ne pas créer de risques inutiles qui pourraient avoir un impact sur l'exécution du plan stratégique.

Ainsi, en collaboration avec la haute direction, il devrait s'assurer du déploiement de processus pour évaluer et gérer l'ensemble des risques opérationnels associés à l'utilisation, la propriété, l'opération et l'adoption des TIC au sein de l'institution. Il devrait notamment :

- implanter une structure opérationnelle TIC adéquate pour supporter les activités d'affaires de l'institution;
- documenter les systèmes en place et comprendre comment ils supportent les processus d'affaires associés;
- établir et supporter un environnement de contrôle approprié à travers l'identification, l'évaluation, la gestion et le suivi des risques opérationnels liés aux TIC selon des préceptes semblables à ceux de la *Ligne directrice sur la gestion du risque opérationnel*;
- créer un environnement opérationnel physique et logique sécure;
- prévoir une continuité et résilience opérationnelle;
- prévoir une sélection, dotation, succession et formation adéquate du personnel liés aux TIC.

La continuité des activités

La gestion de la continuité[24] est une discipline en soi et va au-delà de la portée de la présente ligne directrice. Il existe de nombreux référentiels dans ce domaine, qui définit la continuité comme la capacité stratégique et tactique des organisations à planifier et répondre aux incidents et interruptions d'affaires afin de permettre la poursuite des opérations à un niveau prédéfini acceptable. Cependant, il importe de rappeler ce qui suit :

- Il y a des risques stratégiques de gouvernance et d'opérations liées aux TIC associés à l'absence de structures et de politiques adéquates pour protéger l'institution financière des conséquences d'un désastre.

- Les changements[25] aux TIC d'une institution, dans le cadre des nouvelles stratégies d'affaires, requièrent une évaluation de l'impact sur la planification de la continuité des activités.

- Durant l'exécution des stratégies d'affaires et TIC, les environnements opérationnels seront en changement continuel et il y aura des changements et nouveautés dans les besoins de continuité. Cela est susceptible d'exposer l'institution financière à des risques d'exécution stratégique significatifs, particulièrement lorsque la stratégie s'échelonne sur plusieurs années.

- Bien que la continuité des activités puisse être impartie lorsque la stratégie TIC implique l'utilisation de l'infonuagique, l'institution demeure responsable du recouvrement lorsqu'un désastre affecte ses fournisseurs.

- La continuité et la résilience des TIC devraient être suffisamment robustes et éprouvées pour assurer un recouvrement opportun à la suite d'interruptions opérationnelles.

L'infogérance et l'infonuagique

L'adoption croissante par les institutions financières des services infonuagiques[26] permet de nombreux avantages (économies d'échelle, accès aux bonnes pratiques, agilité, etc.). La nature distribuée de ces services peut aussi améliorer la résilience lors de désastres ou d'interruptions de services.

---

24 La *Ligne directrice sur la gestion de la continuité des activités* énonce d'autres principes de gestion proposés par l'Autorité.

25 Par exemple, les innovations technologiques (infonuagique, l'Internet des objets, les mégadonnées, etc.) et leurs impacts significatifs sur la fonction des opérations TIC (section 3.5 « Autres pratiques »).

26 Les services infonuagiques sont une combinaison de modèle d'affaires et de modèle de livraison, disponibles en mode d'exploitation publique, privé ou hybride, et qui permettent sur demande l'accès à un groupe partagé de ressources (applications, serveurs, emmagasinage, réseaux, sécurité, etc.). Ils sont généralement livrés sous la forme *Software as a Service* (« Saas »), *Platform as a Service* (« PaaS ») et *Infrastructure as a Service* (« IaaS »).

L'Autorité considère ces services infonuagiques comme une forme d'infogérance et dans cette optique, les institutions devraient se référer aux attentes de la *Ligne directrice sur la gestion des risques liés à l'impartition.*

L'institution devrait bien saisir les caractéristiques typiques des services infonuagiques, notamment la colocation, l'amalgamation des données et la forte propension du traitement informatique dans des sites multiples ou distribués. Des actions devraient être envisagées pour identifier et gérer les risques associés à l'accès, la confidentialité, l'intégrité, la souveraineté, la conformité réglementaire et l'audit des données. En particulier, l'institution devrait s'assurer que le fournisseur de service possède l'habilité d'identifier et de faire la ségrégation des données client en utilisant des contrôles physiques et logiques robustes.

Dans le contexte de l'infogérance et l'infonuagique, l'institution financière devrait notamment :

- assurer contractuellement son droit d'auditer (ainsi que celui des autres autorités compétentes, le cas échéant) et leur accès physique aux locaux des fournisseurs de service d'infonuagique;
- assurer la sécurité des données et l'emplacement du traitement informatique par des contrôles adéquats (établis par une approche basée sur les risques) tels que les technologies de chiffrement des données en transit, des données en mémoire et des données au repos;
- mitiger les risques d'impartition en chaîne lorsque les fournisseurs impartissent eux-mêmes certaines activités à d'autres fournisseurs;
- développer des plans de contingence et des stratégies de sortie appropriés afin de pouvoir quitter toute entente contractuelle sans interruption dans la livraison de ses services, sans effets indésirables sur la conformité réglementaire et sans impact sur la continuité et la qualité des services TIC fournis aux clients.

