AUTORITÉ DES MARCHÉS FINANCIERS

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

Février 2020

TABLE DES MATIÈRES

Introduction 2

1. Les types de risques liés aux technologies de l'information et des communications (TIC) 3

2. La gouvernance des TIC 5
   2.1 Rôles et responsabilités 6
   2.2 Probité et compétence 9
   2.3 Documentation à l'égard des TIC 10

3. La gestion des risques liés aux TIC 11
   3.1 Préparation 11
   3.2 Traitement 13
   3.3 Suivi 14

ANNEXE - Normes complémentaires aux lignes directrices de l'Autorité 16

Introduction

La progression rapide des innovations technologiques contribue à transformer les processus et les modèles d'affaires des institutions financières. Ces innovations introduisent par contre des risques significatifs alors qu'en parallèle, ces mêmes institutions sont de plus en plus interconnectées ou dépendantes de systèmes hérités[1] et de fournisseurs externes pour mener à bien leurs activités.

L'adoption des innovations technologiques accentue les risques de perte, de fuite, de vol, de corruption et d'accès non autorisé aux données. Elle expose davantage les institutions aux risques de cyberattaques qui sont de plus en plus sophistiquées, fréquentes, ciblées et difficiles à détecter.

Les risques liés aux technologies de l'information et des communications (« TIC »)[2] peuvent avoir des conséquences défavorables tant au niveau financier et légal que sur les clients et la réputation d'une institution.

Cette ligne directrice énonce les attentes de l'Autorité à l'égard de la gestion du risque TIC, lesquelles visent ultimement le renforcement de la résilience du secteur financier face à ce risque. Ces attentes visent notamment l'établissement d'une hygiène adéquate de sécurité par la mise en place de mesures[3] contribuant à prévenir la matérialisation d'un incident majeur et à limiter ses impacts.

Il est de la responsabilité de l'institution de bien comprendre l'ensemble des risques TIC 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. Il est également de la responsabilité de l'institution de connaître les meilleures pratiques en matière de gestion des risques TIC et de se les approprier dans la mesure où celles-ci répondent à ses besoins.

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 27 février 2021.

1 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, emmagasiner, traiter et distribuer de l'information.

2 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.

3 Ces mesures portent tant sur des pratiques fondamentales de gouvernance des TIC que sur des mesures opérationnelles telles que le déploiement, en temps opportun, des mises à jour de sécurité des logiciels, la détection du trafic non autorisé sur les infrastructures réseau, la gestion des privilèges d'accès à l'information, le renforcement des mécanismes d'authentification pour l'accès aux systèmes critiques ou le contrôle des logiciels malveillants.

1. Les types de risques liés aux technologies de l'information et des communications (TIC)

L'Autorité s'attend à ce que l'institution financière mette en place une taxonomie qui lui est propre afin de s'assurer que tous les types de risques liés aux TIC soient répertoriés.

La taxonomie devrait avoir un caractère prospectif et prendre en considération les risques technologiques omniprésents dans l'ensemble des processus des institutions financières. Cette taxonomie devrait être développée afin d'en faciliter l'agrégation et de contribuer à l'établissement d'un portrait complet. Ainsi, elle 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.

Le risque technologique devrait être évalué de manière holistique, en considérant tant les risques courants que les risques de ne pas répondre adéquatement aux changements ou à l'arrivée de technologies nouvelles ou émergentes, et ce, afin d'accroître l'agilité et la capacité de l'institution à répondre aux changements à travers le temps.

Au-delà des risques opérationnels dérivés des risques liés aux technologies, les risques stratégiques suivants[4] peuvent entraver l'atteinte des stratégies de l'institution et devraient être pris en considération :

- Le risque de gouvernance technologique[5];
- Le risque de positionnement technologique[6];
- Le risque d'exécution technologique[7].

Afin de prévenir un faux sentiment de sécurité ou d'urgence, il importe notamment que l'institution :

- utilise une terminologie TIC et une taxonomie claires et constantes pour la description des risques;
- agrège[8] les risques TIC au niveau de l'institution pour que ceux-ci soient considérés en combinaison avec tous les autres risques qui doivent être gérés.

Dans l'élaboration de sa taxonomie des risques, l'institution financière devrait établir un nombre raisonnable de catégories qui permettent de regrouper adéquatement les risques sans pour autant affaiblir le caractère particulier de chaque catégorie.

La sécurité de l'information, la gestion de crise, l'infogérance et l'infonuagique, la continuité des activités, la gestion de programmes et de projets[9], la gestion des changements, les opérations liées aux TIC, l'éthique, les ressources humaines et la propriété intellectuelle sont quelques-unes des catégories de risques liées aux TIC qui devraient être considérées dans l'élaboration de la taxonomie.

4 Ces trois regroupements de risques stratégiques peuvent être décrits sous d'autres libellés selon la taxonomie établie par l'institution financière.

5 Le risque que le conseil d'administration ne parvienne pas à s'assurer de la mise en place des éléments nécessaires pour gouverner le développement et l'exécution de la stratégie TIC.

6 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 ou ne soit pas réalisable.

7 Le risque que, dans l'exécution de sa stratégie et de son plan stratégique, la haute direction n'atteigne pas les objectifs TIC stratégiques désirés ainsi que les objectifs d'affaires associés.

8 Les risques liés aux TIC peuvent être agrégés selon de multiples dimensions (par unités organisationnelles, par types de risques liés aux TIC, par processus, etc.).

9 Par exemple, des risques peuvent résulter de l'interdépendance entre différents projets ou de la dépendance de plusieurs projets sur les mêmes ressources et expertises.

