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

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

Version du 28 novembre 2019

Présenté à M^e^ Philippe Lebel
Secrétaire et directeur général des affaires juridiques
Autorité des marchés financiers

Décembre 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
Montréal (Québec) H3A 2Y1

Décembre 2019

TABLE DES MATIÈRES

1. INTRODUCTION

Le Bureau d'assurance du Canada (BAC) a pris connaissance de la dernière version de la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* (Ligne directrice TIC) publiée pour consultation et présente ses commentaires. Les nombreux changements apportés par l'Autorité à la suite des consultations avec les assujettis ont permis d'améliorer les versions antérieures et le BAC salue l'ouverture de l'Autorité à cet égard.

Le BAC tient d'abord à souligner que la structure et le langage utilisés dans cette nouvelle version se rapprochent davantage de ceux utilisés dans les autres lignes, ce qui rend sa lecture plus conviviale.

Chaque section comporte maintenant un énoncé de principe (encadré), ce qui permet de mieux comprendre les attentes de l'Autorité. De plus, le retrait des précisions inspirées par une norme spécifique permet à un assureur de sélectionner une ou plusieurs normes qui convient à son profil de risque.

Finalement, le regroupement des rôles et responsabilités du conseil d'administration et de la haute direction dans une même section en facilite la consultation.

Le BAC remarque toutefois que la Ligne directrice TIC demeure plus prescriptive et détaillée que les autres lignes directrices notamment à la section 4 « Normes complémentaires aux lignes directrices de l'Autorité ». Bien que les éléments énumérés dans cette section constituent de bonnes pratiques selon les normes reconnues, l'Autorité devrait maintenir une rédaction basée sur des principes, comme énoncé dans son préambule. Au surplus, il demeure certaines incohérences quant aux responsabilités de la deuxième ligne de défense et redondances avec d'autres lignes directrices dont l'application est générale et qui inclut les TIC, au même titre que tout autre risque.

2. COMMENTAIRES

2.1. Commentaires généraux

Les expressions « parties prenantes » (pages 8, 19 et 20), « parties intéressées » (pages 19), « fournisseur » (pages 5, 11, 13, 16, 17, 24, 25 et 26), « partenaire » (pages 11, 13 et 16), « consultant » (pages 13) sont utilisées à travers le document. Elles sont parfois qualifiées en indiquant « interne » ou « externe » ou en le qualifiant avec les deux.

Le BAC recommande d'harmoniser les expressions utilisées et de les définir, lorsque nécessaire, pour éviter toute confusion. Par exemple, à la page 19, l'assureur doit divulguer aux « parties intéressées internes et externes » un incident opérationnel majeur qui est susceptible d'entraîner un préjudice d'importance significative pour ces parties. Par la suite, lorsqu'on parle de notification et de communication on réfère aux « parties prenantes » (première puce de la page 19 et quatrième puce à la page 20) et non aux « parties intéressées ». Le BAC recommande de clarifier à qui on réfère exactement ou, à tout le moins, de donner des exemples de ce qui est visé ici.

Le BAC remarque que cette Ligne directrice TIC ne comporte pas de section intitulée « *Surveillance des pratiques de gestion saine et prudente* » comme c'est le cas dans toutes les autres lignes directrices.

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

L'Autorité demande aux assureurs de mettre en œuvre cette ligne directrice au plus tard le 23 janvier 2021. Le délai d'un an pour la mise en œuvre d'une nouvelle ligne directrice aussi importante est irréaliste selon le BAC. D'ailleurs, l'Autorité accorde toujours 24 mois aux institutions financières pour se conformer à une nouvelle ligne directrice. Les assureurs sont conscients de l'importance de cette nouvelle ligne directrice, mais plusieurs étapes, dont l'évaluation des ressources et des coûts liés à implantation, devront être franchies avant que les assureurs puissent se conformer aux nombreuses exigences de la ligne directrice TIC. D'ailleurs, la vaste majorité des assureurs ont déjà approuvé leur budget pour l'année 2020. De manière plus réaliste, la plupart des institutions financières ne seront pas en mesure de se conformer pleinement à cette nouvelle ligne directrice dans un délai de seulement un an.

