



October 14, 2022

CAPSA Secretariat  
25 Sheppard Avenue West  
Toronto ON M2N 6S6

Via email: [capasa-acor@fsrao.ca](mailto:capasa-acor@fsrao.ca)

To Whom It May Concern:

**RE: CAPSA Cybersecurity Guideline Draft**

ACPM is the leading advocacy organization for a balanced, effective and sustainable retirement income system in Canada. Our private and public sector retirement plan sponsors and administrators manage retirement plans for millions of plan members, including both active plan members and retirees.

CAPSA has an important role to play in highlighting that cyber risk, for plan sponsors and administrators across Canada and of all plan sizes, is a risk that plans need to be aware of, monitor and prepare for. However, we would like CAPSA to consider whether the current draft, particularly Section 3 and Appendix B, is too prescriptive in its content. Consider whether it should evolve to more principles-based suggestions that will ensure plans of all sizes recognize cyber risk and are aware of the fiduciary duty to manage this risk, but not contain as many specific directions with respect to the ways in which plans will manage those risks.

**Our suggestion to be less specific and more principles-based is based on three specific concerns:**

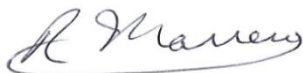
- 1) There is a high risk that this document will become out of date as soon as it is published (particularly with respect to the examples of risk, the content around resiliency plans and incident response, and the examples provided in Appendix A and B). Cyber risk continues to evolve quickly and, as our understanding and technology evolves, so do the relevant descriptors. For example, we note that some will view “hacktivists” as an aged term that should be replaced with, or supplemented by, the concept of “state-sponsored threat actors.” Similarly, in this evolving environment, if completely implemented, would the control examples in Appendix B be sufficient for all plans? Having said that, we do think that examples can be helpful to plans with fewer on-staff expert resources to help illustrate some of the things that, speaking today, might be considered. We suggest the goal is to find the right balance between being helpful and being too prescriptive.

- 2) There is not enough room within the Guideline for plans of different sizes to 'right size' their approaches. For example, while large plans may have specific cyber event resilience plans and incident responses, smaller plans may rely heavily on external service providers where the administrator would be expected to exercise more of a monitoring function as opposed to being required to develop detailed policies or practices of its own that are specific to the plan. Administrators may also have little negotiating power over the terms reflected in their contracts with third party providers with respect to some of the specific recommendations listed in Sections 2 and 3. A more principles-based approach would allow CAPSA to focus the industry on understanding cyber security as an evolving risk and ensure appropriate controls, attention and mitigation strategies suitable to the size of the plan and/or the organization, and its governance structure, are implemented.
- 3) The Guideline should remind administrators that cybersecurity overlaps with several governance approaches that should already be in place to monitor privacy and confidentiality of information more generally. While cyber risk will not always raise privacy concerns, privacy considerations need to be understood in the context of cyber risk. Similarly, we suggest that the Guideline should contain a section reminding members that they also play a role in limiting some forms of cyber risk and in protecting their personal information through the use of best practices with respect to passwords, security of their personal devices and computers, and other related measures.

**In summary**, there is an important role that CAPSA should play in highlighting this risk and reflecting the expectations of regulators that plan administrators consider this risk as part of their fiduciary duties. CAPSA should highlight the need for plans of all sizes to understand the consequences of cyber risk and its evolution and to have appropriate measures in place tailored to their size and circumstances to address this risk, without being too prescriptive.

Please feel free to contact us if you would like to discuss. Thank you.

Sincerely,



Ric Marrero  
Chief Executive Officer  
ACPM