Dans l'éventualité où une institution financière dispose déjà d'une taxonomie des risques dans un secteur fonctionnel donné, par exemple l'audit interne, celle-ci pourrait être considérée dans l'élaboration d'une taxonomie des risques organisationnels, car elle pourrait contenir des catégories dont l'application à l'échelle de l'institution est éprouvée. Une fois développée, cette taxonomie devrait être communiquée à ceux qui participent directement aux activités d'évaluation des risques et aux contrôles, afin d'en assurer une utilisation cohérente dans l'identification et l'agrégation des risques TIC.

2. La gouvernance des TIC

> L'Autorité s'attend à ce que l'institution financière mette en place une gouvernance des TIC développée à partir de sources, de recommandations et de normes reconnues[10].

La gouvernance des TIC devrait 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. Ainsi, la gouvernance des TIC devrait tenir compte en continu des bonnes pratiques reconnues par les organismes professionnels et internationaux existants et s'aligner avec les objectifs d'affaires de l'institution.

Le développement de la gouvernance des TIC devrait notamment considérer :

- la compréhension et l'acceptation des responsabilités liées à l'utilisation des TIC et des données par les individus et les groupes au sein de l'institution;
- l'évaluation des TIC et leurs activités, lors de l'étude des plans et politiques, afin qu'ils soient alignés aux objectifs de l'institution, qu'ils considèrent les bonnes pratiques et répondent aux besoins des parties intéressées;
- l'évaluation des plans de l'institution pour que les TIC supportent les processus d'affaires avec la capacité requise;
- la prise en considération du cycle de vie des données dans la définition des responsabilités;
- la mesure dans laquelle les TIC répondent aux obligations règlementaires, légales, contractuelles ainsi qu'aux standards et normes professionnelles et internationales;
- la façon dont les individus se comportent envers les autres (pour l'ensemble des parties prenantes) dans les pratiques et la prise de décisions liés aux TIC.

Les divers éléments de l'encadrement établi par l'institution financière (stratégies, politiques, etc.) devraient considérer et arrimer entre eux les dispositions déjà existantes[11], inhérentes et utiles à la gestion des risques technologiques.

[11] Ces dispositions sont susceptibles d'avoir été définies et documentées distinctement à travers les années et pourraient comporter des contradictions.

2.1 Rôles et responsabilités

Le conseil d'administration

En sus des attentes[12] déjà émises par l'Autorité, le conseil d'administration devrait notamment s'assurer :

- que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement éthique et sécuritaire dans l'exploitation des technologies;
- d'échanger à l'égard des TIC avec les parties intéressées (internes et externes) afin d'appuyer par une documentation sa compréhension des besoins et porter un jugement sur la conception actuelle et future de la gouvernance des TIC;
- que les rôles et responsabilités de la fonction TIC et des fonctions de gestion de la sécurité de l'information et de la continuité des activités soient clairement définis dans l'établissement et le maintien de la gouvernance des TIC;
- que les structures, rôles et fonctions de support soient évalués régulièrement afin de permettre le développement et l'amélioration continue de la gouvernance des TIC.

De plus, le conseil d'administration devrait, conformément à la section 2.2, veiller à l'attribution des responsabilités liées au développement de l'encadrement des risques TI, notamment par l'appréciation des compétences nécessaires à l'exercice de ces responsabilités. Il devrait par ailleurs veiller à l'assignation :

- d'un responsable[13] pour les systèmes informatiques et les technologies de l'information qui supportent les objectifs de l'entreprise[14];
- d'un responsable à la seconde ligne de défense, tel un chef de la sécurité de l'information[15] (ou une autre personne de la haute direction et de la seconde ligne de défense), pour la surveillance du déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques de l'institution;
- d'un responsable à la seconde ligne de défense, tel un chef des données[16] (ou une autre personne de la haute direction et de la seconde ligne de défense[17]), lequel surveille l'encadrement approuvé à l'égard de la collecte, l'emmagasinage et l'utilisation des données à travers l'institution;
- de responsables, au sein de la haute direction, pour l'ensemble des différents actifs informationnels et risques TIC présents dans l'institution.

Le conseil d'administration devrait s'assurer d'obtenir des mises à jour sur les scénarios considérés dans le développement et la mise à l'essai (tests) des plans de recouvrement en cas de désastre et de continuité des activités afin de comprendre les objectifs de maintien de la disponibilité des opérations et systèmes TIC critiques. De plus, il devrait avoir une compréhension globale des processus d'escalade lors de brèches ou d'incidents de sécurité, incluant le moment où il devrait être notifié.

La haute direction

En sus des rôles et responsabilités qui lui sont généralement dévolus[18], la haute direction devrait notamment :

---

12 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*.

13 Tel un directeur des technologies ou un chef des technologies ou de l'information. Ces derniers portent parfois aussi le nom de *Chief Technology Officer* (CTO) ou *Chief Information Officer* (CIO).

14 Cette personne est notamment responsable de l'exécution des plans stratégiques TIC, des processus reliés aux technologies (opérations, architecture, gestion de risque…), du développement des infrastructures technologiques de l'institution et de la présentation au conseil d'administration des propositions technologiques ainsi que des statuts de la mise en œuvre des stratégies et encadrements liés aux TIC.

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

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

17 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*.

