Commentaires de Desjardins : Consultation publique – Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications (Janvier 2020)

Références # article et page de référence	Libellé AMF	Commentaires
	PROJET	
	LIGNE DIRECTRICE SUR LA GESTION DES RISQUES LIÉS AUX TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS	
	Janvier 2020	
	TABLE DES MATIÈRES	
2	**Préambule**	
2	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.
2	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.
2	**Note de l'autorité**
2	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.
2	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 saine et prudente des risques liés aux technologies de l'information et des communications (« TIC »).
3	**Champ d'application**
3	La présente ligne directrice s'applique aux assureurs autorisés, à une fédération de sociétés mutuelles, aux coopératives de services financiers et personnes morales faisant partie d'un groupe coopératif, aux sociétés de fiducie autorisées, aux sociétés d'épargne et aux autres institutions de dépôts autorisées régis par les lois suivantes : • Loi sur les assureurs, RLRQ, c. A-32.11 ; • Loi sur les coopératives de services financiers, RLRQ, c. 67.32 ; • Loi sur les sociétés de fiducie et les sociétés d'épargne, RLRQ, c. S-29.023 ;

	• Loi sur les institutions de dépôts et la protection des dépôts, RLRQ, c. I-13.2.24. Aux seules fins de cette ligne directrice, les expressions « institution » ou « institution financière » sont utilisées indistinctement pour référer aux entités visées par celle-ci. 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.
4	**Prise d'effet et processus de mise à jour**
4	La Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications est effective à compter du 23 janvier 2020. 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 23 janvier 2021. 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.	
5	**Introduction**	
5	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[5] et de fournisseurs externes pour mener à bien leurs activités.	
5	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.	
5	Les risques liés aux technologies de l'information et des communications (« TIC »)[6] peuvent avoir des conséquences défavorables tant au niveau financier et légal que sur les clients et la réputation d'une institution.	
5	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[7] contribuant à prévenir la matérialisation d'un incident majeur et à limiter ses impacts.	
5	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.	.

5	*Note en bas de page 5* *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.*	La nature de l'industrie de la technologie obligera toujours les organisations à utiliser des systèmes remplacés par des systèmes plus modernes. Nous recommandons d'ajouter à la recommandation en caractérisant les systèmes hérités comme ayant un ou plusieurs facteurs de risque (par exemple, un code exécutable non pris en charge qui ne s'exécute plus sur une version ultérieure d'un système) qui augmente le risque pour l'institution.
5	*Note en bas de page 6* *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.*	Est-ce que l'infogérance doit être traitée différemment de l'impartition en général? Quelle est la différence entre les deux? Une définition de ce concept permettrait une interprétation partagée.
5	*Note en bas de page 7* *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.*	
6	**Les types de risques liés aux technologies de l'information et des communications (TIC)**	
6	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.	Il est recommandé de remplacer **tous les risques** par **risques importants** afin de l'aligner sur l'approche fondée sur les risques de l'AMF.
6	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	L'accent mis sur l'exhaustivité dans cette section est incompatible avec les principes de saine gestion des risques et l'approche fondée sur les risques de l'AMF.

	d'envisager tous les types de risques susceptibles d'avoir des répercussions sur les objectifs de l'institution.	
6	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.	Peut-on simplifier le langage à des fins de clarté ? Proposition : « Le risque technologique devrait être évalué de manière holistique, en considérant tant les risques courants que les risques émergents (ex : incapacité à répondre adéquatement aux changements ou à l'arrivée de technologies nouvelles). » De plus, nous aimerions que l'Autorité précise les termes risque TIC versus risque technologique cités dans la ligne directrice, s'il existe une différence.
6	Au-delà des risques opérationnels dérivés des risques liés aux technologies, les risques stratégiques suivants[8] peuvent entraver l'atteinte des stratégies de l'institution et devraient être pris en considération : • Le risque de gouvernance technologique[9]. • Le risque de positionnement technologique[10]; • Le risque d'exécution technologique[11].	Tel que défini, le risque d'exécution technologique nous apparait comme étant du risque opérationnel (sous ensemble du risque d'exécution). Proposition : « Les risques suivants peuvent entraver l'atteinte des objectifs de l'organisation : • Le risque de gouvernance technologique9. • Le risque de positionnement technologique10 ; • Le risque d'exécution technologique11. »
6	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[12] 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.	L'attente d'une communication intégrée des risques est déjà exprimée dans la ligne directrice sur la gestion intégrée des risques.
6	*Note en bas de page 8* *Ces trois regroupements de risques stratégiques peuvent être décrits sous d'autres libellés selon la taxonomie établie par l'institution financière.*	
6	*Note en bas de page 9* *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.*	Clarifier la distinction entre les définitions énoncées en note en bas de page 9 et 11 afin qu'elles soient mutuellement exclusives.

