BAC IBC | Bureau d'assurance du Canada
Insurance Bureau of Canada

Mémoire sur la Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications

Présenté à l'Autorité des marchés financiers
M^e^ Anne-Marie Beaudoin
Secrétaire générale

Février 2019

BAC IBC | Bureau d'assurance du Canada
Insurance Bureau of Canada

Le Bureau d'assurance du Canada est l'association qui représente les sociétés privées d'assurance de dommages. L'industrie de l'assurance de dommages joue un rôle de premier plan dans l'économie québécoise en permettant à la population de se prémunir contre des sinistres pouvant avoir un impact important sur sa sécurité financière en protégeant son patrimoine.

Pour mener à bien sa mission, le BAC :

- maintient des relations suivies avec le gouvernement, les consommateurs et toute autre partie concernée;
- intervient dans des dossiers règlementaires et législatifs;
- fait équipe avec le gouvernement et avec divers intervenants dans des initiatives de prévention;
- informe le grand public en matière d'assurance, tant dans le quotidien qu'en situation de crise;
- élabore des campagnes de prévention et de sensibilisation à l'intention des consommateurs.

Le BAC est non seulement le porte-parole de l'Industrie, mais aussi un précieux partenaire pour les gouvernements, les intervenants du milieu de l'assurance de dommages et les consommateurs.

Bureau d'assurance du Canada
1981, avenue McGill College, bureau 620
Tour BNP Paribas
Montréal (Québec) H3A 2Y1

Février 2019

TABLE DES MATIÈRES

1. CONTEXTE

Dans ses grandes lignes, les commentaires qui suivent ont déjà fait l'objet de discussions avec l'Autorité des marchés financiers (l'Autorité) notamment lors d'une rencontre tenue le 18 octobre 2018 avec des représentants de l'Autorité, des assureurs membres du BAC et de la permanence du BAC.

Le BAC réitère ci-après les commentaires faits verbalement et expose la position de ses membres de façon détaillée en espérant que cet exercice permettra de faire évoluer l'approche de l'Autorité relativement à ce projet de ligne directrice.

2. INTRODUCTION

2.1. Cohésion des lignes directrices

Le BAC est d'avis qu'il est important de situer la Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications (Ligne directrice TIC) dans la structure des lignes directrices mises en place par l'Autorité au cours des dix dernières années.

Les trois assises de l'encadrement, soit la gouvernance, la gestion intégrée des risques (GIR) et la conformité, font toutes l'objet d'une ligne directrice qui contient les principes applicables à l'ensemble des risques. Ces risques font l'objet de lignes directrices qui énoncent des principes qui leur sont spécifiques. L'Autorité a également créé des lignes directrices propres à certaines activités ou à des aspects importants d'un risque. Par exemple, les risques liés à l'impartition et à la continuité des activités, qui sont des risques opérationnels, font l'objet d'une ligne directrice spécifique dont les principes viennent compléter ceux qui se retrouvent dans la Ligne directrice sur la gestion du risque opérationnel.

Le risque des technologies de l'information et des communications (« TIC ») est le risque lié à l'utilisation des TIC dans le cours des opérations d'une organisation. Comme pour la majorité des risques opérationnels, le risque TIC comporte des enjeux de disponibilité des services et de continuité des affaires, d'adaptation aux changements et de protection des renseignements personnels. Les particularités du risque TIC sont l'atteinte à l'intégrité des données et à la sécurité rendues vulnérables par la perpétration de cyberattaques. La Ligne directrice TIC devrait conséquemment se retrouver sous la Ligne directrice sur la gestion du risque opérationnel et porter sur ces particularités.

Les membres du BAC comprennent l'importance du risque lié à la gestion des TIC et y consacrent des efforts depuis déjà de nombreuses années. Dans leur stratégie d'affaires, il occupe depuis longtemps une place prioritaire. Les lignes directrices existantes, notamment la Ligne directrice sur la gestion intégrée des risques, énoncent des attentes en ce qui concerne le risque stratégique et celles-ci sont respectées de la même manière que les attentes qui visent les risques opérationnels. La présente ligne directrice, qui comporte pour la première

fois un volet éducatif, semble sous-estimer la compétence et la maturité des institutions financières en ce qui a trait à la gestion du risque TIC. Au fil des ans, les assureurs de dommages ont intégré à leurs pratiques les attentes qui se retrouvent dans les différentes lignes directrices et ils gèrent leurs risques de façon intégrée comme le demande l'Autorité. Malheureusement, la nouvelle approche adoptée pour la rédaction de cette ligne directrice fait en sorte que les TIC doivent être traités comme une « compagnie » dans la « compagnie », et cette approche va à l'encontre d'une gestion intégrée des risques.