18 AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*.

- mettre en place une fonction TIC opérant sous la surveillance d'une fonction de contrôle de la deuxième ligne de défense;
- délimiter clairement les responsabilités de la fonction de la sécurité de l'information, pour favoriser son indépendance et objectivité, notamment en la séparant des processus opérationnels TIC et par la mise en place de contrôles compensatoires au besoin. Cette fonction devrait n'être responsable d'aucun audit interne;
- définir les rôles et responsabilités pour le maintien et la diffusion, au sein de l'institution, d'une documentation et de l'information permettant la prise de décision éclairée à l'égard des TIC;
- gérer la relation entre les services offerts par la fonction TIC et les unités d'affaires de manière formelle et transparente et en utilisant un langage commun pour assurer l'atteinte des objectifs stratégiques;
- établir et maintenir une architecture d'entreprise comprenant les processus, informations, données et couches d'architectures d'applications, de technologies et de sécurité;
- distinguer les personnes responsables ou imputables dans la gestion du risque TIC de celles qui doivent être consultées ou informées;
- évaluer régulièrement, en collaboration avec les fonctions de conformité et d'audit interne, 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[19], règlements et obligations contractuelles, etc.);
- revoir périodiquement les écarts de conformité (dont les dérogations approuvées par le conseil d'administration) aux encadrements établis pour le risque TIC[20].

Dans l'établissement de la stratégie TIC, la haute direction devrait notamment :

- établir une vue holistique des environnements d'affaires et des environnements TIC (actuels et à venir) afin d'identifier les initiatives de transformation requises;
- définir et documenter la façon dont elle fera évoluer ses TIC, son architecture technologique, sa structure organisationnelle et ses dépendances clés avec les partenaires et fournisseurs, pour supporter sa stratégie d'affaires;
- arrimer adéquatement et en continu les plans stratégiques TIC et les stratégies d'affaires tout en considérant la capacité des TIC, actuelle et requise dans le futur;
- considérer l'utilisation des innovations technologiques dans la planification stratégique et les décisions d'architecture d'entreprise;
- définir des objectifs prévoyant le maintien de la capacité de l'institution à anticiper les incidents TIC, à les détecter et à en assurer le recouvrement[21] pour assurer la résilience des systèmes TIC.

De plus, en matière de sécurité de l'information, le responsable désigné de la haute direction devrait notamment :

- développer, documenter et diffuser une politique de sécurité de l'information qui définit les principes et les règles à suivre pour la protection de la confidentialité, l'intégrité et la disponibilité des informations de l'institution et de ses clients;
- définir des objectifs de sécurité de l'information clairs pour les systèmes, les services TIC, les processus et les personnes;

[19] Notamment à la *Loi sur la protection des renseignements personnels* dans le secteur privé et à la Loi concernant le cadre juridique des technologies de l'information.

[20] Les dérogations devraient être revues périodiquement, en fonction de la nature évolutive des TIC et des menaces inhérentes, pour assurer qu'elles demeurent à un niveau acceptable et qu'elles soient corrigées en temps opportun.

[21] Un incident TIC, un cyberincident ou un incident de sécurité de l'information se produit notamment lorsqu'une interruption inattendue dans la livraison des services TIC ou une brèche de sécurité d'un système vient compromettre la disponibilité, l'intégrité ou la confidentialité des données ou des systèmes TIC.

- appliquer la politique de sécurité de l'information à toutes les activités de l'institution et inclure l'information traitée chez les intervenants externes[22] au périmètre de l'institution;
- déployer des contrôles pour les actifs[23] informationnels qui soient proportionnels à la criticité et la sensibilité desdits actifs;
- conduire des régimes d'essais systématiques adéquats pour valider l'efficacité des contrôles mis en place;
- déployer des programmes de formation et de sensibilisation en sécurité de l'information;
- produire des indicateurs de performance de la sécurité couvrant notamment les impacts d'affaires (pour le bénéfice du personnel non technique) et l'efficacité des contrôles de sécurité.

À l'égard de la reddition, la haute direction devrait notamment rendre compte :

- des objectifs et des indicateurs recueillis liés aux TIC et à ses processus en temps opportun et de manière systématique;
- des résultats découlant de la vigie conduite sur les bonnes pratiques et les normes en développement, au niveau national et international, liées aux TIC et leurs impacts potentiels sur les activités de l'institution;
- des enjeux clés liés aux TIC incluant les projets, les priorités et les incidents TIC significatifs de même que des rapports réguliers sur le risque TIC.

Autres rôles

La fonction de gestion des risques[24] de l'institution financière devrait surveiller la fonction TIC de l'institution et prendre en charge la surveillance de l'ensemble des risques TIC, tant les risques opérationnels et stratégiques que ceux qui découlent des innovations[25] liées aux TIC. Cette fonction devrait aussi assurer un suivi rigoureux des risques importants ainsi qu'une veille des risques émergents liés aux TIC.

L'assurance objective attendue de la fonction d'audit interne, sur la suffisance et l'efficacité de la gouvernance des TIC, devrait notamment couvrir l'efficience et l'efficacité des opérations TIC, la protection des actifs informationnels et la fiabilité et l'intégrité de leurs processus de divulgation.

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 les contrôles maintenus par les parties externes. L'audit interne devrait aussi revoir les assurances fournies par une partie externe et qui ont le potentiel de nuire à l'institution, à sa clientèle ou à d'autres parties intéressées.

D'autres rôles définis à travers l'institution ont un effet sur la gouvernance et la gestion des risques TIC. Bien qu'ils n'y soient pas directement liés, ils se présentent tout de même comme des parties intéressées et devraient être considérés dans la définition des rôles et responsabilités. Il pourrait s'agir, par exemple, des responsables de la continuité des affaires ou des ressources humaines.

22 Dans le cas d'intervenants externes, il convient ici d'établir des ententes appropriées sur le traitement sécuritaire de l'information.