6	*Note en bas de page 10* *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.*	Retirer le texte barré dans la colonne de gauche
6	*Note en bas de page 11* *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.*	Clarifier la distinction entre les définitions énoncées en note en bas de page 9 et 11 afin qu'elles soient mutuellement exclusives
6	*Note en bas de page 12* *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.).*	
7	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.	Est-ce que l'Autorité pourrait clarifier ce qu'elle entend par « … sans pour autant affaiblir le caractère particulier de chaque catégorie »?
7	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[13], 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.	Les éléments listés ne sont pas tous des risques. Certains sont des éléments d'environnement, d'autres sont des processus. Proposition : « 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[13], la gestion des changements, les opérations liées aux TIC, l'éthique, les ressources humaines et la propriété intellectuelle **sont quelques éléments** qui devraient être considérées **dans la conception des approches de gestion des risques liées** au TIC y compris dans l'élaboration de la taxonomie. »
7	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.	
7	*Note en bas de page 13* *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.*	
8	**La gouvernance des TIC**	
8	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[14]	
8	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.~~	Proposition de formulation pour la 1re phrase : « La gouvernance des TIC devrait refléter les changements qui s'opèrent au fil du temps **dans les bonnes pratiques reconnues par les organismes professionnels et internationaux et dans les objectifs d'affaires de l'institution. »** Cet ajustement permet de retirer la dernière phrase de ce paragraphe. 3e ligne : « confiance des marchés ». Expression généralement utilisée pour les marchés financiers. Est-ce l'intention ?
8	Le développement de la gouvernance des TIC devrait notamment considérer :	
8	• 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;	
8	• 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 de [quoi?] des TIC : la gouvernance ? À notre avis, si on précise bien la puce suivante, l'objectif est rencontré
8	• l'évaluation des plans de l'institution pour que les TIC supportent les processus d'affaires avec la capacité requise;	L'évaluation des plans de l'institution **afin de s'assurer de la contribution et de l'alignement des TIC avec ces plans**
8	• la prise en considération du cycle de vie des données dans la définition des responsabilités;	