La présente Ligne directrice prévoit comment les risques TIC devront être gérés. Conséquemment, les assureurs devront revoir leur structure actuelle de gestion du risque déjà établie selon leurs propres considérations et normes internes, et déterminer si celle-ci est en conformité avec la nouvelle structure requise. La modification d'une structure de gouvernance est exigeante et requiert du temps afin qu'elle soit exécutée avec agilité et efficience. Par exemple, la Ligne directrice TIC prévoit plusieurs assignations au niveau de la haute direction. Celles-ci doivent être faites de manière rigoureuse en collaboration avec les ressources

humaines pour élaborer un profil de compétences identifiant les attentes et les responsabilités liées à ces nouvelles fonctions.

Ainsi, le BAC propose une entrée en vigueur de la ligne directrice le 23 janvier 2023. Les assureurs pourraient par ailleurs préparer un plan d'action, au plus tard le 23 janvier 2021, pour les activités de conformité qui n'ont pas été complétées et qui devront l'être avant le 23 janvier 2023.

2.3. 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. Effectivement, le BAC n'est pas en mesure de situer cette Ligne directrice TIC dans la structure actuelle puisqu'elle comprend plusieurs notions de gouvernance et de gestion du risque.

Une précision semblable à celle qui se retrouve dans la *Ligne directrice sur la gestion du risque opérationnel* serait pertinente. À cet égard, l'Autorité précise à la page 6 de cette dernière :

> *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 sur la gestion de la continuité des activités ainsi que la gestion des risques liés à l'impartition et à la criminalité financière. 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*.

Également, le BAC souhaiterait obtenir des précisions quant à la différence entre « infogérance », à la note de bas de page 5, et l'impartition à laquelle l'Autorité réfère plus loin ainsi que dans d'autres lignes directrices. Pour éviter toute ambiguïté, le BAC suggère d'harmoniser les termes utilisés ou de préciser si l'infogérance doit être traitée différemment de l'impartition en général.

2.4. La gouvernance des technologies de l'information et des communications (p. 8)

2.4.1. Rôles et responsabilités du conseil d'administration (p. 9)

Le BAC recommande de retirer le terme « éthique » de la première puce de la page 9 puisque la *Ligne directrice sur la gouvernance* prévoit déjà cette responsabilité à la page 10, et ce, afin d'éviter de la confusion. La puce se lirait comme suit :

> *Que la haute direction fasse la promotion d'une culture d'entreprise fondée sur un comportement organisationnel sécuritaire dans l'exploitation des technologies.*

Le BAC recommande de modifier la deuxième puce de la page 9, d'une part pour refléter le fait que le rôle du conseil d'administration n'est pas de documenter sa compréhension des besoins, mais d'instaurer des objectifs stratégiques et un cadre de gouvernance tout en s'assurant de son efficacité. D'autre part, le conseil d'administration, qui n'a pas une connaissance optimale des technologies de l'information (TI), ne devrait pas avoir à porter un jugement en cette matière. D'ailleurs, dans la *Ligne directrice sur la gouvernance*, la *Ligne directrice sur la gestion du risque opérationnel* ou la *Ligne directrice sur les critères de probité et de compétence,* on n'attribue jamais une telle responsabilité au conseil d'administration. Comme rédigé actuellement, cette responsabilité nous apparaît être une responsabilité opérationnelle et constituerait une ingérence du conseil d'administration dans la gestion des opérations.

Conséquemment, le BAC recommande de modifier la deuxième puce de la page 9 comme suit :

> *De s'assurer d'obtenir suffisamment de renseignements pertinents des parties intéressées pour être en mesure d'approuver la gouvernance actuelle et future des TIC et de s'assurer de son efficacité.*

Le BAC recommande aussi de modifier les sixième et septième puces de la page 9 puisque l'expression « autre personne de la seconde ligne de défense » infère automatiquement que le responsable pour la surveillance du déploiement de l'encadrement appartient à la seconde ligne de défense. Or, certaines institutions financières peuvent actuellement avoir positionné le rôle du chef de la sécurité de l'information (CISO) à la première ligne de défense. D'ailleurs, dans un rapport sur la gestion du cyberrisque et de la technologie, la firme KPMG recommande de positionner le CISO à la première ligne de défense[1].

Les assureurs doivent conserver la faculté de concevoir leur structure de gouvernance en fonction de leur taille et des besoins particuliers. Ainsi, le rôle du chef de la sécurité de l'information (CISO) pourrait être dévolu soit dans la première ligne de défense, soit dans la seconde selon les besoins.