23 Les actifs informationnels (données, matériels et logiciels) ne sont pas limités uniquement à ceux détenus par l'institution. Ils englobent aussi les actifs informationnels confiés ou livrés par les clients ou des tiers.

24 Le chef de la gestion des risques ou un membre désigné de la haute direction en mesure de synthétiser, vulgariser et communiquer efficacement l'information liée aux TIC auprès de divers auditoires.

25 Par exemple, les risques de biais ou d'utilisation non éthique des technologies de données massives et d'intelligence artificielle.

2.2 Probité et compétence

En concordance avec les attentes de l'Autorité sur les critères de probité et de compétence[26], une gouvernance efficace et efficiente, qui inclut les technologies de l'information et des communications, requiert un niveau adéquat d'expertise, de qualifications professionnelles, de connaissances et d'expériences de la part des instances décisionnelles.

Les membres des instances décisionnelles et les mécanismes de gouvernance établis (par exemple : comités d'audit, gestion de risques et gestion des TIC) devraient avoir la connaissance et la compréhension de l'utilisation des TIC, des tendances et orientations futures des TIC de même que l'autorité nécessaire pour mener à bien leurs responsabilités respectives.

Dans l'évaluation de la compétence des personnes membres des instances décisionnelles, une grille d'aptitudes et de connaissances dont les critères portent sur les TIC, devrait être établie, actualisée et appliquée périodiquement auprès des personnes occupant des postes stratégiques liés à la gouvernance et la gestion des risques liés aux TIC ou plus fréquemment si requis.

Dans cette perspective, il devrait y avoir un recensement périodique de 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.

Afin de minimiser le risque qu'il n'y ait pas suffisamment d'expertise TIC aux postes clés, un processus formel d'acquisition de compétences qui traite des enjeux stratégiques liés aux TIC devrait être développé.

De même, un programme de formation complet sur la sensibilisation à la sécurité des TIC devrait être déployé à l'ensemble du personnel et tenir compte minimalement du paysage courant des menaces (dont les cybermenaces) et de leurs conséquences, des lois, des règlements, des encadrements établis par l'institution et des responsabilités du personnel dans la protection des actifs informationnels.

Ce programme de formation devrait être mis à jour et reconduit régulièrement pour l'ensemble du personnel de l'institution et pour tout fournisseur de service qui accède aux actifs informationnels.

De même, avant l'emploi, tout au long de celui-ci et à sa terminaison, l'institution devrait mener régulièrement des vérifications de sécurité pour les ressources humaines (incluant les consultants, les partenaires et les fournisseurs) ayant accès aux données et aux systèmes TIC et qui peuvent exposer l'institution à des vols de données, du sabotage, de la fraude et d'autres risques liés aux TIC.

[26] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*.

2.3 Documentation à l'égard des 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 sécuritaire de la documentation et l'information permettant la prise de décision éclairée à l'égard des TIC.

Cette documentation ne devrait pas être statique, mais plutôt évoluer dans le temps. Tout comme les affaires, les TIC d'une institution sont en perpétuel changement au rythme des acquisitions, des mises à jour et des changements externes. Cette documentation devrait contenir suffisamment d'informations agrégées pour faciliter la prise de décision concernant la stratégie TIC.

La documentation devrait notamment 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, la méthodologie de développement et les processus d'opérations.

De plus, parmi les documents stratégiques qui sont issus des meilleures pratiques, l'institution financière devrait considérer :

- la description des contextes auxquels fait face l'institution, les lignes d'affaires et les fonctions de support;
- la description de l'impact des risques TIC sur les stratégies d'affaires;
- le registre des risques TIC et la matrice des risques et contrôles TIC;
- les modèles et processus d'opérations des TIC.

Bien que la documentation puisse être préparée et maintenue par diverses composantes de l'institution, les éléments clés[27] devraient toutefois être encadrés par la haute direction et approuvés par le conseil d'administration.

[27] Les éléments clés présentés au conseil d'administration devraient être formulés de manière que ses membres puissent facilement en faire l'appréciation afin de prendre une décision informée.

3. La gestion des risques liés aux TIC

> L'Autorité s'attend à ce que l'institution financière considère l'ensemble des activités nécessaires à la préparation, au traitement et au suivi requis dans la gestion des risques liés aux TIC.

L'élaboration des stratégies, des politiques et des procédures permettant d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et de suivre les risques TIC, devrait considérer les activités nécessaires de préparation, de traitement et de suivi requises pour que les premières heures d'une crise réelle soient moins dommageables. Par exemple, l'ensemble des mesures prévues par l'institution, notamment les mesures de réponse et de recouvrement, devraient faire l'objet de simulations de crise. De plus, les intervenants et spécialistes externes requis par ces mesures devraient être préqualifiés et les termes et conditions contractuels préétablis.

Dans la mise en place de pratiques robustes de gestion des risques TIC à travers l'institution, cette dernière devrait aussi tenir compte de la participation des parties intéressées externes afin de s'assurer que l'information juste et pertinente à la gestion des risques est distribuée et utilisée par tous.

Le cadre de gestion des risques TIC devrait permettre l'établissement et le maintien d'une vue holistique des risques TIC incluant les liens et les dépendances entre les gens, les processus d'affaires de bout en bout, les fonctions de l'institution, les systèmes TIC et les actifs qui supportent ces processus et ces personnes. Le recensement des rôles, processus et fonctions d'affaires devrait permettre d'identifier leurs importances relatives et leurs interdépendances aux risques TIC.