Même si l'Autorité réfère à la Ligne directrice sur la gouvernance, en indiquant qu'il s'agit de ses attentes « en sus », on se rend rapidement compte, en lisant les 12 pages qui suivent à propos de la gouvernance, qu'on reprend tous les principes qui se retrouvent déjà dans la Ligne directrice sur la gouvernance ainsi que dans la section portant sur la gouvernance de la Ligne directrice sur la gestion du risque opérationnel. Dans plusieurs cas, seul le mot « TIC » est ajouté dans l'énoncé.

Le BAC questionne le changement d'approche de l'Autorité qui reprend dans cette ligne directrice tous les principes qui se retrouvent déjà dans les lignes directrices cadres (gouvernance, GIR et conformité) pour en faire une ligne directrice « autoportante ». À sa lecture, le BAC constate qu'elle a été écrite en se basant sur les principes internationaux, et ce, sans tenir compte du cadre réglementaire déjà en place au Québec, ce qui n'est pas opportun selon nous.

Afin d'illustrer nos propos, nous avons retracé de nombreux exemples de principes et d'exigences qui se retrouvent déjà dans d'autres lignes directrices applicables aux risques TIC (voir l'Annexe 1 - TABLEAU). Cette situation crée beaucoup d'ambiguïté, de confusion et une absence certaine de convivialité lors de la consultation.

2.2. Approche basée sur des principes

Comme mentionné au début de chaque ligne directrice, l'approche de l'Autorité en matière de surveillance est basée sur des principes dans le but de permettre aux assureurs de déterminer eux-mêmes les stratégies, les politiques et les procédures pour la mise en œuvre de ces principes. Or, le BAC remarque que pour la Ligne directrice TIC, l'Autorité a adopté une approche beaucoup plus prescriptive et détaillée que dans les autres lignes directrices.

Plusieurs des attentes concernent l'organisation des activités liées aux TIC, ce qui constitue de la gestion opérationnelle. D'ailleurs, à plusieurs reprises dans la ligne directrice on parle de « gestion des TIC » et non de « gestion du risque TIC ». On s'éloigne ainsi beaucoup de l'approche basée sur les principes. Le BAC est d'avis qu'une telle ingérence dans la façon d'organiser les opérations n'est pas appropriée.

2.3. Structure et langage

Comme mentionné précédemment, la rédaction de la Ligne directrice TIC est très prescriptive et diffère de ce que l'on retrouve généralement tant pour le vocabulaire utilisé que dans la structure, ce qui rend le texte difficile à suivre et à comprendre et crée de la confusion. Il aurait été préférable d'amender les autres lignes directrices, lorsque nécessaire, pour viser les enjeux spécifiques aux TIC plutôt que de tenter d'y intégrer tous les principes existants. Ainsi, la Ligne directrice TIC traiterait uniquement des attentes spécifiques de l'Autorité relativement aux risques liés aux TIC et se limiterait à la gestion des risques liés aux TIC. Le BAC note aussi l'utilisation de termes et d'expressions qu'on ne retrouve pas dans les autres lignes directrices, ce qui complique l'interprétation de ce projet de ligne directrice et rend difficiles les liens avec les autres lignes directrices.

Certaines sections ne contiennent pas d'énoncé de principe (encadré), ce qui fait en sorte que les attentes de l'Autorité ne sont pas exprimées clairement dans chaque section et entraîne un manque d'uniformité.

En ce qui concerne la gouvernance, l'Autorité a décidé de réitérer ses attentes relativement aux rôles et responsabilités des administrateurs dans chacune des lignes directrices même lorsque ces attentes se retrouvent déjà dans la Ligne directrice sur la gouvernance. Cette façon de faire rend déjà complexe la consultation des lignes directrices de façon générale tant pour les responsables de la conformité que pour les administrateurs. En plus, dans la Ligne directrice TIC, les concepts en matière de gouvernance et de gestion des risques se retrouvent éparpillés un peu partout au lieu d'être regroupés dans une section qui leur est réservée.

Le BAC note également que dans plusieurs cas, la formulation utilisée ou les phrases trop longues rendent le texte difficilement compréhensible. Par exemple, on peut lire à la page 8 :

> *« Les parties intéressées à la gestion des risques TIC occupent plusieurs rôles qui requièrent des ensembles distincts de compétences dont les objectifs se rapportent à des niveaux variables d'éducation, de qualification, d'expérience, de connaissances et d'aptitudes techniques et/ou comportementales. »*

Sachant que l'Autorité travaille actuellement sur la convivialité de la consultation des lignes directrices, le BAC s'explique mal comment elle peut proposer une ligne directrice qui s'éloigne autant de la structure de toutes les autres et qui est aussi difficile à comprendre.