8	• la mesure dans laquelle les TIC répondent aux obligations règlementaires, légales, contractuelles ainsi qu'aux standards et normes professionnelles et internationales;	
8	• 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.	Que veut-on dire ? Un exemple serait aidant pour illustrer ce point et clarifier l'objectif
8	Les divers éléments de l'encadrement établi par l'institution financière (stratégies, politiques, etc.) devraient considérer et arrimer entre eux les dispositions déjà existantes[15], inhérentes et utiles à la gestion des risques technologiques.	Que veut-on dire par dispositions déjà existantes? Préciser l'objectif de ce paragraphe. Cela semble plus un conseil qu'une attente concrète
8	*Note en bas de page 14* *Exemples : OCDE, G7, NIST, ISACA-Cobit et ISO.*	
8	*Note en bas de page 15* *Ces dispositions sont susceptibles d'avoir été définies et documentées distinctement à travers les années et pourraient comporter des contradictions.*	
9	**Rôles et responsabilités**	
9	**Le conseil d'administration**	Certaines responsabilités attribuées au conseil d'administration sont de nature opérationnelle et dépassent ou sont en conflit avec les attentes des administrateurs exprimées dans les lignes directrices sur la gestion des risques opérationnels et la gestion intégrée des risques.
9	En sus des attentes[16] déjà émises par l'Autorité, le conseil d'administration devrait notamment s'assurer :	
9	• que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement organisationnel éthique et sécuritaire dans l'exploitation des technologies;	
9	• d'échanger à l'égard des TIC avec les parties intéressées (internes et externes) afin de documenter sa compréhension des besoins et porter un jugement sur la conception actuelle et future de la gouvernance des TIC;	Cette section n'est pas claire.
9	• 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;	
9	• 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.	Nous recommandons de simplifier cette section en déclarant que le conseil d'administration devrait assurer une surveillance pour s'assurer que la gouvernance des TIC est périodiquement évaluée. Il faudrait minimalement clarifier ce que l'Autorité veut dire par « fonctions de support »
9	De plus, le conseil d'administration devrait s'assurer de la compétence des gestionnaires responsables du développement de l'encadrement des risques TIC et voir à l'assignation :	
9	• d'un responsable[17] pour les systèmes informatiques et les technologies de l'information qui supportent les objectifs de l'entreprise[18]	Cette responsabilité incombe à la haute direction
9	• d'un responsable à la haute direction, tel un chef de la sécurité de l'information[19] ou autre personne 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;	La précision « à la haute direction » impose un positionnement organisationnel. Nous croyons que la latitude doit être laissée à l'organisation. La formulation actuelle positionne le CISO comme une 2e ligne de défense : merci de confirmer. La complémentarité avec la puce suivante portant sur le CDO n'est pas évidente. La sécurité de l'information vise à protéger les données : disponibilité, confidentialité et intégrité.
9	• d'un responsable à la haute direction, tel un chef des données[20] ou autre personne de la seconde ligne de défense[21], lequel supervise l'encadrement approuvé à l'égard de la collecte, l'emmagasinage et l'utilisation des données à travers l'institution;	La précision « à la haute direction » impose un positionnement organisationnel. Nous croyons que la latitude doit être laissée à l'IF. La formulation actuelle positionne le CDO comme une 2e ligne de défense : merci de confirmer.

		La complémentarité avec la puce précédente portant sur le CISO n'est pas évidente. La qualité des données vise à fournir des données de qualité selon les objectifs établis en fonction de certains axes (exactitude et intégrité – exhaustivité – Actualité – Adaptabilité).
9	*Note en bas de page 16* *AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gouvernance, Septembre 2016.*	
9	*Note en bas de page 17* *Tel un directeur des technologies ou un chef des technologies ou de l'information[17]. Ces derniers portent parfois aussi le nom de Chief Technology Officer (CTO) ou Chief Information Officer (CIO).*	
9	*Note en bas de page 18* *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.*	
9	*Note en bas de page 19* *Ce poste porte parfois aussi le nom de Chief Information Security Officer (CISO).*	
9	*Note en bas de page 20* *Ce poste porte parfois aussi le nom de Chief Data Officer (CDO).*	
9	*Note en bas de page 21* *AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gouvernance, Septembre 2016.*	
10	• de responsables, au sein de la haute direction, pour l'ensemble des différents actifs informationnels et risques TIC présents dans l'institution.	Cette responsabilité incombe à la haute direction
10	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	Cette section est normative. Nous recommandons que la ligne directrice se concentre sur les résultats souhaités (par exemple, le conseil d'administration a une compréhension de l'état de préparation à la continuité des activités de l'organisation).

	de la disponibilité des opérations et systèmes TIC critiques. De plus, il devrait avoir une compréhension complète des procédures et processus d'escalade lors de brèches ou d'incidents de sécurité, incluant le moment où il devrait être notifié.	Modification proposée au paragraphe : De plus, il devrait avoir une **bonne** compréhension ~~complète des procédures et~~ **des** processus d'escalade lors de brèches ou d'incidents de sécurité, incluant le moment où il devrait être notifié.
10	**La haute direction**	
10	En sus des rôles et responsabilités qui lui sont généralement dévolus[22], la haute direction devrait notamment :	
10	• mettre en place une fonction TIC opérant sous la supervision d'une fonction de contrôle de la deuxième ligne de défense;	
10	• 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;	
10	• 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;	Nous proposons l'ajout suivant : « la prise de décision éclairée, **tout en équilibrant les risques, les contraintes de ressources et le besoin en termes d'innovation** »
10	• 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;	Fonction TI : à définir
10	• établir et maintenir une architecture d'entreprise comprenant les processus, informations, données et couches d'architectures d'applications, de technologies et de sécurité;	
10	• distinguer les personnes responsables ou imputables dans la gestion du risque TIC de celles qui doivent être consultées ou informées;	Préciser l'attente/l'objectif
10	• évaluer régulièrement, en collaboration avec les fonctions de conformité et d'audit interne, l'environnement de	Le terme « fonctions de conformité » devrait être remplacé par « fonctions de supervision », qui est le terme utilisé dans la LD

