College Pension Board of Trustees | Municipal Pension Board of Trustees | Public Service Pension Board of Trustees | Teachers' Pension Board of Trustees

October 13, 2023

CAPSA Secretariat
capsa-acor@fsrao.ca

To: Whom it may concern

Subject: Submission to Consultation on the Guideline for Risk Management for Plan Administrators

This letter is in response to the stakeholder consultation on CAPSA's revised draft Guideline for Risk Management for Plan Administrators (Guideline). This submission is made on behalf of the BC College Pension Plan, Municipal Pension Plan, Public Service Pension Plan, and Teachers' Pension Plan. Collectively, our plans hold more than $150 billion in assets on behalf of over 700,000 members.

We continue to support CAPSA's work to support pension plan administrators in meeting their fiduciary duty and help enhance the protection provided to pension plan members across Canada. It is critical that plan administrators understand and take a holistic approach to managing the risks that they are exposed to. Consequently, we are generally supportive of the draft consolidated Guideline.

Pension plans in Canada are diverse in size, nature, governance structure, and depth of professional resources available to them. Our comments are made from the perspective that for the Guideline to be effective, they should be easily right sized by plans of any size. A principles-based approach with specific examples to guide understanding of the principle or suggested practice best accomplishes this.

Our comments are included as an attachment to this letter. The essence of our comments is that any efforts to make the Guideline shorter and more concise will help readers to identify the key takeaways and principles that CAPSA intends to communicate. We have also identified areas where the draft guideline reads as being more prescriptive than principles-based.

Sincerely,

Cameron McRobb, Chair
College Pension Board of Trustees

Tom Vincent, Chair
Public Service Pension Board of Trustees

Gary Yee, Chair
Municipal Pension Board of Trustees

Reg Bawa, Chair
Teachers' Pension Board of Trustees

Appendix: Specific feedback on the draft Guideline for Risk Management for Plan Administrators

Section	Commentary
3 – Risk Management	• Use call out boxes consistently. For example, they are currently used for multiple purposes including: to highlight principles; define key terms; highlight an example; and to pose thought provoking questions. • Given the wide variation of plan designs in Canada, it is important to note that plan sponsors and plan administrators may share plan governance responsibilities in different ways than implied by the Guideline.
4 – Risk Capacity	• Page 7: o The concepts of risk appetite, tolerance, capacity and limits are not clear. A single example that illustrates each of these terms would be helpful to compare and contrast the terminology. o It is important for the Guideline to note that plan administrators may define and use these terms with slight variations.
5 – Risk Management Process	• Incorporate reference to the resources required to implement a sound risk framework (people, systems, data). • Page 9: o The link on page 9 to the UK Pension Regulator Risk Register Template is helpful. The Guideline should specify that this is included for illustration only and that it is not the only approach. o Only sophisticated large plans are likely to be able to "examine the interaction between different risks and consider their interconnectedness." While this is a nice to have, we expect that it is largely out of reach of smaller plans with more limited resources.
6.1 – Outsourcing	• Page 17: o This is not an exhaustive list of questions and may be impacted by specific plan situations (e.g., size, type of plan, governance structure etc.). The Guideline should position these as questions that plan administrators "may find helpful to consider" rather than "should consider" consider.
6.2 – Cyber Security	• Pages 19 and 20 - key consideration boxes: o The contents of these boxes are granular and prescriptive. Our suggestion is to make them more principles-based. o Some of the key considerations could be difficult to implement in practice and lead to more documentation without contributing to a stronger security posture. There are likely more efficient ways for an organization to develop an understanding and confirm the appropriateness of its risk profile. • Page 19 – key considerations box o Refers to identifying data protection frameworks. We recommend focusing on cyber security frameworks, as that is the focus of this section and cyber security frameworks would typically incorporate data protection. o This suggests organizations should assess the likelihood of different breaches occurring. There are thousands of potential breach scenarios. Cyber security controls are designed to be blended in a manner that addresses the scenarios holistically, as opposed to on a scenario-by-scenario basis. For that reason, we don't believe this is a practical route

	for most organizations to take and would suggest encouraging organizations to identify and adopt a cyber security controls framework that is appropriate for their organization's size and risk profile, and ensuring it is effectively implemented. ○ The Guideline suggests that the goal is to implement controls to minimize risk. We suggest avoiding the word "minimize". The goal should not be to minimize risk but rather to ensure a proportionate control environment that contains/limits the risk to acceptable/appropriate levels. ○ It may be beneficial to incorporate into the considerations box having an appropriate strategy in place to obtain assurance that the control environment is sound and risk exposure is at an acceptable level. That is in essence what organizations should be driving towards. We believe that's a more critical consideration than some of the more granular recommendations offered. • Page 20 - key considerations box ○ Would recommend staying away from operational details towards broader considerations around understanding the organization's potential sources of cyber exposure from outsourcing activities to a third party. We believe that the focus should be on getting comfortable that the risk exposure is contained/appropriate. ○ Getting into the details of a third party's individual controls is potentially duplicative if the third party has strong risk oversight, and in our view is too much to ask of plan administrators. ○ Additionally, suggesting that the organization should understand the third party's certifications and seals of compliance with standards is too narrow. We believe the guidelines should focus more on understanding and obtaining comfort with the third party's cyber risk governance and sources of assurance on its cyber security posture. If the dialogue with the third party focuses on its governance and sources of assurance, the third party's responses will naturally cover certifications and seals of compliance where applicable, and allow for other potential forms of assurance. ○ The process for how and when plan administrators would be notified in an incident is a good consideration to include. However, dimensions like frequency of updates are potentially too granular. Breaches vary considerably in nature and potential impact, and the appropriate communication cadence will depend on the circumstance. For this reason, it's very difficult to define/legislate communication requirements down to that level of detail. ○ We think that the bullet on third-party cyber insurance should focus on the third party's insurance process and adequacy of coverage, not necessarily obtaining the details (i.e., "extent" or amount) of the third party's coverage. Cyber insurance policy details are sensitive and should be safeguarded. We need to be cautious about circulating this information too widely as it increases the risk that it lands in the hands of cybercriminals. If cybercriminals know an organization's insurance limits (especially if the limits are high), they are more likely to attack it. Indicates that Plan Administrators must "minimize the risk of a cyber incident occurring". As stated earlier, we recommend avoiding use of the word minimize. The only way to minimize the risk is to avoid it outright, which is not practical with organizations becoming so heavily dependent on technology.