2.4. Rôle du conseil d'administration

La Ligne directrice TIC augmente de façon importante les rôles et responsabilités des membres du conseil d'administration et leur attribue, dans plusieurs cas, des tâches de nature opérationnelle qui ne leur appartiennent pas. Le rôle des membres du conseil d'administration est de : « *superviser la gestion effectuée par la haute direction. Il devrait donc s'assurer de la mise en place des dispositifs nécessaires à l'atteinte d'une saine gouvernance et voir à leur efficacité,*

notamment en prenant connaissance des rapports pertinents provenant de la haute direction et découlant de l'application de ces dispositifs (...) » comme mentionné dans la Ligne directrice sur la gouvernance. Or, dans la présente ligne directrice, on demande aux administrateurs, par exemple de définir de l'information (page 6), d'évaluer dans quelle mesure la gouvernance des TIC opère efficacement (page 6), de s'assurer que des ressources suffisantes et adéquates soient disponibles (page 7), d'examiner et évaluer les besoins courants et futurs (page 7), des rôles et responsabilités qui devraient plutôt être attribués à l'audit interne ou à la haute direction.

Pour la composition du conseil d'administration, on vise normalement une composition mixte de compétences, mais il est plutôt précisé dans la Ligne directrice TIC que les membres doivent avoir des connaissances en TI alors qu'aucune exigence de compétence spécifique n'est requise pour d'autres champs de compétence importants comme l'actuariat par exemple.

Le BAC réitère que l'Autorité devrait adopter une approche « à guichet unique » en ce qui a trait à ses attentes quant aux rôles et responsabilités attribués au conseil d'administration qui sont communs à toutes les activités de l'organisation en les regroupant dans la Ligne directrice sur la gouvernance. Une telle façon de procéder conférerait au conseil d'administration une marge de manœuvre suffisante pour choisir la manière dont il doit agir pour répondre aux attentes formulées dans les lignes directrices (en fonction de la nature, de la taille et de la complexité des activités de leur institution) et simplifierait l'identification de leurs obligations et responsabilités.

Finalement, le BAC est d'avis qu'il y aurait lieu de préciser qui sont les « officiers responsables » et quels sont leurs rôles et leur imputabilité puisqu'il s'agit d'un terme qui n'est pas utilisé dans les autres lignes directrices. Aussi, pour la première fois, on parle du président-directeur général (page 8), ce qui pourrait créer des problèmes d'application puisqu'une telle fonction n'existe pas dans toutes les organisations. De plus, les niveaux hiérarchiques ne sont pas clairement exprimés et on n'utilise pas la même formulation en ce qui a trait aux lignes de défense que celle utilisée dans la Ligne directrice sur la gouvernance. Conséquemment, le BAC recommande de revoir la terminologie de façon à ce qu'elle soit harmonisée avec les autres lignes directrices.

3. COMMENTAIRES

Les commentaires suivants ont notamment pour objectif de proposer une autre structure pour la Ligne directrice TIC que celle proposée afin qu'elle soit cohérente avec les autres lignes directrices. Cette nouvelle structure permettrait également de rencontrer l'objectif de l'Autorité de favoriser la convivialité de la consultation des lignes directrices. À cet égard, le BAC recommande notamment de retirer les nombreuses redondances ce qui évitera de créer de la confusion quant aux attentes et permettra aux assureurs d'adopter une approche globale de gestion des risques. En effet, isoler une ligne directrice, comme le fait l'Autorité

pour celle-ci, entraînera une charge de travail additionnelle importante en termes de conformité pour les assureurs. Ceux-ci devront se livrer à un exercice de comparaison long et fastidieux pour s'assurer que la mise en application des attentes pour une même activité respecte tant la Ligne directrice TIC que l'ensemble des lignes directrices.

Le mémoire contient les commentaires généraux du BAC concernant la Ligne directrice TIC. Pour la première fois, considérant l'ampleur des éléments à porter à l'attention de l'Autorité, le BAC a commenté de manière spécifique la majorité des paragraphes dans un tableau joint en annexe. Ce tableau comprend une colonne intitulée « Redondances » qui vise à illustrer le nombre important de redondances et les risques de confusion que cela entraîne avec les autres lignes directrices et avec le projet de Ligne directrice TIC. Il comprend également une colonne où l'on retrouve les commentaires détaillés du BAC. Plusieurs de ces commentaires proposent un retrait complet de sections ou de paragraphes en indiquant pourquoi un tel retrait est suggéré et indique également comment le texte devrait être modifié dans l'éventualité où l'Autorité décide de le conserver.

3.1. Prise d'effet et processus de mise à jour (p. 4)

L'Autorité prévoit que les assureurs doivent mettre en œuvre cette ligne directrice pour le 1er juin 2020. Ce délai est jugé irréaliste. Nous portons à votre attention qu'en 2013, le Comité de Bâle a émis des principes pour la protection des données et que, bien que les banques avaient trois ans pour s'y conformer, à la date butoir, une seule y était parvenue. En 2018, le Comité de Bâle a émis un document[1] pour expliquer pourquoi celles-ci n'avaient pas été en mesure de mettre en œuvre ces principes.

Le BAC recommande de prévoir une période de trois ans pour l'entrée en vigueur de la ligne directrice, soit le 1er juin 2022.