	contrôle (les autoévaluations, les revues d'assurance, l'identification des déficiences dans les contrôles, la conformité des processus supportés par les TIC aux lois[23], règlements et obligations contractuelles, etc.);	sur la gouvernance pour englober les équipes de 2e lignes de défense. Ne devrait-on pas ici mentionné la gestion des risques? « l'environnement de contrôle **et la gestion des risques** »
10	• revoir périodiquement les écarts de conformité (dont les dérogations approuvées par le conseil d'administration) aux encadrements établis pour le risque TIC[24]	
10	*Note en bas de page 22* *AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gouvernance, Septembre 2016.*	
10	*Note en bas de page 23* *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.*	
10	*Note en bas de page 24* *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 seront corrigées en temps opportun.*	
11	Dans l'établissement de la stratégie TIC, la haute direction devrait notamment :	Cette section est trop normative. Nous recommandons à l'AMF d'identifier les résultats souhaités plutôt que les moyens.
11	• établir une vue holistique des environnements d'affaires et des environnements TIC (actuels et à venir) afin d'identifier les initiatives de transformation requises;	Proposition : conserver uniquement « identifier les initiatives de transformation requises »
11	• 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;	Cette section n'est pas claire et est normative. Quel est l'objectif recherché? Est-il différent du point précédent?
11	• 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;	Proposition : « S'assurer de la cohérence avec les stratégies d'affaires »

11	• considérer l'utilisation des innovations technologiques dans la planification stratégique et les décisions d'architecture d'entreprise;	Cette section devrait être supprimée car elle suppose que les institutions ont le désir stratégique et l'appétit pour le risque d'envisager l'utilisation de technologies innovantes.
11	• 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[25] pour assurer la résilience des systèmes TIC.	Cette section n'est pas claire. Proposition : « s'assurer de la capacité à anticiper les incidents. »
11	De plus, en matière de sécurité de l'information, le responsable désigné de la haute direction devrait notamment :	
11	• 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;	
11	• définir des objectifs de sécurité de l'information clairs pour les systèmes, les services TIC, les processus et les personnes;	Nous proposons d'ajouter : « • définir des objectifs de sécurité de l'information clairs pour les systèmes, les services TIC, les processus et les personnes **alignés sur le plan stratégique de l'organisation** »
11	• appliquer la politique de sécurité de l'information à toutes les activités de l'institution et inclure l'information traitée chez les intervenants externes[26] au périmètre de l'institution;	
11	• déployer des contrôles pour les actifs[27] informationnels qui soient proportionnels à la criticité et la sensibilité desdits actifs;	
11	• conduire des régimes d'essais systématiques adéquats pour valider l'efficacité des contrôles mis en place;	Proposition : « Valider l'efficacité des contrôles » afin de ne conserver que l'objectif et non les moyens
11	• déployer des programmes de formation et de sensibilisation en sécurité de l'information;	
11	*Note en bas de page 25* *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.	
11	*Note en bas de page 26* *Dans le cas d'intervenants externes, il convient ici d'établir des ententes appropriées sur le traitement sécuritaire de l'information.*	
11	*Note en bas de page 27* *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.*	
12	• 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.	L'Autorité fait elle ici allusion à l'efficacité des contrôles selon une vue risques?
12	À l'égard de la reddition, la haute direction devrait notamment rendre compte :	
12	• des objectifs et des indicateurs recueillis liés aux TIC et à ses processus en temps opportun et de manière systématique;	Cette section n'est pas claire.
12	• 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;	Cette section est incompatible avec le préambule de la ligne directrice où il était fait référence à une saine pratique plutôt qu'à une meilleure pratique.
12	• 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.	
12	**Autres rôles**	Nous recommandons à l'AMF de profiter de cette section pour clarifier les responsabilités attribuées aux 3 lignes de défense en matière de risques liés aux TIC et pour bien distinguer les rôles faisant partie de la 1re et de la 2e ligne de défense (fonction TI, CISO, CDO, etc.).
12	La fonction de gestion des risques[28] de l'institution financière devrait superviser la fonction TIC de l'institution et prendre en charge la responsabilité de la gestion de l'ensemble des risques TIC, tant les risques opérationnels et stratégiques que ceux qui dérivent des innovations[29] liées aux TIC. Cette fonction devrait aussi assurer	La responsabilité de gestion des risques incombe à la première ligne de défense et non à la gestion des risques ; cette dernière encadre et surveille la 1LDD.