Aussi, dans la conduite de sa revue diligente, l'institution pourrait choisir de considérer l'adhésion du fournisseur à des normes internationales pertinentes pour la livraison des services TIC. L'assurance obtenue à partir ces normes internationales sera probablement insuffisante, mais elle contribue à la réduction des risques et devrait être considérée.

Au-delà des attentes de l'Autorité sur la gestion des risques liés à l'impartition[27], l'institution financière devrait considérer le risque TIC, et notamment le cyberrisque, dans l'évaluation du niveau d'expérience et d'expertise requis pour l'activité impartie et la gestion des relations d'impartition. L'institution financière devrait de plus maintenir, dans sa liste centralisée d'ententes d'impartition importantes, toute information utile à la gestion des risques de ses données (nature, sensibilité, emplacement(s) du traitement, de l'emmagasinage et de la circulation des données, etc.).

[27] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion des risques liés à l'impartition*, décembre 2010.

Considérant le nombre de fournisseurs et la variété des impacts potentiels de l'infogérance et l'infonuagique chez les institutions financières, un niveau de contrôle serré devrait être mis en place. Ainsi, l'institution financière devrait identifier les risques stratégiques liés aux TIC inhérents aux initiatives d'infogérance, mettre en place un programme efficace de gestion de ces risques et suivre les risques émanant de toute entente d'infogérance.

Projets et programmes de transformation

Dans l'identification des risques des projets de transformation, l'institution devrait considérer notamment la perturbation des services fournis aux clients, la perte d'avantages concurrentiels, l'impact négatif sur la réputation et le retard dans la mise en œuvre de produits ou de processus critiques et stratégiques.

L'origine de ces risques peut remonter à une combinaison de décisions techniques, d'affaires et de gestion de projets. Cela pourrait, par exemple, comprendre l'incapacité à reconnaître les changements dans les affaires et les environnements technologiques susceptibles d'influencer leurs stratégies, l'incapacité à intégrer les secteurs et les plans affaires et TIC, et l'échec à impliquer les utilisateurs d'affaires, les fournisseurs et les technologies pour comprendre les besoins et permettre la livraison des plans stratégiques TIC.

Bien que les orientations de la *Ligne directrice sur la gestion intégrée de risques* soient applicables à tous les types de risques, le risque opérationnel inhérent notamment aux TIC sollicite l'engagement des responsables de l'ensemble des activités, processus et systèmes d'une institution financière. L'efficacité de cette gestion devrait être régulièrement validée et vérifiée, notamment en fonction de la variation attribuable, par exemple, aux modifications résultant des transformations organisationnelles touchant les systèmes. Conséquemment à ces changements, il pourrait s'avérer nécessaire de réviser les niveaux de tolérance au risque opérationnel lié aux TIC[28].

Dans ce contexte, l'institution financière devrait notamment :

- s'assurer de la contribution de la haute direction pour la cohérence avec la stratégie, le soutien financier et l'assistance dans la résolution des conflits;
- s'assurer que la vision, les objectifs et les systèmes d'information soient bien compris, qu'ils concordent entre eux et que le projet de transformation soit cohérent avec sa stratégie;
- comprendre la gestion du portefeuille de projets, la gestion de projet, ses propres pratiques, sa terminologie, ses normes ainsi que la méthodologie qu'elle a adoptées;
- normaliser et outiller sa méthodologie de gestion du projet;

[28] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion du risque opérationnel*, décembre 2016.

- définir le cycle de vie de développement qui comprend différentes étapes, dont l'ordre devrait être respecté afin que les besoins métiers puissent être transformés en systèmes ou en applications et que leur entretien puisse être maîtrisé;
- gérer les changements au niveau des structures et des processus, notamment les aspects informels ou intangibles (perceptions de l'impact, modifications d'habitudes de travail, etc.), la communication, l'état de préparation organisationnelle (p. ex., résistance aux changements), la formation et le support postérieur au lancement.

4. Surveillance des pratiques de gestion saine et prudente

En lien avec sa volonté de favoriser l'instauration de pratiques de gestion saine et prudente au sein des institutions financières, l'Autorité entend procéder dans le cadre de ses travaux de surveillance à l'évaluation du degré d'observance des principes énoncés à la présente ligne directrice, en considérant les attributs propres à chaque institution. En conséquence, l'efficacité et la pertinence des stratégies, politiques et procédures mises en place ainsi que la qualité de la supervision et du contrôle exercé par le conseil d'administration et la haute direction seront évaluées.

Les pratiques en matière de gestion des risques liés aux technologies de l'information et des communications évoluent constamment. L'Autorité s'attend à ce que les instances décisionnelles de l'institution financière connaissent les meilleures pratiques en la matière et se les approprient, dans la mesure où celles-ci répondent à leurs besoins.