3.2. Introduction (p. 5)

Le BAC souhaite que l'Autorité précise dans son introduction comment cette ligne directrice se positionne par rapport aux autres lignes directrices. En effet, la ligne directrice sur la gestion intégrée des risques a pour objectif d'émettre des principes de gestion prudentielle pour l'ensemble des risques de l'institution. Lorsque l'Autorité a jugé nécessaire de venir préciser des orientations prudentielles concernant un risque en particulier, l'interaction entre celle-ci et les autres lignes est précisée. Par exemple, dans la Ligne directrice sur la gestion du risque opérationnel, l'Autorité précise à la page 6 :

> *Compte tenu de sa nature générale, cette ligne directrice se situe dorénavant en amont de l'encadrement plus spécifique portant sur des sujets liés au risque opérationnel, notamment*

[1] Basel Committee on Banking Supervision, *Progress in adopting the "Principles for effective risk data aggregation and risk reporting"*, June 2018, https://www.bis.org/bcbs/publ/d399.htm.

> *sur la gestion de la continuité des activités[10] ainsi que la gestion des risques liés à l'impartition[11] et à la criminalité financière[12]. Conséquemment, tout nouvel encadrement prudentiel en matière de risques inhérents aux personnes, processus, systèmes ou évènements externes nécessitera que des précisions soient apportées aux grands principes énoncés dans la présente.*

Le BAC recommande de retirer les deux derniers paragraphes de l'introduction. L'avant-dernier paragraphe est redondant avec le dernier paragraphe de la section « Prise d'effet et processus de mise à jour ».

Quant au dernier paragraphe de l'introduction, le BAC demande son retrait pour deux raisons. Premièrement, une partie de ce paragraphe est redondante quant à l'importance de bien comprendre les risques et de s'assurer qu'ils soient pris en considération. Deuxièmement, la mise en garde quant au fait que la ligne directrice ne couvre pas tous les aspects de la gestion des risques liés aux TIC semble viser la gestion opérationnelle des TIC et non la gestion des risques. Le BAC comprend que l'encadrement de la gestion des risques TIC a pour objectif d'émettre des principes afin que les institutions puissent atteindre leurs objectifs stratégiques tout en ayant une bonne gestion prudentielle. Il n'a pas pour objectif d'établir une liste exhaustive de méthodes précises pour encadrer le risque.

3.3. Le cadre de gouvernance des technologies de l'information et des TIC (p. 6)

L'objectif de la présente ligne directrice est de faire connaître les attentes de l'Autorité quant à la gestion des risques liés aux TIC. Toutefois, la structure actuelle expose des attentes au niveau de la gouvernance, de la gestion du risque et des pratiques de gestion des technologies de l'information. Il est important de faire une distinction entre ces différentes attentes et d'émettre uniquement celles qui concernent la gestion des risques liés aux TIC.

Le BAC recommande de modifier le nom de cette section pour « Gouvernance de l'institution financière ». Cette modification permet d'harmoniser cette ligne directrice avec les autres lignes directrices pertinentes notamment avec la Ligne directrice sur la gestion du risque opérationnel. Ainsi, on évitera de sous-entendre que l'institution doit avoir deux cadres de gouvernance, ce qui n'est pas le cas. Pour cette même raison, le BAC suggère de modifier l'attente pour qu'elle se lise comme suit : « *L'Autorité s'attend à ce que le conseil d'administration et la haute direction mettent en place une solide structure de gouvernance afin de favoriser la conformité des orientations en matière de gestion du risque des technologies de l'information et des communications* ».

Comme mentionné en introduction, les rôles et responsabilités qui y sont précisés ne devraient pas reprendre ceux déjà prévus dans les autres lignes directrices. Une telle répétition alourdit le texte et complexifie la lecture de l'ensemble des lignes directrices, sans ajouter de valeur sur le plan de la gouvernance. Aussi, deux textes qui sont libellés

différemment pourront être interprétés de deux façons et créer de la confusion quant à la portée des attentes de l'Autorité.

L'Autorité devrait identifier uniquement les attentes supplémentaires qui s'appliquent au cadre précis de la gestion des risques liés aux TIC. Par exemple, la Ligne directrice sur la gestion du risque opérationnel vient préciser, à la page 7, cinq responsabilités supplémentaires pour le conseil d'administration et six responsabilités supplémentaires pour la haute direction. De son côté, la Ligne directrice TIC prévoit dix responsabilités à la section 1, neuf responsabilités à la section 1.2 et huit responsabilités à la section 1.5. Or, plusieurs de ces responsabilités sont redondantes avec ce qui est déjà prévu dans d'autres lignes directrices.

Le nombre de responsabilités attribuées au conseil d'administration est démesuré et celles-ci ne cadrent pas dans le rôle de surveillance du conseil d'administration puisqu'elles sont souvent de nature opérationnelle. D'ailleurs, certaines de ces responsabilités pourraient être perçues comme une ingérence dans la prérogative de gestion de la haute direction et du responsable de la gestion des risques. C'est le cas notamment pour les deux dernières puces de la page 6.