6.3 ESG	• The terms “ESG information”, “ESG factors”, and “ESG considerations” appear to be used interchangeably in this section and throughout the document. We suggest that “ESG factors” be the chosen term, this is the commonly used language.
	• References to “relevant” ESG information should be replaced with “material”.
	• Page 24
	  ○ We would caution against saying that it is aligned with fiduciary duty to use ESG for ethical or social impact purposes, generally, as it implies having objectives other than financial returns, which won’t apply to most pension plans. However, it is reasonable and prudent to use material ESG factors to provide risk/financial insights or to break a tie.
	  ○ The sentence “*Plan administrators may determine it is consistent with their fiduciary duty to use ESG information, including for ethical or social impact purposes, as a deciding factor or tiebreaker between otherwise economically equivalent investment options (that is, options that provide equivalent expected risk-adjusted returns)*” should be reworded to “*Plan administrators may determine it is consistent with their fiduciary duty to use ESG factors, assessed like any other investment risk in the analysis process, to inform better long-term investment decision-making*".
	• Page 26, footnote 9
	  ○ We suggest that the footnote is reworded to say “*Physical risks include rising sea levels, increased flooding, extreme heat events and wildfires. Transition risks are those risks associated with transitioning to a low-carbon economy and include increasing disclosure requirements, shifting asset values, changes in consumer preferences and changes in regulations, technology, and business practices*”.
	• Page 27
	  ○ Section 6.3.5 on Investment Decision-Making includes a reference to investments in ‘green’ assets. We recommend that CAPSA provide a more complete definition for what this means or suggest that Plan Administrators could follow existing taxonomies. It is prudent to be careful and conservative when categorizing ‘green’ investments as scrutiny around greenwashing is increasing.

6.4 Use of Leverage	• Now that CAPSA has decided to merge all documents (leverage, ESG, cyber) in one single guidance document, Sections 6.4.4 to 6.4.8 could be streamlined as the principles to manage the risk have been already discussed in Section 5.

6.6 Investment Risk Governance	• Section 6.6: risk governance is addressed throughout sections 2 to 5 so we don’t see the need of this section. The following observations are made should CAPSA decide to retain section 6.6.
	• Page 39
	  ○ Section 6.6.2 – move Portfolio Limits section from 6.6.3 to here, as it is generally applicable to most if not all plan administrators.
	• Page 40
	  ○ Given the wording in 6.6.2, it seems that the practices in 6.6.3 are not necessarily applicable to all plans, especially smaller plans. That could be made plainer.
	  ○ Section 6.6.3 - typically, stress testing and sensitivities analysis are used to complement risk metrics that are used to set limits. We are not sure they should be used to set limits.
	• Page 42
	  ○ Regarding alternative assets, we believe that there is too much focus on valuation which is covered by other industry guidelines (e.g.: IFRS). Also,

	in a period of high volatility, we do not expect our investment manager/agent to sell illiquid assets, so market risk should not be the focus for private assets. The guidance seems to be tailored to large pension plans with internal investment teams making buy/sell decisions. Guidance is missing for those plan administrators that invest in externally managed alternative asset funds or that delegate buy/sell decisions to an agent. • Page 43 ○ Section 6.6.4 - in the scope of risk reporting, we do not see a necessity to list the risks. Each plan should assess what risks matter for their portfolio and when they need to be reported.

Appendix A – Risk Table	• Pages 45-49
	  ○ Plan administrators may aggregate or disaggregate risks so this appendix is a good starting point, but plan administrators need to be aware that their approach should be tailored to their unique governance structure and approach to risk management. For example:
	  ▪ "Model risk" is unlikely to be a common risk in most plan administrator's risk registers.
	  ▪ Our investment agent/manager has been delegated authority to manage investment risk, and then reports out on those risks. Individual types of investment risk are not necessarily in our risk register even though they are a critical part of our oversight process and practices

Appendix B – Risk Assessment Tools	• Page 50 We think that the list of tools to evaluate risks should not be limited to sophisticated models or simulation techniques. Sometimes, reporting and monitoring key ratios driven from accounting data are sufficient to track the risk. Liquidity Coverage Ratio (LCR) and leverage ratios are examples of simple but powerful metrics commonly used to monitor (and support management of) the risk.