	un suivi rigoureux des risques importants ainsi qu'une veille des risques émergents liés aux TIC.	Proposition : « La fonction de gestion des risques28 de l'institution financière devrait encadrer et superviser la fonction TIC dans sa prise en charge […]. »
12	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.	
12	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.	Redondant avec le point précédent. À retirer.
12	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.	
12	*Note en bas de page 28* *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.*	
12	*Note en bas de page 29* *Par exemple, les risques de biais ou d'utilisation non éthique des technologies de données massives et d'intelligence artificielle.*	
13	**Probité et compétences**	**Les exigences que contient cette section sont déjà exprimées dans la ligne directrice sur les critères de probité et de compétence**
13	En concordance avec les attentes[30] déjà émises par l'Autorité, 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.	

13	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.	La Ligne directrice sur les critères de probité et de compétence prescrit déjà qu'il appartient à l'institution d'évaluer périodiquement si les membres des instances décisionnelles détiennent les attributs pertinents à l'exercice de leurs fonctions respectives (à la p 9). Elle aborde également la possibilité d'offrir des formations additionnelles, du mentorat ainsi que le recours à des ressources externes. Des mesures de contrôle et de suivi sont aussi requises (aux pp 13-14).
13	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.	Bien que la détermination des compétences et des ensembles de compétences soit une bonne pratique de gouvernance d'entreprise, il est démesuré de s'attendre à ce que les membres du conseil d'administration et la haute direction complètent les grilles d'aptitudes et de connaissances pour tous les risques liés aux TIC identifiés dans la présente directive (c.-à-d. Sécurité de l'information, gestion de crise, externalisation, cloud computing, continuité des affaires, gestion de programmes et de projets, 13 gestion du changement, opérations TIC, éthique, ressources humaines et propriété intellectuelle). Cependant, ce niveau de compétence est requis du personnel qualifié au niveau opérationnel. Nous craignons également que des évaluations de compétences et de connaissances similaires soient nécessaires pour toutes les autres taxonomies des risques. La Ligne directrice sur les critères de probité et de compétence prescrit que le niveau approprié d'expertise, de qualifications professionnelles, de connaissance ou d'expérience, peut être atteint de façon collective (i.e. la complémentarité des attributs propres aux personnes qui siègent dans les instances décisionnelles). Il faudrait distinguer selon le niveau (supervision ou opérationnel), selon l'instance décisionnelle (conseil d'administration, haute direction, audit) afin de demeurer