Finalement, le BAC recommande que les rôles et responsabilités supplémentaires du conseil d'administration soient déplacés à un même endroit dans la ligne directrice, soit à la section 1.2 (rôles et responsabilités). Cette section devrait être renommée « Rôles et responsabilités du conseil d'administration ».

3.4. Compétence (p. 7)

Cette section devrait être complètement retirée puisqu'elle reprend en grande partie les attentes énoncées dans la Ligne directrice sur les critères de probité et de compétence. L'encadré de la page 7 devrait être déplacé à la section 1.2 (Rôles et responsabilités) et modifié afin de préciser que le conseil d'administration doit *« s'assurer de bien comprendre les risques liés aux TIC notamment quant à l'utilisation, les directions et les tendances des TIC »*.

3.5. Rôles et responsabilités (p. 8)

Le BAC recommande de fusionner cette section avec la section subséquente qui se trouve à la page 9 afin qu'elle se lise comme suit : « Rôles et responsabilités du conseil d'administration ».

L'attente prévue à cette section est redondante avec la Ligne directrice sur la gouvernance qui prévoit déjà l'obligation de définir clairement les rôles et responsabilités du conseil d'administration et de la haute direction. De plus, tous les rôles et responsabilités qui sont déjà précisés dans les autres lignes directrices devraient être retirés pour les raisons notamment citées aux sections 2.3 et 3.3 du présent mémoire.

3.6. Le conseil d'administration (p. 9)

Comme précisé plus haut, le BAC recommande de fusionner cette section afin qu'elle se lise comme suit : « Rôles et responsabilités du conseil d'administration ».

3.7. La haute direction (p. 10)

La section sur la haute direction devrait être retirée complètement de la ligne directrice à moins d'y préciser des rôles et responsabilités qui concernent spécifiquement la gestion des risques liés aux TIC qui ne sont pas prévus dans les autres lignes directrices. Actuellement, les rôles et responsabilités qui y sont indiqués sont redondants avec les rôles et responsabilités prévus dans les autres lignes directrices. Dans certains cas, ceux-ci sont repris intégralement et cela crée uniquement de la redondance. Dans d'autres cas, les rôles et responsabilités sont décrits différemment, ce qui engendre de la confusion puisqu'il faut essayer de déterminer qu'elle est l'exigence supplémentaire par rapport aux autres lignes directrices. Dans certains cas, les exigences sont les mêmes malgré la différence de vocabulaire.

Lorsque ces rôles et responsabilités ne sont pas redondants, ils concernent la gestion opérationnelle des TIC et non la gestion des risques TIC. Par exemple, la deuxième puce de la page 10 précise une responsabilité concernant la gestion opérationnelle et non de la gestion des risques. C'est le cas également pour la quatrième puce de la page 11 qui est un rôle lié à la performance organisationnelle et non à la gestion prudentielle. Considérant l'objectif de la Ligne directrice TIC et les attentes émises par l'Autorité au niveau de la gestion des risqués liés aux TIC, le BAC recommande de retirer tous les rôles et responsabilités liés à la gestion des affaires et à la performance organisationnelle.

3.8. Rôles des lignes de défense (p. 11)

Actuellement, la ligne directrice ne prévoit pas de rôles et responsabilités supplémentaires à ceux que l'on retrouve dans les autres lignes directrices. Conséquemment, cette section devrait être retirée complètement de la ligne directrice à moins d'y préciser les rôles et responsabilités pour les lignes de défense qui sont spécifiques aux TIC. Dans cette éventualité, le BAC suggère que l'Autorité utilise l'attente prévue à la page 8 de la Ligne directrice sur la gestion du risque opérationnel. Pour les risques liés aux TIC, l'attente se lirait comme suit : « Afin d'optimiser la gestion du risque TIC, l'institution financière devrait disposer d'une structure de gouvernance fiable en s'inspirant du modèle des trois lignes de défense ».

Dans l'éventualité où l'Autorité précise des rôles et responsabilités supplémentaires pour les lignes de défense, le BAC recommande d'harmoniser cette section avec les autres sections sur les rôles et responsabilités. À cet égard, il y a lieu d'ajouter « et responsabilités » après « Rôles » et d'ajouter comme paragraphe introductif : « En sus des rôles et responsabilités qui leur sont généralement dévolus, les lignes de défense devraient notamment : ».

3.9. Structure de la gouvernance des TIC (p. 12)

La section 1.4 sur la structure de la gouvernance des TIC devrait être retirée complètement. Elle n'apporte pas de précision ou de spécification quant à la gestion des risques liés aux TIC. De plus, chaque institution doit pouvoir constituer sa structure de gouvernance selon ce qu'elle juge le plus efficient et pertinent. Les attentes de cette section sont inutilement prescriptives et prévoient une façon de faire spécifique sans préciser les objectifs souhaités. Par exemple, la quatrième puce indique que l'institution devrait s'assurer de la surveillance de l'encadrement relatif à la sécurité de l'information par un haut dirigeant et précise que celui-ci est souvent appelé chef de la sécurité (CISO). La ligne directrice associe le rôle de surveillance à un CISO alors que c'est le rôle du chef de la gestion des risques comme membre de la haute direction. D'ailleurs, la ligne directrice a mis le rôle du CISO à la deuxième ligne de défense alors que certaines institutions peuvent le placer à la première ligne de défense.

