ACPM | ACARR
The Association of Canadian Pension Management
L'Association canadienne des administrateurs de régimes de retraite

[VERSION FRANÇAISE NON OFFICIELLE]

Le 9 mai, 2022

Winnie Vong, FICA, FSA, CFA
Senior Risk Analyst, Pensions Department
BC Financial Services Authority
600-750 West Pender Street
Vancouver, C-B. | V6C 2T8

Mme Vong,

RE: Projet de ligne directrice de l'ACOR sur le cyberrisque

Nous vous remercions de l'occasion de prendre connaissance et de formuler des commentaires préliminaires sur la nouvelle ligne directrice de l'ACOR sur le cyberrisque. D'après ce que nous comprenons du processus, cette ligne directrice sera publiée au cours de l'été afin de recueillir d'autres commentaires. Par conséquent, pour l'instant, nous nous en tenons à des commentaires relativement généraux.

L'ACARR représente des promoteurs, des administrateurs et des fiduciaires de régimes, de concert avec leurs fournisseurs de services. Nos membres gèrent des régimes de revenu de retraite qui couvrent des millions de participants et comprennent des régimes de toutes tailles et de tous types.

L'ACOR a un rôle important à jouer pour mettre l'emphase sur le fait que le cyberrisque, pour les promoteurs et les administrateurs de régimes de retraite de toutes tailles à travers le Canada, est un risque dont les régimes doivent être conscients, qu'ils doivent surveiller et auquel ils doivent se préparer. Toutefois, nous suggérons que l'ACOR reconsidère si le projet actuel, en particulier la section 3 et l'annexe B, est trop prescriptif dans son contenu. L'ACOR pourrait plutôt développer des lignes directrices davantage fondées sur des principes généraux qui garantiront que les régimes de retraite de toutes tailles reconnaissent le cyberrisque et demeurent conscients de leur obligation fiduciaire afin de gérer ce risque, au lieu d'émettre plusieurs directives précises sur la façon dont les régimes doivent gérer ce risque.

Notre suggestion qu'elle soit moins spécifique et davantage fondée sur des principes généraux est basée sur les trois préoccupations suivantes :

1. Il existe un risque élevé que ce document devienne obsolète dès sa publication (notamment en ce qui concerne les exemples de risques, le contenu relatif aux plans de résilience et à aux rapports d'incidents, et les exemples fournis aux annexes A et B). Le cyberrisque continue d'évoluer rapidement et, à mesure que notre compréhension et la technologie évoluent, les descripteurs pertinents évoluent également. Par exemple, nous notons dans la version anglaise du projet de lignes directrices que certains considéreront les « hacktivistes » comme un terme dépassé qui devrait être remplacé ou complété par le concept « des activistes parrainés par l'État », tel qu'indiqué dans la version française du projet de lignes directrices. De même, dans cet environnement en constante évolution, il faut se demander si les exemples de contrôles

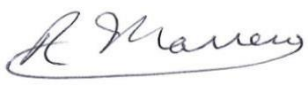
énumérés à l'annexe B, même si entièrement mis en œuvre, seraient suffisants pour tous les régimes de retraite. Cela étant dit, nous sommes d'avis que des exemples concrets peuvent être utiles aux régimes de retraite ayant une expertise limitée à l'interne afin d'illustrer les éléments qui pourraient être envisagés. Nous suggérons que l'objectif soit de trouver le juste équilibre entre être utile et trop prescriptif.

2. Il n'y a pas assez de flexibilité dans la ligne directrice pour que des régimes de différentes tailles puissent adapter leurs approches. Par exemple, alors que les régimes de grande taille ont peut-être des plans de résilience et de réponse aux cyber incidents, les régimes de plus petite taille s'appuient typiquement fortement sur des fournisseurs de services externes, dans quel cas on s'attend à ce que l'administrateur exerce davantage une fonction de surveillance plutôt que d'être tenu d'élaborer des politiques ou des pratiques détaillées propres au régime. Il est également possible que des administrateurs aient peu de pouvoir de négociation quant aux modalités de leurs contrats avec des tiers fournisseurs en ce qui concerne certaines des recommandations spécifiques énumérées aux sections 2 et 3. Une approche davantage fondée sur des principes généraux permettrait à l'ACOR d'amener l'industrie à comprendre la cybersécurité comme un risque en évolution et à veiller à ce que des contrôles, une attention et des stratégies d'atténuation appropriés et adaptés à la taille du régime et de l'organisation ainsi qu'à sa structure de gouvernance, soient mis en œuvre.
3. La ligne directrice devrait rappeler aux administrateurs que la cybersécurité recoupe plusieurs approches de gouvernance qui devraient déjà être en place pour protéger la vie privée et la confidentialité des renseignements personnels de manière plus générale. Bien que le cyberrisque ne soulève pas toujours des préoccupations en matière de vie privée, les considérations relatives à la vie privée doivent être comprises dans le contexte du cyberrisque. De même, nous suggérons que la ligne directrice contienne une section rappelant aux participants qu'ils jouent également un rôle pour réduire certaines formes de cyberrisque et pour protéger leurs renseignements personnels en utilisant les meilleures pratiques en matière de mots de passe, de sécurité de leurs appareils et ordinateurs personnels et d'autres mesures connexes.

En résumé, l'ACOR a un rôle important à jouer pour souligner l'importance de ce risque et identifier les attentes des organismes de réglementation selon lesquelles les administrateurs de régimes de retraite doivent tenir compte de ce risque dans le cadre de leurs obligations fiduciaires. L'ACOR devrait souligner la nécessité pour les régimes de retraite de toutes tailles de comprendre les conséquences du cyberrisque et son évolution, et de mettre en place des mesures appropriées et adaptées à leur taille et à leur situation pour faire face à ce risque, sans être trop prescriptif.

N'hésitez pas à nous contacter si vous souhaitez en discuter. Merci.

Veuillez agréer, Madame Vong, l'expression de mes sentiments distingués,



Ric Marrero
Chef de la direction
ACPM

cc : Steve Anu, gestionnaire, Politique et administration, BC Financial Services Authority