The Institute of Internal Auditors
Elevating Impact

31 mars 2023

L'autorité ontarienne de réglementation des services financiers (ARSF)
25 Sheppard Avenue West, Suite 100
Toronto, ON
M2N 6S6

Objet : La proposition de l'ARSF en matière de gestion de risques liés aux technologies de l'information

Monsieur,
Madame,

Au nom de l'Institut des auditeurs internes (IAI), j'ai le plaisir de vous soumettre les commentaires suivants à prendre en considération. Ces commentaires sont en lien avec la proposition de l'ARSF en matière de gestion de risques liés aux technologies de l'information. Depuis plus de 80 ans, l'IAI et ses maintenant plus de 230 000 membres à travers le monde, avec plus de 7 000 membres au Canada, ont contribué à la bonne gouvernance et à la gestion des risques dans les organisations des secteurs public et privé, en encourageant des contrôles internes rigoureux et une approche à l'échelle de l'entreprise.

L'IAI apprécie la complexité d'offrir la gestion de risques liés aux TI pour tous les secteurs réglementés par l'ARSF et pour les particuliers. Pour les secteurs qui sont tenus de se conformer aux lignes directrices des principes et celles spécifiques aux secteurs, nous constatons que les lignes directrices spécifiques aux secteurs varient. Plutôt qu'une approche harmonisée dans tous les secteurs, les recommandations suivantes sont formulées afin de suffisamment et équitablement traiter les risques liés aux TI de chaque secteur.

La ligne directrice proposée reconnaît uniquement l'audit interne comme une fonction de surveillance indépendante pour les credit unions et les caisses populaires et fait référence à des sources externes potentielles d'assurance en matière de gestion de risques liés aux TI dont la portée est généralement limitée. La gestion de risques liés aux TI est un élément clé d'une gouvernance, d'un risque et de contrôles efficaces et est plus grande que la cybersécurité ou le contrôle des rapports financiers. Nous recommandons de développer les références de lignes directrices de façon à inclure l'audit interne pour les autres secteurs.

- **Retour sur les recommandations : Pratique 1 - La gouvernance** *devrait faire référence à l'audit interne comme source indépendante d'assurance sur la gestion des risques liés aux TI, lorsque l'entité réglementée ou le particulier a une gouvernance et une surveillance adéquate de ses risques liés aux TI et reçoit une assurance indépendante de la part d'une fonction d'audit interne sur la gestion de risques liés aux TI.*

De plus, les principes en matière d'orientation sont largement compatibles avec les cadres de gestions de risques de la TI et les standards. Nous recommandons que les lignes directrices réitèrent l'importance de l'adhésion à un cadre/standard reconnu en matière de TI. Conformément à ces cadres et ces standards, les lignes directrices liées aux contrôles d'accès logiques devraient être séparées et distinctes des exigences en matière de gestion des données.

- **Retour sur les recommandations : Pratique 2 - La gestion des risque** *devrait faire référence à un cadre ou un standard reconnu axé sur le risque en matière de TI pour démontrer le règlement des différents en gestion des risques liés aux TI.*

Finalement, les exigences de déclaration d'incidents comprennent des termes subjectifs comme « important » et « significatif » pour décrire les incidents. Afin d'assurer une interprétation et une exécution appropriées, il pourrait être utile d'élargir la liste d'exemples d'incidents découlant de risques liés aux TI énumérés à l'annexe 1 de la ligne directrice en intégrant les commentaires des parties prenantes et/ou en s'inspirant de lignes directrices similaires, tels que l'avis du BSIF du 16 août 2021 sur le signalement des incidents liés à la technologie et à la cybersécurité.

- **Retour sur les recommandations : Lignes directrices sur le signalement des incidents - Les lignes directrices** *devraient être révisées dans le but de minimiser l'utilisation d'une terminologie vague/subjective et des exemples devraient être plus étoffés et inspirés de contributions pratiques de praticiens de la TI et d'auditeurs.*

L'IAI souhaite poursuivre son engagement auprès de l'ARSF en ce qui concerne le projet de gestion des risques liés aux technologies de l'information et/ou toute autre question relative à la gouvernance dans le secteur des services financiers de l'Ontario. Si vous avez des questions concernant cette lettre ou des questions relatives à l'audit interne ou à la gouvernance organisationnelle, je vous prie de bien vouloir me contacter à l'adresse suivante jillian.fernandez@theiia.org.

Veuillez agréer, l'expression de mes sentiments distingués.

Jillian Fernandez
Directrice, défense des intérêts et promotion (Canada)
L'institut des auditeurs internes du Canada