Dans cette section, le BAC recommande également de préciser les attentes de l'Autorité par rapport aux rôles des gestionnaires responsables des risques TIC au lieu d'énumérer qui doit

[1]KPMG, *Technology and cyber risk management, Protect and enable the business with a holistic risk and governance framework,* September 2018, p. 3 et 5, consulté en ligne le 9 décembre 2019 : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&ved=2ahUKEwiAi5betKnmAhUNvJ4KHUkYC5YQFjAKegQIAxAC&url=https%3A%2F%2Fadvisory.kpmg.us%2Fcontent%2Fdam%2Fadvisory%2Fen%2Fpdfs%2Ftechnology-cyber-risk-managment.pdf&usg=AOvVaw3In3K3vblNPB99vEHZ8-rp À cet égard, les auteurs mentionnent : *"Identifying, mitigating, and managing cyber risk should have lines of sight from the Chief Information Security Officer (CISO) as the first line, and the Cyber Risk Management leader as the second line, which elevates the positions and puts it at the heart of the business's decision-making process. (...) This arrangement, which creates a clear system of checks and balances, is radically different than the traditional Information Technology Risk Management function that has emerged in recent year. (...)There has been ambiguity across industries as to whether the CISO should be the first or second line of defense, KPMG's stance is that this role belong in the first line. The CISO should focus on technology and control implementation, as well as the operational metrics specific to the first line technology risk framework needed to protect and secure the enterprise."*

assumer ces fonctions. En énumérant ainsi plusieurs responsables, il devient difficile de savoir si les responsabilités visées peuvent être cumulées par une même personne ou non.

Le BAC demande de clarifier les attentes quant à l'assignation des trois responsables identifiés (responsable pour les systèmes informatiques et les technologies de l'information, chef de la sécurité et chef des données). Le BAC propose de remplacer la liste actuelle par les attentes de l'Autorité, ce qui éviterait d'être trop prescriptif quant à la structure de la gouvernance et permettrait une certaine flexibilité afin qu'un assureur puisse établir sa structure en regard de la nature, de la taille, de la complexité de ses activités et de son profil de risques.

Le BAC recommande finalement de retirer la référence aux « procédures » dans la dernière phrase du dernier paragraphe de la section 2.1 sur les rôles et responsabilités du conseil d'administration pour ne conserver que la référence au processus, ce niveau de documentation étant jugé beaucoup trop détaillé pour le conseil d'administration. Aussi le conseil d'administration devrait avoir une « bonne compréhension » et non une « compréhension complète », car il ne devrait pas être tenu de connaître le moindre détail de ces processus.

2.4.2. Rôles et responsabilités de la haute direction (p. 10)

Le terme « supervision » employé à la première puce réfère généralement à l'encadrement ou à la gestion à l'égard d'une autre fonction. Or, la fonction TIC devrait plutôt être « surveillée » par une fonction de contrôle de la deuxième ligne de défense. Le BAC recommande donc de modifier la première puce de cette section à la page 10 par :

> *Assurer la surveillance de la fonction TIC par une fonction de contrôle de la deuxième ligne de défense.*

Le BAC recommande également à l'Autorité de préciser ce qu'elle entend par « notamment en la séparant des processus opérationnels et par la mise en place de contrôles compensatoires au besoin » à la deuxième puce de la page 10, car ses assureurs membres ne comprennent pas la signification de cet énoncé.

Finalement, le BAC recommande de modifier l'avant-dernière puce de la page 10 comme suit :

> *Évaluer régulièrement l'environnement de contrôle en collaboration avec la deuxième ou la troisième ligne de défense.*

Cette modification permet de ne pas être trop prescriptif quant à la fonction qui effectuera l'évaluation, sans compromettre l'objectivité de cette évaluation, et de préserver l'indépendance entre les fonctions. De plus, elle permet une plus grande flexibilité pour les assureurs dans l'établissement de leur structure de gouvernance.

2.4.3. Rôles et responsabilités – autres rôles (p. 12)

Pour les raisons exprimées précédemment, le BAC recommande de modifier le premier paragraphe pour remplacer le terme « superviser » par « surveiller ». La fonction de gestion des risques ne supervise pas les activités de la fonction TIC, mais exerce une surveillance à son égard. Notons que, dans certains cas, ces deux fonctions peuvent relever de la même ligne de défense.

D'ailleurs, dans les autres lignes directrices dont la *Ligne directrice sur la gouvernance,* la *Ligne directrice sur la gestion intégrée des risques* et la *Ligne directrice sur la conformité*, l'utilisation du terme « fonction » semble réservée à la seconde ligne de défense. Or, dans la Ligne directrice TIC, l'utilisation de ce terme est utilisée pour référer à des fonctions de première et deuxième ligne de défense, ce qui porte à confusion.