		cohérent avec la Ligne directrice sur la gouvernance. Les attentes et les besoins ne sont pas les mêmes selon le niveau de responsabilité et les fonctions visées. De même, la Ligne envisage les moyens d'actions afin de remédier à tout constat défavorable lors des évaluations. Le processus formel d'acquisition mentionné ici est couvert par un processus décisionnel détaillé (à la p 13).
13	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.	
13	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.	Qu'entend-t-on par postes clés ? membres du personnels, membres des instances décisionnelles ou les deux.
13	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.	
13	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.	
13	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.	L'attente d'un contrôle continu de la sécurité ou des antécédents est déraisonnable et normative. L'obligation d'appliquer cette attente aux personnes qui ont accès aux systèmes et aux données TIC n'est pas pratique étant donné l'étendue de l'accès à la technologie et aux données pour les opérations quotidiennes. Proposition : « … 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 risques importants de vols de données, de sabotage et de fraude.** »
13	*Note en bas de page 30* *AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur les critères de probité et de compétence, Juin 2012.*	
14	**Documentation à l'égard des TIC**	**Cette section est normative.**
14	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.	Très large : préciser objectif
14	Bien que la documentation puisse être préparée et maintenue par diverses composantes de l'institution, les éléments clés devraient toutefois être encadrés par la haute direction et approuvés par le conseil d'administration.	Très large : préciser objectif
14	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.	
14	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.	
14	Parmi les documents stratégiques qui sont issus des meilleures pratiques, l'institution financière devrait considérer :	La ligne directrice décrit les meilleures pratiques, ce qui n'est pas conforme aux commentaires précédents et à l'approche de l'AMF en matière de réglementation et de surveillance fondée sur les risques.
14	• la description des contextes auxquels fait face l'institution, les lignes d'affaires et les fonctions de support;	L'Autorité pourrait-elle préciser ce qu'elle veut dire par « contextes »?

14	• les composantes de la stratégie TIC, son plan stratégique et l'état de son déploiement;	
14	• la description de l'impact des risques TIC sur les stratégies d'affaires;	
14	• le registre des risques TIC et la matrice des risques et contrôles TIC;	
14	• l'architecture stratégique actuelle et visée des TIC;	
14	• les modèles et processus d'opérations des TIC.	L'Autorité pourrait-elle préciser ce qu'elle veut dire par « modèles d'opérations »?
15	**La gestion des risques liés aux TIC**	Cette section est normative et nous apparaît en conflit avec d'autres lignes directrices de l'AMF qui stipulent que les établissements devraient mettre en œuvre des stratégies de gestion des risques pour assurer l'alignement avec l'appétit pour le risque approuvé par le conseil d'administration, proportionné à la taille et à la complexité de l'organisation. Les attentes normatives telles que: • « l'ensemble des mesures prévues par l'institution, notamment les mesures de réponse et de recouvrement, devraient faire l'objet de simulations de crise » • « les intervenants et spécialistes externes requis par ces mesures devraient être préqualifiés et les termes et conditions contractuels préétablis » • « 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 » De plus, c'est la première fois qu'une que la segmentation selon Préparation, Traitement et Suivi est utilisée et nous trouvons que cela devrait être précisé.

		• La portion Préparation semble traiter d'éléments d'encadrements et préalables nécessaires à opérer des TIC • La portion Traitement semble parler d'éléments permettant de monitorer/identifier les risques (surveillance des opérations TIC par la fonction TIC) • La portion suivi se limite aux incidents majeurs/crises
15	L'Autorité s'attend à ce que l'institution financière considère l'ensemble des activités, provenant de sources et normes reconnues, nécessaires à la préparation, au traitement et au suivi requis dans la gestion des risques liés aux TIC.	
15	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.	Introduction à clarifier : On inclue des concepts généraux de gestion de risque et des concepts de gestion de crise sans départager clairement les 2 idées. Qu'entend-on par simulation de crise : test et exercice de type « table-top » ? Le terme simulation de crise peut avoir une connotation de stress test (ex : Macro stress test de la banque du Canada).
15	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.	À clarifier
15	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.	
15	**Préparation**	
15	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[31].	L'Autorité peut-elle clarifier ce qu'elle veut dire par des activités préparatoires? Préparatoires à quoi? Préparatoire à l'opérationnalisation des TIC?
15	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 :	
15	*Note en bas de page 31* *Les sections 4.1 à 4.4 abordent 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.*	
16	• d'assurer un alignement de l'ensemble des outils et des échelles d'évaluation des risques utilisés et une utilisation constante, convenue et transparente;	
16	• 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	« … et les locaux les abritant », ne s'agirait-il pas ici de sécurité physique? La portée des actifs informationnels est trop large (par exemple, le personnel, les composants logiciels des systèmes).

