**COMMENTAIRES DU MOUVEMENT DESJARDINS**

# Introduction

Desjardins a pris connaissance de la nouvelle proposition de Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications (TIC) et présente ses commentaires.

Notre organisation tient à souligner l'effort de simplification du langage effectué par l'AMF depuis la dernière consultation. Cela rend la lecture de la ligne directrice plus fluide et est plus aligné sur le langage utilisé dans les autres lignes directrices de l'AMF.

# Commentaires

## Commentaires généraux

Nous soutenons l'approche fondée sur les principes de l'AMF. Nous notons cependant que la ligne directrice, telle qu'elle est rédigée, contient plusieurs mentions s'apparentant à une approche fondée sur les règles.

Desjardins reconnaît l'importance de protéger les informations de ses membres et clients et de gérer adéquatement ses actifs informationnels. Cependant, certaines des attentes proposées dans cette ligne directrice, nous semble dépasser celles qui s'appliquent aux institutions financières sous réglementation fédérale.

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

Compte tenu de la portée des attentes exprimées, une entrée en vigueur fixée au 31 janvier 2021 nous apparait ambitieuse. Nous avons observé dans l'industrie que la mise en œuvre trop rapide de changements TIC complexes peut entraîner des effets indésirables pour les membres/clients. C'est pourquoi Desjardins s'engage à mettre tout en œuvre pour se conformer à la date souhaitée et établir un plan d'action axé sur des priorités clairement établies.

Nous soutenons l'engagement en faveur de l'évolution continue de cette ligne directrice intégrant les résultats des examens prudentiels et des développements externes. Nous demandons cependant qu'il y ait une juste période d'observation et de consultation de l'industrie avant d'introduire de nouvelles exigences. Cela réduira l'incertitude réglementaire, soutiendra les efforts de gestion des changements internes et fournira la stabilité nécessaire pour concevoir avec soin et mettre en œuvre efficacement des stratégies de remédiation à long terme.

## Introduction (p. 5)

La nature de la technologie obligera toujours les organisations à utiliser des systèmes remplacés par des systèmes plus modernes. Nous recommandons de modifier la note en bas de page 5 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 augmentent le risque pour l'institution.

De plus, nous souhaiterions obtenir des précisions quant à la différence entre « infogérance », à la note de bas de page 6, et l'impartition à laquelle l'AMF réfère plus loin ainsi que dans d'autres lignes directrices. Pour éviter toute ambiguïté, nous suggérons d'harmoniser les termes utilisés ou de préciser si l'infogérance doit être traitée différemment de l'impartition en général.

## Gouvernance des TIC (p. 8)

Nous n'avons pas noté dans le ligne directrice le besoin de produire une information exécutive pour appuyer une prise de décision éclairée au plus haut niveau. Cet élément devrait ressortir en priorité notamment en lien avec les responsabilités du conseil d'administration. On exprime un besoin détaillé de documentation des contrôles au détriment de cette vision globale essentielle à l'établissement d'une bonne stratégie de gestion des risques liés aux TIC.

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

Certaines responsabilités attribuées au conseil d'administration sont de nature opérationnelle et dépassent ou sont en conflit avec les attentes exprimées dans les lignes directrices sur la gestion des risques opérationnels et la gestion intégrée des risques. Nous recommandons que la ligne directrice se concentre sur les résultats souhaités et non pas sur les moyens utilisés pour atteindre ces objectifs.

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

Tout comme pour la section portant sur les rôles et responsabilités du conseil d'administration, nous recommandons à l'AMF d'identifier les résultats souhaités afin d'offrir aux institutions plus de souplesse dans le choix de leurs approches.

À la page 11, il est précisé que l'établissement de la stratégie TIC devrait notamment « considérer l'utilisation des innovations technologiques dans la planification stratégique et les décisions d'architecture d'entreprise ». Nous considérons que cette section devrait être retirée, car elle suppose que les institutions ont le désir stratégique et l'appétit pour le risque d'envisager l'utilisation de technologies innovantes. Selon nous, la ligne directrice devrait être neutre sur ce point.

## Autres rôles (p. 12)

La responsabilité de gestion des risques incombe à la 1re ligne de défense et non à la gestion des risques qui est une 2e ligne de défense. Nous considérons que cette notion devrait être clairement indiquée dans la ligne directrice. Actuellement, certains éléments de rédaction laissent croire que la 2e ligne de défense est responsable de l'ensemble de la gestion des risques TIC, notamment le 1er paragraphe de cette section.

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.).

## Probité et compétences (p. 13)

Cette section est redondante avec la Ligne directrice sur les critères de probité et de compétence.

Bien que la détermination des 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 de la haute direction complètent les grilles d'aptitudes et de connaissances pour tous les risques liés aux TIC identifiés dans la présente ligne directrice. Cependant, ce niveau de compétence est requis du personnel qualifié au niveau opérationnel.

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

Cette section est très normative. De plus, elle décrit les meilleures pratiques, ce qui n'est pas conforme à l'approche de l'AMF en matière de réglementation et de surveillance fondée sur les risques.

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

Cette section est normative et nous apparaît en conflit avec d'autres lignes directrices de l'AMF qui stipulent que les organisations 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, proportionnées à la taille et à la complexité de l'organisation.

Nous pensons qu'il serait important de mieux définir ce qui compose la 1re et la 2e ligne de défense en matière de TIC puisque le texte, en général, manque de clarté et rend parfois difficile la distinction entre ces 2 rôles.

De plus, c'est la première fois que la segmentation selon la préparation, le traitement et le suivi est utilisée dans une ligne directrice et nous trouvons que cela devrait être précisé.

- La portion « Préparation » semble traiter d'éléments d'encadrements et préalables nécessaires à opérer des TIC. L'Autorité peut-elle clarifier ce qu'elle veut dire par des activités préparatoires?
- La portion « Traitement » semble parler d'éléments permettant de monitorer/identifier les risques (surveillance des opérations TIC par la fonction TIC). Les termes traitement des risques et options de traitement des risques doivent être clarifiés.
- La portion « Suivi » se limite aux incidents majeurs/crises.

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

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.

## Infogérance et infonuagique (p. 24)

Dans le contexte de l'infogérance et de l'infonuagique, la ligne directrice précise que « l'institution financière devrait notamment assurer contractuellement son droit d'auditer (ainsi que celui des autres autorités compétentes, le cas échéant) de même que leur accès physique aux locaux des

fournisseurs de service d'infonuagique ». Nous suggérons de modifier cette puce afin d'identifier l'objectif à atteindre plutôt que le moyen, il n'est effectivement pas toujours possible d'obtenir ce droit contractuellement de fournisseurs majeurs en infonuagique.

## Conclusion

Afin de répondre aux attentes exprimées par l'AMF dans cette nouvelle ligne directrice et de mieux protéger ses membres et clients, des adaptations et des changements au niveau de la structure de gouvernance et au niveau organisationnel sont nécessaires. Comme mentionné précédemment, Desjardins mettra tout en œuvre pour atteindre la conformité à la date souhaitée et proposera un plan d'action axé sur des priorités clairement établies.