Le BAC recommande de remplacer le terme « non éthique » à la note de bas de page 29 de la page 12 par « non autorisé ». L'éthique a pour objectif d'évaluer l'impact d'une décision et les actions à prendre pour y arriver en fonction des valeurs communes et elle est, de par sa nature, très subjective.

Finalement, le BAC demande le retrait du troisième paragraphe de la page 12, car l'audit interne ne peut être responsable des activités des parties externes et les responsabilités de la fonction d'audit interne sont bien encadrées dans la *Ligne directrice sur la gouvernance.*

2.4.4. Probité et compétences (p. 13)

Le BAC constate que cette section comporte de nombreuses redondances avec la *Ligne directrice sur les critères de probité et de compétences*, ce qui risque de créer de la confusion.

Le dernier paragraphe de la page 13 devrait être modifié pour éviter que l'assureur ait la responsabilité d'effectuer des vérifications de sécurité pour les consultants et les employés des partenaires et des fournisseurs infonuagiques. D'ailleurs, il sera parfois impossible de le faire avec des fournisseurs infonuagiques d'envergure mondiale.

Il existe par ailleurs d'autres mécanismes pour s'assurer que les vérifications de sécurité soient effectuées notamment par le biais d'un engagement contractuel du consultant ou du fournisseur infonuagique. La Ligne directrice TIC devrait reconnaître ces autres mécanismes.

2.4.5. Documentation à l'égard des TIC (p. 14)

Le BAC recommande de retirer le deuxième paragraphe de cette section et de le déplacer dans la section sur les rôles et responsabilités du conseil d'administration afin de rassembler toutes les responsabilités du conseil d'administration dans une même section. De plus, pour éviter que le conseil d'administration doive approuver les éléments clés de chaque document, le BAC recommande de spécifier que l'on vise les éléments clés de la stratégie TIC.

2.5. La gestion des risques liés aux TIC (p. 15)

L'attente telle qu'elle est libellée n'est pas claire. À sa lecture, on dirait que « l'ensemble des activités » provient de sources et normes reconnues et plusieurs interprétations peuvent en découler. Le BAC est d'avis que le libellé de l'attente devrait s'inspirer celle de la page 9 de la *Ligne directrice sur la gestion des risques opérationnels*.

2.5.1. Préparation (p.17)

Il y a une coquille à la quatrième puce de la page 17. Le terme « assurant » devrait se lire « assurer ».

2.5.2. Traitement (p.17)

L'attente de la deuxième et troisième puce de la section 3.2 de la page 17 n'est pas claire. Le BAC recommande de remplacer la deuxième et la troisième puce comme suit :

> *Répertorier les mesures d'atténuation des risques afin de s'assurer que l'ensemble des risques respecte la tolérance aux risques TIC de l'institution.*

2.5.1. Suivi (p. 19)

L'Autorité s'attend à ce que l'institution financière avise promptement les parties intéressées « susceptibles de subir un préjudice d'importance significative » à la suite d'un incident opérationnel majeur. Ce critère de dénonciation diffère de celui qui se retrouve dans la *Ligne directrice sur les saines pratiques commerciales* qui exige, à la page 20, que l'institution financière avise les consommateurs « en temps opportun de tout bris de confidentialité susceptible de nuire à leurs intérêts ou à leurs droits ».

Par ailleurs, le critère proposé dans la Ligne directrice TIC est similaire à celui utilisé dans la *Loi sur la protection des renseignements personnels et les documents électroniques*[2] et la *Ligne directrice sur le risque opérationnel* qui requiert une déclaration de toute atteinte aux mesures de sécurité lorsque l'atteinte peut créer un « risque réel de préjudice grave à l'endroit d'un individu ».

Le BAC recommande à l'Autorité d'harmoniser les critères de divulgation auxquels elle réfère dans les différentes lignes directrices.

[2] L.C. 2000, ch.5, article 10.1 (1).

2.6. Normes complémentaires aux lignes directrices de l'Autorité (p. 21)

2.6.1. Sécurité des TIC (p. 21)

À la note de bas de page 39 de la page 21, le BAC recommande de remplacer le terme « encryption » par « chiffrement » pour éviter l'usage d'un anglicisme[3].