3.1 Préparation

La sélection des mesures préparatoires pour la gestion des risques TIC devrait notamment contribuer à la protection des données sensibles (telles que les informations des clients) contre la divulgation, la fuite ou les accès non autorisés. Elle devrait aussi contribuer à la résilience de l'environnement TIC. Ces mesures devraient couvrir, entre autres, les contrôles d'accès, l'authentification, l'intégrité et la confidentialité des données, l'enregistrement des activités et le suivi des événements de sécurité[28].

Dans sa préparation, l'institution financière 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'approche intégrée pour gérer le risque TIC devrait être appliquée à l'échelle de l'institution. Elle devrait permettre notamment :

- d'assurer un alignement de l'ensemble des outils et des échelles d'évaluation des risques utilisés et une utilisation constante, convenue et transparente;
- d'utiliser un processus rigoureux pour le recensement périodique des actifs informationnels et leurs vulnérabilités, afin d'associer adéquatement les risques aux actifs de manière holistique. Il en va 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. Cette gestion des actifs devrait aussi couvrir les données, le personnel, les systèmes TIC (incluant ses diverses composantes matérielles et logicielles) et les locaux les abritant;

[28] L'annexe aborde plusieurs mesures complémentaires à considérer et qui ont fait leurs preuves dans la gestion des risques liés à la sécurité de l'information, aux opérations TIC, à l'infogérance et aux projets de transformation TIC.

- d'exploiter un cadre de classification[29] permettant de définir la criticité des données et des actifs informationnels (incluant ceux qui sont gérés par des parties intéressées externes) minimalement selon leurs exigences de disponibilité, d'intégrité et de confidentialité;
- d'utiliser des processus de gestion d'incidents TIC, dotés d'objectifs de reprise et recouvrement adéquats et permettant la proactivité dans la gestion des risques;
- d'assurer un suivi adéquat et en temps opportun des activités de mitigation des risques présents au registre des risques TIC;
- de suivre l'efficacité des mesures de mitigation, de même que le nombre d'incidents signalés afin de les corriger lorsque nécessaire;
- de considérer des facteurs financiers, légaux, règlementaires, opérationnels ainsi que des facteurs liés à la clientèle et à la réputation dans l'évaluation du risque TIC.

Outre l'évaluation du risque TIC inhérent à ses activités, ses produits ou ses services (incluant particulièrement le cyberrisque), l'institution financière devrait considérer l'impact que ce risque représente pour ses partenaires, fournisseurs, clients ainsi que pour les autres participants du secteur financier, lorsque pertinent.

L'institution financière devrait réaliser des évaluations des risques liés aux TIC à intervalles planifiés, lorsque des changements significatifs sont prévus ou ont lieu et lorsque des incidents opérationnels ou de sécurité significatifs se matérialisent, en tenant compte de critères établis. L'évaluation des risques liés aux TIC devrait s'inscrire dans un processus systématique et cyclique permanent.

Par ailleurs, l'institution financière devrait utiliser des méthodes permettant de faire le lien entre les scénarios de risques liés aux TIC et leurs impacts potentiels sur les actifs informationnels et sur les processus d'affaires afin que l'ensemble des parties intéressées comprennent[30] les effets des événements indésirables liés aux technologies de l'information et des communications.

De plus, l'institution financière devrait :

- identifier tous les points individuels de défaillance potentielle dans les systèmes TIC et les architectures de réseaux afin que des mesures appropriées soient déployées pour mitiger les risques d'interruption;
- conduire les analyses d'impact d'affaires de bout en bout pour les processus d'affaires critiques afin que les plans de recouvrement (en cas de désastre) et de continuité des activités priorisent adéquatement les opérations critiques de l'institution dans le recouvrement des systèmes TIC;
- considérer un ensemble plausible[31] d'événements et de scénarios de désastre, incluant des événements de cybersécurité, dans la planification des plans de recouvrement et de continuité;
- inclure les dispositions régissant le recouvrement dans les délais requis et la conduite de tests périodiques dans la stratégie de sauvegarde des données pour assurer l'efficacité des procédures.

Les processus et les procédures assurant la résilience des systèmes TIC devraient tenir compte continuellement de l'évolution rapide des menaces. Ils devraient permettre de contenir les impacts des incidents de sécurité potentiels et accélérer le retour aux opérations normales. Parmi ces processus et procédures, il y a notamment la planification des plans de réponse et de recouvrement, les communications, l'analyse, la mitigation et l'amélioration continue.

---

29 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.

30 Les évaluations des risques liés aux TIC requièrent que les résultats soient exprimés en des termes d'affaires clairs et non ambigus. Une gestion efficace des risques liés aux TIC requiert une compréhension commune, 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 événements ou incidents défavorables interagissent sur les objectifs d'affaires de l'institution.

31 L'institution devrait notamment considérer des scénarios à faible probabilité qui entraînent des impacts élevés de nature financière et non-financière (réputation, conformité, etc.).

Afin d'éviter d'accroître son exposition à des risques de sécurité et de stabilité, l'institution financière devrait établir des plans de remplacement en temps opportun de son matériel et logiciel TIC avant qu'ils n'atteignent la date de fin de support annoncée par leurs fournisseurs.

3.2 Traitement

Dans le traitement des risques TIC, l'institution financière devrait notamment :

- déterminer les mesures nécessaires à la mise en œuvre des options de traitement des risques identifiés;
- comparer les mesures déterminées avec les meilleures pratiques existantes et vérifier qu'aucune mesure nécessaire n'a été omise;
- produire une déclaration des contrôles répertoriant les mesures et la justification de leur inclusion ou exclusion;
- maintenir et utiliser des encadrements de sécurité, et les processus et les procédures qui en découlent, pour gérer les systèmes d'information et les actifs;
- effectuer la maintenance et la réparation des éléments composant les systèmes TIC conformément aux encadrements établis par l'institution.