	(incluant ses diverses composantes matérielles et logicielles) et les locaux les abritant;	
16	• d'exploiter un cadre de classification[32] 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;	Que signifie la notion de cadre de classification pour la criticité des données ? Quel est son périmètre ?
16	• 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;	
16	• d'assurer un suivi adéquat et en temps opportun des activités de mitigation des risques présents au registre des risques TIC;	
16	• de suivre l'efficacité des mesures de mitigation, de même que le nombre d'incidents signalés afin de les corriger lorsque nécessaire;	
16	• 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.	L'Autorité pourrait-elle préciser ce qu'elle veut dire par « facteurs liés à la clientèle »?
16	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.	
16	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.	
16	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[33] les effets des évènements indésirables liés aux technologies de l'information et des communications.	
16	*Note en bas de page 32* *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.*	
16	*Note en bas de page 33* *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.*	
17	De plus, l'institution financière devrait :	
17	• 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;	Proposition : « identifier ~~tous~~ les points individuels de défaillance majeur potentielle dans les systèmes TIC… »
17	• 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;	
17	• considérer un ensemble plausible[34] d'événements et de scénarios de désastre, incluant des événements de cybersécurité, dans la planification des plans de recouvrement et de continuité;	
17	• inclure les dispositions régissant le recouvrement dans les délais requis et la conduite de tests périodiques dans la	

	stratégie de sauvegarde des données pour assurant l'efficacité des procédures.	
17	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.	
17	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.	Pourquoi ne pas parler simplement de la prise en considération de la désuétude comme facteur de risque important ? Proposition : « Afin de maitriser son exposition à des risques de sécurité et de stabilité, l'institution financière devrait assurer une gestion holistique, structurée et proactive de la désuétude applicative et des infrastructures ».
17	**Traitement**	
17	Dans le traitement des risques TIC, l'institution financière devrait notamment :	Les termes **traitement des risques** et **options de traitement des risques** doivent être clarifiés.
17	• déterminer les mesures nécessaires à la mise en œuvre des options de traitement des risques identifiés;	
17	• comparer les mesures déterminées avec les meilleures pratiques existantes et vérifier qu'aucune mesure nécessaire n'a été omise;	
17	• produire une déclaration des contrôles répertoriant les mesures et la justification de leur inclusion ou exclusion;	Quel est l'objectif de cet énoncé, d'assurer une supervision saine et prudente des options de traitement des risques ? La phrase ne nous semble pas claire.
17	*Note en bas de page 34* *L'institution devrait notamment considérer des scénarios à faible probabilité qui entraînent des impacts élevés de nature financière et non-financière (réputation, conformité, etc.).*	
18	• 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;	

18	• effectuer la maintenance et la réparation des éléments composant les systèmes TIC conformément aux encadrements établis par l'institution.	
18	De plus, l'institution financière devrait:	
18	• 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;	
18	• mettre à l'essai et maintenir les processus de détection précités afin d'assurer une connaissance adéquate et opportune des événements anormaux;	
18	• 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;	
18	• recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité);	
18	• exécuter et réviser les activités planifiées pour empêcher l'expansion d'un évènement auprès d'autres systèmes TIC, en atténuer les effets et résoudre l'incident.	
18	L'accès aux dispositifs[35] 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.	
18	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.	L'utilisation de « infrastructure » me semble inadéquate, car trop restreinte par rapport au support requis aux opérations critiques. Il faudrait inclure les technologies, applications, etc.
18	*Note en bas de page 35*	

	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.	
18-19	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 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[36].	
19	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.	Est-ce que les mécanismes de protection correspondent au traitement?
19	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).	
19	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.	L'Autorité pourrait-elle clarifier ce qu'elle veut dire par « attributs »?
19	**Suivi**	

