



March 31, 2023

Caroline Blouin
Executive Vice President, Pensions
Financial Services Regulatory Authority of Ontario
5160 Yonge Street, 16th Floor
Toronto, ON M2N 6L9

RE: FSRA Proposed IT Risk Management Guidance (“Guidance”)

Dear Ms. Blouin:

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.

Principles-Based Guidance

The Guidance frames FSRA’s interest in this topic with reference to its statutory objects of consumer confidence, protecting pension benefits and rights of pension plan beneficiaries and promoting the good administration of pension plans. As the regulator of a diverse set of regulated entities, the Guidance acknowledges the need for sector-specific considerations, including those of Ontario pension plan administrators (“Administrators”).

Administrators are subject to a fiduciary standard that distinguishes pension administration from the consumer model in brokerages and other regulated Ontario sectors. We support principles-based Approach Guidance that acknowledges this unique role of Administrators and is consistent with industry-accepted practices and CAPSA guidelines. However, the proposed reporting framework for Administrators is problematic and should be reconsidered.

We ask FSRA to consider whether cross-sectoral Guidance will, in practice, consistently support the intended outcomes of improved oversight and risk mitigation in the pension sector, and whether the prescriptive elements of the Guidance are consistent with a principles-based approach that provides flexibility, consistent with the varied size and nature of Ontario pension plans. In particular, we are concerned that the proposed real-time reporting framework for material IT risk incidents may, in some respects and situations, result in a diversion of resources away from incident management, and the creation of additional risk through the sharing of sensitive information. The resourcing and coordination associated with such reporting may be particularly burdensome for smaller, single employer plans. Best practices guidance would be preferable for the pension sector, given the nature of the sector and FSRA’s supervisory powers.

We also refer you to [our recent letter](#) on the Cybersecurity Guideline proposed by the Canadian Association of Pension Supervisory Authorities (“CAPSA”), which provides suggestions that are relevant to this Guidance.

We note that the federal Office of the Superintendent of Financial Institutions (“OSFI”) has limited the application of [Guideline B-13 – Technology and Cyber Risk Management](#) (“B-13”) to federally regulated financial institutions, but not pension plans. OSFI has recently advised in [InfoPensions Issue 27](#) that federally-regulated pension plan administrators may refer to B-13, pending the release of the CAPSA Cybersecurity Guideline. A principles-based approach is preferable for Administrators in Ontario and other jurisdictions.

Practices for Effective IT Risk Management (“Practices”)

Practice 7 of the Information – All Sectors section of the Guidance establishes a framework for a regulated entity, including an Administrator, to notify FSRA of a material IT risk incident. Appendix 2 includes an IT Risk Notification Form detailing the information FSRA expects to receive from the Administrator.

FSRA’s Interpretation Guidance, which informs enforcement and supervisory actions, states that a failure to follow the Practices will likely result in a breach of sections 22(1) and 30.1(2) of the Pension Benefits Act (“PBA”), i.e., the statutory fiduciary standard and the provisions governing the electronic transmission of personal information or any prescribed information. This approach to the standard of fiduciary duty and references to breach of the PBA is overly stringent. Whether or not there has been a breach of fiduciary duty requires an analysis of all relevant facts in a given situation.

Administrators, in their fiduciary capacity, are already accountable to have appropriate governance, risk management and data management frameworks that encompass the risks associated with information technology and the management of confidential or personal data and information, including where this is subject to delegation or service agreements with third-parties. We question whether introducing a notification framework is consistent with the overall objectives of these Practices and Guidance. We ask FSRA to consider whether this notification framework may instead discourage organizations from offering or continuing to participate in registered pension plans, and evolving their digital communications, which can be an effective and cost-efficient way to engage with members.

Notification of Material IT Risk Incidents

This section of the Guidance outlines a process for administrators to report material IT risk incidents to FSRA that is intended to be real-time and confidential and may lead to a continuous engagement and oversight by FSRA for a period of time, through resolution. This notification may also activate FSRA’s three-phase Protocol for IT Risk Incidents. FSRA’s statutory authority to request information from Administrators is also generally noted.

The Guidance states that FSRA will accept being notified of a material IT risk incident with a comparable form issued by another financial services regulator, where applicable. This approach may still result in duplicative reporting to different regulatory authorities and does not account for situations where the plan sponsor and Administrator are the same entity. Also, it does not address the provision of sensitive information to FSRA that is outside the scope of its regulatory authority, such as where the IT risk incident is not limited to the pension plan and its members, but also involves organizational information security and management. Some of the indicators listed are beyond the scope of the PBA and may not result in any actual impact to plan members.

For example, the reference to an incident that “is reported to senior management or the board of directors” might serve to discourage prudent internal reporting and prejudices the materiality. The inclusion of an incident that “is reported to another regulator, a law enforcement agency, the Office of the Privacy Commissioner, etc.” raises the concern of duplicative reporting, as noted above.

Our key concerns are that the notification obligation is overly broad and would introduce inappropriate risk, for example:

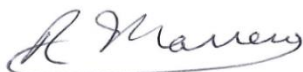
- it will require Administrator resources and attention to provide information to FSRA information needs rather than focusing on incident response; and
- the lack of confidentiality regarding the detailed information FSRA is requesting (such as through a disclosure request under the PBA or Freedom of Information and Protection of Privacy Act) could result in an inappropriate release of information about the cause, nature and status of incidents that is inconsistent with an Administrator’s risk management governance and practices and could itself pose a threat to other pension plans and/or the pension plan sponsor by revealing sensitive information about data security and management.

In addition, before reporting an IT risk incident information to FSRA outside of a statutory enforcement request, an Administrator may appropriately wish to seek reassurance as to the proper handling and security of such information. The brief description of FSRA’s Protocol for IT Risk Incidents does not address this consideration. The proposed transmission of such sensitive information to a central FSRA email inbox would be inconsistent with risk management practices. If FSRA is to compel such reporting, it will be imperative for FSRA to have its own robust governance and IT security in place to manage the risks associated with receiving such information and to be able to demonstrate this to regulated organizations and other stakeholders.

Finally, we note that the Guidance is proposed to become effective in June 2023. This does not provide sufficient time for Administrators to establish processes to comply with the proposed Interpretation Guidance for IT Risk Notification in Practice 7 of the Guidance. We encourage FSRA to reconsider the application of this Guidance to Administrators, and to instead focus on supporting a principles-based CAPSA Cybersecurity Guideline.

We appreciate the opportunity to offer these suggestions and are available if any further assistance is required.

Sincerely,



Ric Marrero
Chief Executive Officer
ACPM