De plus, l'institution financière devrait:

- détecter en continu les activités anormales sur les infrastructures réseau, les systèmes TIC et les actifs informationnels afin de comprendre l'évolution d'événements non désirés et leurs impacts potentiels et de vérifier l'efficacité des mesures de protection;
- mettre à l'essai et maintenir les processus de détection précités afin d'assurer une connaissance adéquate et opportune des événements anormaux;
- exécuter et maintenir les processus et procédures de réponse et de récupération afin d'assurer la réponse aux incidents de cybersécurité détectés et la restauration des systèmes ou des actifs;
- recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité);
- exécuter et réviser les activités planifiées pour empêcher l'expansion d'un événement auprès d'autres systèmes TIC, en atténuer les effets et résoudre l'incident.

L'accès aux dispositifs[32] de retrait ou d'extraction des données devrait aussi faire l'objet d'une évaluation de risque et devrait être autorisé uniquement lorsqu'un besoin d'affaires réel existe, afin de prévenir les risques de fuite de données.

L'institution financière devrait démontrer qu'elle évalue 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 les systèmes hérités supportent des opérations critiques, l'institution financière devrait avoir en place une stratégie pour gérer l'infrastructure vieillissante.

Les applications développées ou acquises par les utilisateurs finaux pour l'automatisation de leurs opérations, incluant les applications accessibles par l'Internet, devraient être approuvées par les secteurs d'affaires pertinents et la fonction TIC de l'institution. Ces applications devraient être prises en considération dans les processus de gestion des actifs informationnels et de gestion des risques TIC. L'institution financière devrait s'assurer de la mise en place de mesures de sécurité adéquates contre la perte ou la fuite de données et

[32] Par exemple, l'utilisation d'appareils informatiques portatifs (tablette, cellulaire, etc.), de dispositifs d'emmagasinage (clé USB, disque dur portable, etc.), de courriels, de messagerie instantanée et de copies imprimées.

l'exposition à des virus malicieux liées à ces applications. De plus, l'institution financière devrait déployer des contrôles permettant de surveiller et détecter l'utilisation non autorisée de ces applications[33].

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 d'affaires particulière. Ils peuvent aussi inclure l'atténuation du risque à travers les contrôles ou le partage ou transfert du risque.

L'institution financière devrait évaluer régulièrement l'adéquation de ses ressources avec l'appétit pour le risque par des exercices de simulation de crise pour l'ensemble des risques matériels et potentiels, classifiés selon leur probabilité et leur impact (p. ex. : les risques TIC, dont le cyberrisque).

Dans le maintien régulier de son registre des risques TIC, connus et potentiels, l'institution devrait décrire notamment leurs attributs et activités de contrôles de façon claire et suffisamment détaillée. Le registre des risques TIC devrait être mis à jour de manière prospective et l'adéquation des contrôles devrait être évaluée régulièrement.

3.3 Suivi

En concordance avec les attentes[34] déjà émises, les bonnes pratiques généralement reconnues de même que la législation applicable, l'Autorité s'attend notamment, en matière de divulgation et de transparence, à ce que l'institution financière mette en place les mécanismes nécessaires pour notifier promptement les parties intéressées internes et externes, incluant l'Autorité, lors d'un incident opérationnel.

Les processus et les procédures mis en place dans le cadre de la gestion des incidents de l'institution financière devraient permettre d'intervenir et de rétablir les services le plus rapidement possible lors d'incidents liés aux TIC. Ils devraient notamment :

- coordonner les réponses et les activités de recouvrement requises suite à la notification aux parties prenantes internes et externes;
- contribuer à minimiser les impacts sur la clientèle;
- rendre compte des incidents selon des critères préétablis;
- partager l'information utile contribuant au rehaussement de la sécurité de l'information;
- gérer les relations publiques et l'impact sur la réputation de l'institution.

De plus, l'institution financière devrait conduire des analyses spécifiques suite à un incident majeur pour améliorer ses plans de réponse et de recouvrement. Elle devrait notamment :

- explorer les données recueillies dans ses infrastructures par ses systèmes de détection;
- identifier et mesurer les impacts de l'incident;
- mitiger ou accepter et documenter le risque des nouvelles vulnérabilités identifiées;
- formuler et communiquer aux parties prenantes internes les leçons apprises dans la résolution de l'incident;
- recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité).

À partir des leçons apprises, des constats et des décisions prises lors de la gestion des risques TIC, l'institution financière devrait procéder à la révision de ses stratégies, notamment celles établies à partir de ses activités préparatoires (Section 3.1). Cette révision devrait être conduite à l'aide d'objectifs d'évaluation

[33] **Shadow IT** (parfois **Rogue IT**) est aussi un terme utilisé pour désigner des systèmes TIC mis en œuvre au sein d'organisations sans approbation.

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

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.

ANNEXE - Normes complémentaires aux lignes directrices de l'Autorité

L'Autorité s'attend à ce que la mise en œuvre des pratiques de gestion saine et prudente, énoncées dans l'ensemble de ses lignes directrices, considère les pratiques spécifiques liées aux TIC qui ont fait leurs preuves et sont généralement reconnues.

La gestion du risque TIC repose sur l'appropriation par l'institution financière des attentes émises dans plusieurs lignes directrices de l'Autorité dont celles portant notamment sur la gouvernance, la gestion intégrée des risques et la conformité. Toutefois, elle repose aussi sur les attentes émises dans les sections précédentes de la présente ligne directrice et sur la mise en œuvre de plusieurs pratiques spécifiques aux TIC.