L'Autorité précise à la page 22 que les privilèges d'accès octroyés doivent être établis sur la base de certains principes notamment le principe du « jamais seul ». Cette expression n'est pas comprise par les membres du BAC qui recommandent de la retirer ou de la préciser. Par ailleurs, s'il s'agit du principe du « two-person integrity » ou TPI comme défini par le National Institute of Standards and Technology[4], le BAC se questionne quant à l'applicabilité de ce principe à l'industrie de l'assurance.

Finalement, le BAC recommande de préciser le dernier paragraphe de la page 22. Il est difficile d'identifier l'attente de l'Autorité en ce qui concerne les rôles d'ingénierie et d'architecture. De plus, ce qui est énoncé dans ce paragraphe ne semble pas cohérent avec le premier paragraphe de la section « Autres rôles » à la page 12 qui se lit comme suit :

> *La fonction de gestion des risques[8] 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.*

2.6.2. Infogérance et infonuagique (p. 24)

Le BAC recommande d'ajouter le terme « forcément » à la première phrase de la section afin qu'elle se lise comme suit, car dans certaines circonstances, l'infogérance peut réduire ce risque:

> *L'infogérance ne réduit pas <u>forcément</u> les risques inhérents liés aux TIC.*

Bien qu'il s'agisse d'une bonne pratique, le BAC recommande de modifier la première puce de la page 25, car il n'est pas toujours possible d'obtenir ce droit contractuellement d'un fournisseur infonuagique d'envergure mondiale.

---

[3] Office québécois de la langue française, Fiche terminologique : Chiffrement, consulté en ligne le 10 décembre 2019 : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8387607 L'office indique qu'il s'agit d'un terme déconseillés puisque : « Le calque direct *encryption* est à éviter puisqu'il ne comble aucune lacune lexicale et entre inutilement en concurrence avec *chiffrement* et *cryptage*. »

[4] NIST, Computer Security Resource Center, Two-person integrity (TPI), consulté en ligne le 10 décembre 2019: https://csrc.nist.gov/glossary/term/two_person-integrity. Voir également, le Centre de la sécurité des télécommunications, Directrice en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein des entreprises du secteur privé canadien, consulté en ligne le 10 décembre 2019. https://www.cse-cst.gc.ca/fr/node/1923/html/27625.

Finalement, la question de l'« emplacement du traitement informatique » ne devrait pas être visée dans cette puce, car les exigences retrouvées à la fin du paragraphe, qui sont applicables à la sécurité des données, ne le sont pas pour l'emplacement du traitement informatique. De plus, il est parfois impossible de contrôler efficacement l'emplacement des données considérant l'utilisation de centres de données en réplication.

Le BAC recommande donc de remplacer la deuxième puce de la page 25 par ce qui suit :

> *Assurer la sécurité des données par des contrôles adéquats (établis par une approche basée sur les risques) comme les technologies de chiffrement des données en transit, en mémoire et au repos;*

Le BAC souhaite avoir des précisions quant à l'attente de l'Autorité lorsqu'elle indique à la deuxième phrase du premier paragraphe de la page 26 :

> *La cybersécurité ne devrait pas être considérée uniquement au niveau des fournisseurs majeurs ou des fournisseurs de services critiques, mais aussi au niveau des maillons jugés les plus faibles.*

3. CONCLUSION

Afin de répondre aux attentes exprimées par l'Autorité dans cette nouvelle Ligne directrice TIC, des adaptations et des changements au niveau de la structure de gouvernance et au niveau organisationnel seront nécessaires. Par conséquent, le BAC est d'avis que le délai de mise œuvre devrait être exceptionnellement de trois ans. Par ailleurs, pour s'assurer de l'avancement des travaux, un plan d'action visant à planifier les étapes restantes et leur échéancier pourrait être préparé par chaque assureur un an après la publication. De plus, les ambiguïtés et les contradictions dans les rôles et responsabilités des administrateurs et hauts dirigeants devraient être clarifiées ou retirées, le cas échéant.

Le BAC est également d'avis que l'Autorité devrait épurer la section « *Normes complémentaires aux lignes directrices de l'Autorité* » pour retirer les éléments qui n'apportent pas des précisions quant aux attentes de l'Autorité, mais qui réitèrent les meilleures pratiques découlant de sources, de recommandations et de normes reconnues. Cette épuration permettrait également une harmonisation plus grande avec les autres sections de la Ligne directrice TIC et serait davantage conforme à l'approche basée sur des principes.

Le BAC demeure disponible pour discuter de ce qui précède.

– Fin du document –