

March 31, 2023

Caroline Blouin, Executive Vice President, Pensions
Financial Services Regulatory Authority of Ontario
Via email: Caroline.Blouin@fsrao.ca

Dear Ms. Blouin,

Re: Proposed Guidance - *Information Technology (“IT”) Risk Management (ID 2023-001)*

We are pleased to provide OPB’s submission in response to FSRA’s consultation on its proposed Guidance on IT Risk Management (the “draft IT Guidance”). We appreciate FSRA’s efforts in putting together the draft IT Guidance and its willingness to receive industry feedback. We also support the recommendations made in the submission of the Association of Canadian Pension Management and the joint submission made by the Ontario Teachers’ Pension Plan, OPSEU Pension Trust, the Healthcare of Ontario Pension Plan, the Colleges of Applied Arts and Technology Pension Plan and the Ontario Municipal Employees’ Retirement System.

About OPB

OPB is the administrator of the Ontario Public Service Pension Plan (“PSPP”), a major defined benefit, single employer pension plan sponsored by the Government of Ontario. Our membership is made up of certain employees of the provincial government and its agencies, boards and commissions. With \$33.7 billion in assets, 45,251 active members, 40,521 retired members and 7,324 former members, the PSPP is one of Canada’s largest pension plans. It is also one of the country’s oldest pension plans, successfully delivering the pension promise since the early 1920s. Our commitment is to protect the long-term sustainability of the PSPP, invest assets astutely and with discipline, keep contribution levels stable and affordable and deliver exceptional service to our stakeholders.

Principles-based regulation

FSRA has stated on many occasions that it embraces principles-based regulation. As explained in the draft Approach Guidance, *Proposed Principles-based regulation (“PBR Approach”)*, this regulatory posture “reduce[s] regulatory burden through a more flexible regulatory approach, which allows regulated entities to determine how to best achieve adherence with outcomes based on their size, complexity, and risk profile”. Principles-based regulation stands in contrast to, and tends to be more efficient than, the imposition of prescriptive requirements. The PBR Approach also notes that FSRA intends to impose prescriptive requirements only where

appropriate, based on circumstances including the applicable legal framework and the sophistication and resources of the regulated entity.

The sections of the draft IT Guidance relating to IT risk incident notification contemplate a prescriptive regulatory approach, imposing a requirement to notify FSRA of material incidents based on a lengthy and detailed list of considerations, and setting out a response protocol and detailed notification form. However, at least in the context of the Pensions Sector, IT risk management strongly lends itself to principles-based regulation. In this regard:

- The legal framework established under the *Pension Benefits Act* (“PBA”) does not appear to support a hard requirement to report IT incidents to FSRA.
- As recognized in the draft IT Guidance, other legal frameworks may apply to regulated entities; the existence of such alternative regulatory regimes tilts towards a less prescriptive approach to incident reporting to FSRA, based on the respective judgements of FSRA and the administrator in the specific context of any IT incident.
- Pension plan administrators possess widely varying levels of sophistication and resources. The need for the support of, and supervision by, FSRA in the context of an IT incident will therefore also vary considerably between administrators. Accordingly, a one-size-fits-all approach to reporting requirements, and to FSRA’s response to any such reporting, is ill-suited to this area of regulation.
- Efficiency is a central consideration. The incident reporting framework currently proposed would consume considerable resources on the part of both FSRA and the administrator, without necessarily yielding any meaningful benefit for plan beneficiaries. For the administrator in particular, those resources may be more effectively deployed in remedying the consequences of the IT incident.

In light of the foregoing, OPB recommends either removing Practice 7 and the Approach section “Notification of material IT risk incidents” from the draft IT Guidance, or the disapplication of those provisions to the Pensions Sector. Insofar as it applies to the Pensions Sector, the focus of such guidance should be on integration of IT risk management into plan governance, forward-looking incident response plans and voluntary reporting to FSRA where appropriate in the circumstances. That regulatory approach would be more consistent with FSRA’s foundational commitment to principles-based regulation.

The draft Guideline circulated by the Canadian Association of Pension Supervisory Authorities in June 2022, *Cyber Risk for Pension Plans* (the “draft CAPSA Guideline”), exemplifies principles-based regulation and would serve as a suitable model for the application of such an approach in Ontario’s Pensions Sector. Provided any final version is materially similar to the draft CAPSA Guideline, we propose that FSRA adopt that model for any regulatory guidance on IT risk management. Alignment in this regard would also promote jurisdictional harmonization, which is a principle that FSRA strives to apply, according to its *Pension Sector Guiding Principles*.

Confidentiality in IT incident reporting

If FSRA proceeds to adopt the draft IT Guidance, the confidentiality of any information provided to FSRA in an IT incident report would give rise to serious concerns, particularly given that FSRA is subject to the *Freedom of Information and Protection of Privacy Act*. Public disclosure of the details of an IT incident, including remediation and operational disruptions, could pose significant risk to pension plan administrators, and may even heighten the risk of a further IT incident. These concerns provide further support for removing the incident reporting provisions or, at the very least, delaying implementation of those provisions until a legal framework clearly exempting such information from disclosure by FSRA is in place.

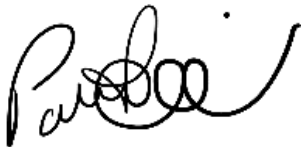
Other recommendations

Regarding the sections of the draft IT Guidance unrelated to IT incident reporting, we suggest the following revisions:

- Definition of “cyber risk” (page 6): we advise leveraging the more complete definition of “cyber risk” set out in the draft CAPSA Guideline, which references internal and external risk of “unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification, or destruction” of IT systems or data stored in those systems.
- Application of practices (page 7): the draft IT Guidance states that FSRA expects regulated entities to follow the Practices for Effective IT Risk Management and will consider adherence to those practices in its regulatory supervision. We recommend that this section explicitly acknowledge that the practices may not be applicable in the same way to all entities, which vary greatly in characteristics including size and resources.
- Remarks about fiduciary obligations (page 34): the statement that failure to follow the Practices for Effective IT Risk Management “will likely” breach pension plan administrators’ duties under subsections 22(1) and 30.1(2) of the PBA should be removed. Sweeping statements about the legal consequences of failing to follow those practices, which are broad in nature, are unhelpful.

Once again, thank you for the opportunity to comment on the draft IT Guidance. Please contact me at patrick.simon@opb.ca or 416 607 4234 if you have any questions.

Yours sincerely,



Patrick Simon
Manager (A), Policy and Procedures