Au lieu de préciser des titres qui attribuent des responsabilités spécifiques à chacun, la Ligne directrice TIC devrait mettre l'accent sur les fonctions de ces personnes. Cette manière de procéder permettrait à l'institution d'attribuer les responsabilités aux personnes les mieux qualifiées pour exercer ces fonctions. Cela permettrait également le cumul des fonctions pour certains rôles.

Dans certains cas, les rôles et responsabilités de chacun doivent être distincts et indépendants pour s'assurer que le cadre de gouvernance soit robuste. Actuellement, l'expression « ségrégation adéquate entre la sécurité opérationnelle et la gestion des risques » ne nous apparaît pas claire et diverge des expressions utilisées dans les lignes directrices sur la gouvernance et la gestion intégrée des risques. Par exemple, l'une des attentes pourrait indiquer que l'Autorité s'attend à ce que l'ensemble des risques liés aux TIC ne soit pas assigné à une même personne et que ces responsabilités soient réparties parmi les différentes lignes de défense.

3.10. Préceptes et propriétés du cadre de gouvernance des TIC (p. 14)

Les préceptes qui sont énumérés à la section 1.5 s'inspirent de la norme ISO/IEC 38-500[2] qui est un modèle de bonne gouvernance. Or, il existe d'autres modèles de bonne gouvernance qui pourraient mieux convenir à certaines institutions en fonction de leur cadre de gouvernance. Toutefois, en venant apporter des précisions inspirées par la norme ISO/IEC 38-500, l'Autorité semble prioriser ce cadre au lieu des autres normes qu'elle mentionne à la note de bas de page 17. L'imposition d'un modèle de gouvernance trop précis limite la flexibilité et la capacité de l'institution à se démarquer et ultimement à créer de la valeur à travers ses technologies de l'information. Elle mine également la confiance de l'institution dans la

[2] ISO/IEC 38500 :2015, Technologies de l'information – Gouvernance des technologies de l'information pour l'entreprise, https://www.iso.org/fr/standard/62816.html

sélection d'une autre norme de gouvernance pour se conformer aux attentes de l'Autorité puisqu'elles ne sont pas précisées contrairement à celles de la norme ISO/IEC 38-500. De plus, les normes évoluent rapidement, de sorte qu'il serait préférable de ne pas référer à une norme en particulier.

Le BAC s'interroge également sur la pertinence d'avoir une section sur la gouvernance aussi imposante. Les autres lignes directrices qui traitent d'un risque précis n'ont pas une section sur la gouvernance qui crée un cadre de gouvernance complètement séparé de celui proposé par la Ligne directrice sur la gouvernance. Par exemple, la Ligne directrice sur le risque opérationnel vient préciser à la page 8 les attentes supplémentaires de l'Autorité quant au risque opérationnel et met l'accent sur l'importance de disposer d'une structure de gouvernance fiable inspirée des trois lignes de défense prévue à la Ligne directrice sur la gouvernance. De la même façon, les commentaires quant à la gouvernance dans la Ligne directrice sur la gestion des risques liés à l'impartition se limitent à attribuer deux responsabilités supplémentaires à la haute direction et au conseil d'administration pour les ententes d'impartition.

Conséquemment, le BAC recommande de retirer complètement cette section à l'exception du paragraphe qui commence par « Les divers éléments de l'encadrement des TIC (...) » de la page 17. Celui-ci pourrait être déplacé dans l'introduction à la page 5.

De plus, le choix du terme « précepte » est surprenant, car l'objectif d'une ligne directrice est d'émettre des principes et de donner la liberté aux institutions d'orienter ses activités de manière à répondre aux attentes. Si cette section est conservée, le BAC recommande de modifier ce terme par « principe ».

3.11. Documentation de l'environnement des TIC (p. 17)

Le BAC recommande de conserver l'attente de l'Autorité dans l'encadré de la section 1.6 ainsi que le premier et dernier paragraphe, mais de les déplacer à la section 2. L'attente de l'Autorité quant à la nécessité de documenter son environnement technologique est une bonne pratique et est en lien avec la gestion des risques, mais les autres précisions apportées à la section 1.6 sont de nature opérationnelle et dictent le « comment documenter » alors qu'elles devraient se limiter au « pourquoi documenter ». Par exemple, en venant préciser au troisième paragraphe que la documentation doit contenir suffisamment d'informations agrégées, l'Autorité vient dicter « comment » documenter.