19	En concordance avec les attentes[37] déjà émises, 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 aviser promptement les parties intéressées internes et externes, dont l'Autorité, susceptibles de subir un préjudice d'importance significative suite à un incident opérationnel majeur (cyberincident, dysfonctionnement des systèmes, etc.).	
19	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 :	
19	• coordonner les réponses et les activités de recouvrement requises suite à la notification aux parties prenantes internes et externes;	
19	• contribuer à minimiser les impacts sur la clientèle;	
19	• rendre compte des incidents selon des critères préétablis;	
19	• partager l'information utile contribuant au rehaussement de la sécurité de l'information;	Partager l'information à qui?
19	• gérer les relations publiques et l'impact sur la réputation de l'institution.	
19	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 :	« incident **TIC** majeur ». Il y a une certaine confusion dans la ligne directrice entre un incident opérationnel majeur et un incident TIC majeur.
19	*Note en bas de page 36* *Shadow IT (parfois Rogue IT) est aussi un terme utilisé pour désigner des systèmes TIC mis en œuvre au sein d'organisations sans approbation.*	
19	*Note en bas de page 37* *AUTORITÉ DES MARCHÉS FINANCIERS, Ligne directrice sur la gestion de risque opérationnel, Décembre 2016.*	
20	• explorer les données recueillies dans ses infrastructures par ses systèmes de détection;	
20	• identifier et mesurer les impacts de l'incident;	

20	• mitiger ou accepter et documenter le risque des nouvelles vulnérabilités identifiées;	
20	• formuler et communiquer aux parties prenantes internes les leçons apprises dans la résolution de l'incident;	
20	• recevoir, analyser et répondre aux vulnérabilités dévoilées par des sources internes ou externes (tests conduits à l'interne, bulletins ou recherches spécialisées en sécurité).	
20	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 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.	
21	**Normes complémentaires aux lignes directrices de l'Autorité**	Nous pensons que cette section devrait être déplacée en annexe puisqu'elle fait état d'exemples des bonnes pratiques énoncées par des organismes professionnels et internationaux. On semble vouloir y former le lecteur aux éléments importants d'une gestion des TIC et aux éléments qui devraient, par conséquent, faire partie des modes de fonctionnement d'une institution. Nous croyons que ceci n'est pas du ressort d'une ligne directrice.
21	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, considèrent les pratiques spécifiques aux TIC qui ont fait leurs preuves et sont généralement reconnues.	
21	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.	

21	Dans cette perspective, les pratiques[38] 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.	
21	**Sécurité des TIC**	
21	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.	
21	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[39] 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.	
21	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.	
21	*Note en bas de page 38* *Les thèmes abordés dans cette section sont tirés des meilleures pratiques recommandées par différents organismes nationaux ou internationaux dont notamment le NIST, Cobit, G7 et ISO.*	
21	*Note en bas de page 39* *Par exemple : coupe-feu, contrôle d'accès réseau, dispositif de détection et prévention d'intrusion, antivirus, encryption, outil de suivi et analyse des journaux.*	Nous proposons de changer le mot « encryption » pour le terme « chiffrement »
21	*Note en bas de page 40*	

	Cela comprend tout autant les accès des usagers réguliers ou à hauts privilèges que les accès à distance.	
21-22	L'institution financière devrait s'assurer que l'accès[40] 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.	
22	Les privilèges d'accès octroyés devraient être établis sur la base des principes « besoin de savoir », « jamais seul », « 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.	Qu'est-ce que le principe du « jamais seul »?
22	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.	
22	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[41] et des exercices de type « Red Team [42] ».	
22	Dans l'évaluation des risques de la sécurité de l'information, l'institution financière devrait notamment :	
22	• 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;	
22	• 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.	
22	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[43] et son environnement d'affaires.	
22	Les rôles d'ingénierie et d'architecture dans le développement d'une sécurité de l'information adéquate pour les systèmes TIC de	Nous ne sommes pas certains de bien comprendre les attentes formulées dans ce paragraphe.

	l'institution devraient être accompagnés d'une ségrégation adéquate entre la sécurité opérationnelle et la gestion des risques.	
22	*Note en bas de page 41* *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.*	Nous convenons que « les tests d'intrusion et les évaluations de vulnérabilités ne sont pas des substituts pour l'évaluation des risques TIC », mais l'évaluation des risques doit tenir compte de ces tests. Devrait-on le préciser?
22	*Note en bas de page 42* *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.*	
22	*Note en bas de page 43* *Ceci fait référence au processus traitant de la planification et de la conception des actifs informationnels jusqu'à leur déclassement et élimination.*	
23	**Opérations liées aux TIC**	La quasi-totalité de cette section semble redondante avec des éléments déjà mentionnés dans les sections précédents
23	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.	
23	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 :	

Commentaires de Desjardins : Consultation publique – Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications (Janvier 2020)