Dans cette perspective, les pratiques[35] qui suivent concourent à l'établissement d'une approche holistique. Leur utilisation contribue à prévenir et à atténuer les risques TIC, comme par exemple, ceux liés à son utilisation et à son opération.

Sécurité des TIC

L'institution financière devrait mettre en place des mécanismes robustes de sécurité permettant d'assurer la livraison de ses services critiques et l'identification des incidents liés aux TIC.

Parmi les mécanismes à considérer, il y a notamment la gestion des identités et des accès, la formation et sensibilisation, la ségrégation des réseaux et la protection de leur intégrité, la sécurité des données, la protection des appareils de types « endpoints », la vérification de l'intégrité des logiciels et du microcode, les processus de protection de l'information et les solutions[36] technologiques de protection contribuant à la résilience des systèmes et des actifs informationnels. De même, la détection d'événements et d'anomalies, la surveillance en continu des systèmes d'information et la mise à l'essai des processus de détection devraient être considérées.

L'institution financière devrait définir un processus pour recueillir, sécuriser, entreposer, consolider, traiter et revoir les journaux d'événements TIC pour faciliter les opérations de surveillance de sécurité. Cela devrait comprendre notamment les journaux d'événements des coupe-feu, des applications, des systèmes d'exploitation et des événements d'authentification.

L'institution financière devrait s'assurer que l'accès[37] logique et physique aux actifs informationnels et aux ressources associées est limité aux utilisateurs, processus ou appareils autorisés ainsi qu'aux activités autorisées selon un processus rigoureux et prédéfini.

Les privilèges d'accès octroyés devraient être établis sur la base des principes « besoin de savoir », « moindre privilège » et « ségrégation des tâches », uniquement au personnel autorisé et de façon à prévenir les accès injustifiés à de larges ensembles de données et prévenir le contournement des contrôles de sécurité.

L'institution financière devrait limiter l'usage de compte d'accès génériques ou partagés et s'assurer que les usagers puissent être identifiés dans l'utilisation des systèmes TIC. Les exceptions devraient être justifiées, recensées et approuvées.

35 Les thèmes abordés dans cette annexe sont tirés des meilleures pratiques recommandées par différents organismes nationaux ou internationaux dont notamment le NIST, Cobit, G7 et ISO.

36 Par exemple : coupe-feu, contrôle d'accès réseau, dispositif de détection et prévention d'intrusion, antivirus, chiffrement, outil de suivi et analyse des journaux.

37 Cela comprend tout autant les accès des usagers réguliers ou à hauts privilèges que les accès à distance.

L'institution financière devrait soumettre ses contrôles à l'égard de la sécurité de l'information à différents types d'évaluation, de tests et des revues indépendantes périodiques et à des tests d'intrusions[38] et des exercices de type « Red Team[39] ».

Dans l'évaluation des risques de la sécurité de l'information, l'institution financière 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 responsables des risques;
- 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.

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[40] et son environnement d'affaires.

Dans le développement d'une sécurité de l'information adéquate pour les systèmes TIC, l'institution devrait s'assurer d'une ségrégation adéquate entre la sécurité opérationnelle et la gestion des risques.

Opérations liées aux TIC

Les innovations technologiques, telles que l'infonuagique, l'Internet des objets et les mégadonnées, ont un impact significatif sur la fonction 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 personnel des opérations TIC ait l'information, les ressources et les outils requis pour détecter tout problème qui s'introduit dans les opérations des centres de traitement, des réseaux, des infrastructures de sécurité de l'information et dans le support aux utilisateurs. Ces éléments devraient contribuer notamment :

- à l'établissement d'un inventaire exhaustif du matériel de traitement de l'information, des ressources, des emplacements, etc.;
- à la priorisation des efforts de mitigation des risques TIC;
- à l'identification de contrôles de mitigation comme des politiques et des procédures pour la sécurité physique et logique, la gestion des données, du personnel et des changements, la distribution et transmission d'informations, les sauvegardes et le support utilisateurs, etc.;
- au suivi et à la reddition de la performance, de la planification de la capacité et de l'autoévaluation des contrôles.

L'institution financière devrait déployer un processus de gestion des configurations du matériel et du logiciel constituant ses systèmes d'information permettant d'avoir une visibilité et un contrôle efficace et sécuritaire de ses systèmes.

L'institution financière devrait s'assurer de minimiser les risques d'interruptions aux opérations par la mise en place de processus adéquats pour la gestion des changements touchant les équipements TIC (matériels et logiciels) et les procédures liées au développement, l'exécution, le support et l'entretien des systèmes TIC de production. Ces processus devraient prévoir notamment :

---

38 Les tests d'intrusion 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.

39 Les exercices de type Red Team consistent à effectuer une simulation permettant à l'institution de détecter et répondre à des attaques ciblées. Les processus de contrôle des personnes et de la technologie en place dans l'institution sont revus tout au long de l'exercice en simulant les objectifs et les actions d'un attaquant.

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

- des évaluations de risques de sécurité et d'impacts (notamment en relation avec les autres actifs informationnels) avant l'implantation des changements proposés;
- des tests suffisants pour les nouvelles TIC, les rehaussements et les correctifs envisagés aux systèmes existants avant leur déploiement;
- les exigences et les niveaux d'approbation requis pour le déploiement des changements;
- des procédures clairement définies pour l'évaluation, l'approbation et le déploiement des changements d'urgence, incluant les approbateurs, afin de réduire les risques de sécurité et de stabilité des environnements de production;
- une ségrégation stricte des tâches dans le processus de mise à jour des logiciels afin de restreindre la possibilité qu'un seul individu développe, compile et déploie du code logiciel d'un environnement de développement à un environnement de production;
- l'activation de l'enregistrement des activités dans les journaux d'audit et de sécurité.