3.12. Information pour la prise de décision (p. 18)

Le BAC recommande de retirer une partie de la section 1.7 puisqu'elle est redondante avec la section 1.6 de la Ligne directrice TIC et n'ajoute pas de précisions supplémentaires. D'ailleurs, elle ne contient pas d'attente spécifique (encadré) de l'Autorité qui pourrait la distinguer de la section 1.6. Seule la phrase « Parmi les différents éléments d'information soutenant une saine

gouvernance et gestion des risques liés aux TIC que l'institution devrait considérer dans ses pratiques, il y a notamment : » qui se retrouve dans le premier paragraphe ainsi que les puces qui suivent devraient être déplacées à la section 2 puisque celles-ci sont des livrables de la section 2.

3.13. L'identification et la gestion des risques liés aux technologies (p. 20)

Le BAC est d'avis que cette section constitue le cœur de la Ligne directrice TIC qui a pour objectif d'émettre des attentes précises quant à la gestion des risques liés aux TIC. Pour bien refléter cet objectif, le titre de cette section devrait être modifié par « Le cadre de gestion des risques liés aux TIC ».

De plus, le BAC recommande de compléter cette section avec des éléments qui se retrouvent actuellement dans la section 3, mais qui concernent le cadre de gestion des risques. Cette modification à la structure permettrait de regrouper à un seul endroit tous les éléments nécessaires à un cadre de gestion des risques, ce qui en faciliterait la lecture et l'interprétation.

3.14. Les types de risques liés aux technologies (p. 20)

Le BAC recommande de retirer complètement la section 2.1 puisque l'attente quant à la mise en place d'une taxonomie est déjà prévue à la section 1.6[3]. Les trois types de risque identifiés dans la ligne directrice est une taxonomie des risques qui s'inspire vraisemblablement de la norme du National Institute of Standards and Technology (norme NIST). Or, la taxonomie adoptée par l'institution pourrait différer de celle de la norme NIST. Comme mentionné à la section 3.10 de ce mémoire, en venant apporter des précisions inspirées par une norme spécifique, l'Autorité semble favoriser cette norme au lieu des autres. Ces précisions limitent la flexibilité et la capacité de l'institution à instaurer une gestion des risques liés aux TIC propre à son profil de risque selon la norme qu'elle choisit.

3.15. Tolérance pour le risque TIC (p. 22)

Le BAC recommande de déplacer la section 2.2 dans l'introduction de la section 2 afin de regrouper toutes les exigences concernant le cadre de gestion des risques liés aux TIC au même endroit. De plus, seules les exigences supplémentaires qui ne sont pas déjà prévues dans la Ligne directrice sur la gestion intégrée des risques et dans la Ligne directrice sur le risque opérationnel devraient être conservées.

[3] Le BAC aimerait préciser que dans le cadre de sa révision de la ligne directrice, le BAC a recommandé de déplacer la section 1.6 à la section 3.0.

3.16. Attributs du cadre de gestion des risques liés aux technologies (p.22)

Le BAC recommande de fusionner l'attente citée à la section 2.3 avec l'introduction de la section 2 afin de regrouper toutes les exigences concernant les attributs du cadre de gestion des risques liés aux technologies. Le BAC recommande également de se limiter aux exigences d'un cadre de gestion des risques liés aux TIC et, conséquemment, retirer toutes les précisions concernant les bonnes pratiques de gestion opérationnelle. Par exemple, les trois dernières puces de la page 25 sont très détaillées et établissent « comment » évaluer la sécurité de l'information au lieu d'indiquer que l'institution doit considérer la sécurité de l'information dans le cadre de sa gestion des risques. La méthode sélectionnée par l'institution pour y arriver, en autres mots le « comment », relève de la gestion opérationnelle et non de la gestion du risque.

3.17. L'agrégation des risques liés aux technologies (p. 26)

Le BAC recommande de retirer la section 2.4, sauf la troisième puce de la page 26, afin de l'intégrer dans l'introduction de la section 2 pour compléter les attributs du cadre de gestion des risques liés aux TIC.

3.18. L'impact d'affaires des risques liés aux technologies (p. 26)

Le BAC recommande de retirer la section 2.5, car cette section réitère les attributs nécessaires à une gestion intégrée des risques. De plus, c'est l'objectif même de la gestion du risque opérationnel d'identifier les causes et les impacts des risques (impacts financiers, réputation et non atteinte des objectifs d'affaires). D'ailleurs, la Ligne directrice sur le risque opérationnel y est entièrement dédiée.

3.19. Les pratiques de gestion des risques liés aux technologies (p. 27)

Le BAC recommande d'intégrer la section 3 à la section 2 sur le cadre de gestion des risques liés aux TIC. Seules les notions de gestion des risques TIC devraient être intégrées à cette section. Actuellement, la section contient beaucoup de notions de gestion opérationnelle ce qui n'est pas l'objectif de la Ligne directrice TIC.