Dans l'optique de réduire les risques d'interruptions des opérations provenant de l'exploitation mal intentionnée de bogues ou vulnérabilités des logiciels, l'institution financière devrait établir des pratiques et des standards sécurisés pour encadrer la programmation, la revue des codes sources et la mise à l'essai de la sécurité applicative de ses systèmes TIC. Lorsque l'application de ces pratiques soulève des enjeux de disponibilité, d'intégrité et de confidentialité de l'information et des systèmes TIC, ces derniers devraient être compilés, suivis et corrigés.

L'institution financière devrait s'assurer du déploiement de processus pour que soit évalué et géré l'ensemble des risques opérationnels associés à l'utilisation, la propriété, l'opération et l'adoption des TIC au sein de l'institution. Elle devrait notamment :

- implanter une structure opérationnelle TIC adéquate pour supporter les activités d'affaires de l'institution;
- revoir et comprendre comment les systèmes en place supportent les processus d'affaires associés;
- 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 sécuritaire;
- prévoir une continuité et résilience opérationnelle;
- prévoir une sélection, dotation, succession et formation adéquate du personnel lié aux TIC.

Infogérance et infonuagique

L'infogérance ne réduit pas nécessairement les risques liés aux TIC. Elle peut exposer l'institution financière à des risques accrus de sécurité, de performance opérationnelle et de continuité des activités en cas de mauvaise gestion. La gestion adéquate de ces risques demeure toujours sous la responsabilité de l'institution. 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.

En concordance avec les attentes[41] émises par l'Autorité, l'institution financière demeure responsable du recouvrement de ses activités lorsqu'un désastre affecte ses fournisseurs lors de l'impartition de sa stratégie TIC avec l'infonuagique. Aussi, elle 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.

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

L'institution financière devrait s'assurer de l'efficacité de son cadre de gestion des risques TIC lorsque des ententes d'infogérance sont conclues avec des fournisseurs de services externes ou des membres de son groupe.

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

L'institution financière devrait bien comprendre 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 règlementaire et l'audit des données. Notamment, l'institution financière devrait s'assurer que le fournisseur de services possède l'habilité d'identifier et de faire la ségrégation des données client en utilisant des contrôles physiques et logiques robustes. De plus, l'institution financière devrait 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.).

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) de même que 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[42] adéquats (établis par une approche basée sur les risques) comme les technologies de chiffrement des données en transit, en mémoire et 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 règlementaire et sans impact sur la continuité et la qualité des services TIC fournis aux clients;
- suivre le développement du risque potentiel de concentration lorsque la livraison de ses services critiques repose sur un nombre restreint de fournisseurs de services;
- suivre et obtenir l'assurance de la conformité des fournisseurs aux objectifs et mesures de sécurité et aux attentes de performance.

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. La cybersécurité ne devrait pas être considérée uniquement au niveau des fournisseurs majeurs ou des fournisseurs de services critiques. De fait, certains autres fournisseurs pourraient constituer un maillon faible dans les processus de sécurité.

L'utilisation des services de certaines tierces parties peut ne pas constituer une forme d'impartition. Par contre, plusieurs de leurs services sont fournis à l'aide des TIC ou mettent en jeu des informations potentiellement confidentielles. Ces tierces parties peuvent aussi être exposées à des bris de sécurité. L'institution financière devrait évaluer les risques de bris de confidentialité, d'intégrité et de disponibilité des informations traitées par ces services et les gérer adéquatement.

[42] L'institution devrait considérer notamment, dans l'établissement des ententes contractuelles et de niveaux de services, l'utilisation d'objectifs et de mesures de sécurité de l'information, l'utilisation de sa propre définition du cycle de vie des données, et l'établissement de ses besoins de surveillance de la sécurité et chiffrement de ses données.

Projets et programmes de transformation

La mise en place de toute stratégie TIC requiert le démarrage formel de programmes de gestion du changement technologique. De tels programmes nécessitent des ressources, une gestion et un suivi approprié et ils introduisent aussi de nouveaux risques qui doivent être mitigés. Parmi ces risques, il y a 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'institution financière devrait établir un cadre de gestion des projets assurant l'utilisation constante de pratiques de gestion pour la livraison de résultats répondant aux besoins et aux objectifs d'affaires et de sécurité. La gestion des risques prévue dans ce cadre devrait permettre d'identifier, d'évaluer, de gérer et de suivre les risques associés tout au long du cycle de vie des projets.

Ce cadre de gestion devrait couvrir les pratiques nécessaires pour gérer tout le cycle de vie des projets. Il devrait aussi permettre d'établir les plans de projets TIC complets requis pour la mise en place des stratégies. Ces plans de projet devraient définir clairement la portée du projet, les analyses coûts-bénéfices et de faisabilité, les activités, les livrables et les jalons importants et les rôles et responsabilités des ressources requises pour chaque phase du projet.

Lorsque les projets portent spécifiquement sur l'acquisition, le développement ou la modification de systèmes TIC nouveaux ou existants, l'institution financière devrait s'assurer que les processus, les procédures et les contrôles de son cadre respectent le principe de prise en compte de la sécurité dès la conception («*security by design*») afin de permettre la mise en place de système TIC fiable et résilient aux attaques.

L'institution financière devrait normaliser et outiller sa méthodologie de gestion du projet. Elle devrait définir clairement le cycle de vie du développement des systèmes TIC qui comprend différentes étapes, dont notamment l'identification des besoins en sécurité de l'information, et 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; de plus, l'institution devrait gérer les changements engendrés par les projets 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.