De plus, afin d'éviter de créer des sections qui ne sont pas complètes, tous les rôles et responsabilités qui y sont précisés devraient se retrouver aux sections 1.2 et 1.3 dans la mesure où ils sont nouveaux et pertinents pour le conseil d'administration, la haute direction ou les lignes de défense.

3.20. Les pratiques d'identification (p. 27)

Le BAC recommande de déplacer la section 3.1 et de l'intégrer de façon plus succincte à la section 2. De plus, les attentes de l'Autorité devraient être précisées pour éviter qu'elles reprennent des notions de la norme NIST. Bien que cette norme établisse de bonnes pratiques de gestion de la cybersécurité, elle n'est pas la seule norme qui établit celles-ci. En détaillant les attentes de l'Autorité sur la norme NIST, il devient difficile pour une institution de choisir, en toute confiance, une autre norme pour se conformer aux attentes de l'Autorité. Considérant que l'objectif de cette section est de s'assurer, entre autres, que l'institution documente son environnement technologique, le BAC recommande que l'Autorité fusionne cette section avec le texte de la section 1.6 (Documentation de l'environnement des TIC) puisque cette dernière ne s'inspire pas de la norme NIST et permet ainsi à chaque institution de sélectionner la norme qui lui convient le mieux.

3.21. Les pratiques de détection (p. 28)

Le BAC recommande de déplacer la section 3.3 et de l'intégrer de façon plus succincte à la section 2. Comme mentionné précédemment, les attentes de l'Autorité devraient être précisées afin de permettre à une institution de sélectionner la norme qui lui convient le mieux sans reprendre nécessairement la norme NIST.

3.22. Les pratiques de réponse et de recouvrement en cas d'incident (p. 29)

La section 3.4 couvre spécifiquement la réponse aux incidents de sécurité. Le BAC recommande de déplacer cette section 3.4 et de l'intégrer de façon plus succincte à la section 2. De plus, à certains endroits, on dicte le « comment » gérer la sécurité alors qu'on devrait parler de la gestion des risques liés aux TIC qui est beaucoup plus large que la sécurité. Conséquemment, le BAC recommande de retirer tous les paragraphes qui constituent de la gestion opérationnelle des TIC.

3.23. Autres pratiques (p. 29)

La sous-section sur les opérations liées aux technologies précise, à la page 30, des rôles et responsabilités pour la haute direction et le conseil d'administration. Or, ces rôles et responsabilités devraient se retrouver à la section appropriée dans la ligne directrice, soit à la section 1.2 (Rôles et responsabilités) en s'assurant qu'ils soient en sus des responsabilités déjà prévues ailleurs.

Les sous-sections sur l'infogérance et l'infonuagique ainsi que les projets et programmes de transformation devraient être intégrés à la section 2. Quant à la sous-section sur la continuité des activités, elle devrait être retirée puisqu'elle fait l'objet d'une ligne directrice complète.

4. CONCLUSION

Depuis plusieurs années maintenant, la technologie a pris une place importante dans la stratégie d'affaires des institutions. Les membres du BAC comprennent donc que la gestion des risques liés aux technologies de l'information et des communications est très importante et doit être bien encadrée. Cependant, il est primordial que l'encadrement proposé par l'Autorité se limite aux attentes relatives à la gestion prudentielle spécifique aux risques des TIC de façon à assurer une cohérence entre les lignes directrices.

Afin de répondre aux attentes exprimées par l'Autorité dans cette nouvelle ligne directrice, des adaptations et des changements sur le plan opérationnel seront nécessaires. Le BAC est d'avis qu'un délai de trois ans serait nécessaire dans les circonstances.

Comme le BAC l'a mentionné à maintes reprises dans le passé, l'Autorité devrait éviter d'ajouter des responsabilités au conseil d'administration spécifiques à une ligne directrice en rassemblant plutôt l'ensemble de ces responsabilités dans la Ligne directrice sur la gouvernance. Une telle façon de faire a été adoptée ailleurs au Canada et facilite grandement la compréhension par le conseil d'administration de ses rôles et responsabilités.

De plus, afin de favoriser une industrie dynamique et innovante de même qu'une saine concurrence du marché, l'encadrement doit se limiter à résoudre des problèmes réels ou à prévenir un risque qui n'est pas déjà encadré. Les nombreuses lignes directrices existantes couvrent une partie importante du contenu de la Ligne directrice TIC de sorte que le projet de ligne directrice tel qu'il est présenté créerait un encadrement démesuré et non nécessaire, en plus de le complexifier sans raison.

Finalement, le BAC est d'avis que l'Autorité devrait revoir le projet de la Ligne directrice TIC afin qu'elle se limite aux particularités des technologies de l'information et des communications, par exemple aux enjeux de sécurité liés aux cyberattaques.

Le BAC sera heureux de continuer de travailler avec l'Autorité afin de s'assurer que les risques liés aux technologies de l'information fassent l'objet d'un encadrement adéquat adapté à la réalité des assureurs de dommages actifs au Québec.

– Fin du document –