OBA Submission to the Financial Services Regulatory Authority of Ontario regarding the Proposed Information Technology ("IT") Risk Management Guidance

Submitted to:	Financial Services Regulatory Authority of Ontario
Submitted by:	Ontario Bar Association
Date:	April 13, 2023

ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

L'ASSOCIATION DU BARREAU DE L'ONTARIO
Une division de l'Association du Barreau canadien

Table of Contents

Introduction

The Ontario Bar Association (**"OBA"**) appreciates the opportunity to provide this proactive submission to the Financial Services Regulatory Authority of Ontario (**"FSRA"**) on the Proposed Information Technology "IT" Risk Management Guidance (**"Guidance"**).

The OBA is the largest and most diverse volunteer lawyer association in Ontario, with over 16,000 members who practice on the frontlines of the justice system, providing services to individuals and businesses in virtually every area of law in every part of the province. Each year, through the work of our 40 practice sections, the OBA provides advice to assist legislators and other key decision-makers in the interests of both the profession and the public.

This submission has been prepared on behalf of the OBA's Pensions and Benefits Law Section. This Section represents lawyers who serve as legal counsel to stakeholders in the pension and benefits industry, including pension and benefit plan administrators, employers, plan members, bargaining agents, pension and benefit consultants, investment managers, actuarial firms, and other stakeholders. Our members have analyzed and aided decision makers over the years on several important legislative and policy initiatives in the pension field. We have also prepared this submission in consultation with members of the Insurance Law Section, Information Technology Law Section, and Privacy and Access to Information Law Section.

Overview

The OBA supports FSRA's mandate to promote good pension plan administration through a principles-based approach to regulation and appreciates the opportunity to provide comments on the Guidance.

We acknowledge that IT risks can be significant for pension plans given the sensitivity of pension data and agree that plans should have flexibility in addressing such risks in a manner which suits the size and nature of their business. Consistent with the foregoing, the OBA believes it would be helpful for FSRA to consider revising elements of the Guidance, as further explained below. We also believe that in order to promote harmonization, it would be helpful to defer consultation on the Guidance pending completion of the work being undertaken by the Canadian Association of Pension Supervisory Authorities (**"CAPSA"**) relating to IT risk.

Comments & Recommendations

Categorization of Principles in the Guidance

In our view, it is not apparent whether FSRA views the principles set out in the Guidance as good practice or as statutorily required. For instance, under the category of "Information" which is understood to not create compliance obligations,[1] the Guidance includes Practices for Effective IT Risk Management ("**Practices"**). Among other items, the Practices include that a "regulated entity notifies its regulator(s) in the event of a material IT risk incident" and FSRA's desired outcomes for this reporting.[2] Under "Approach", which is also understood to not create compliance obligations but may be indicative of FSRA's position, the Guidance indicates that regulated entities should notify regulators as soon as possible after determining that an IT risk incident is material. Under "Interpretation", which is understood to mean that non-compliance can result in regulatory intervention, FSRA

[1] See FSRA's Guidance Framework.
[2] See Practice 7.

indicates that the failure to follow the Practices (which would include Practice 7) will likely result in a breach of the *Pension Benefits Act* (**"PBA"**).[3]

To avoid confusion by users, we would suggest clarifying under which category of guidance the Practices described fall under. Where the PBA does not set out a specific course of action to be taken by a plan administrator and FSRA is providing guidance on what it views as good practice, we suggest labeling such guidance as "Information".

Should FSRA ultimately categorize the Guidance as "Interpretation", we suggest that the Guidance become effective at a later date or, in the alternative, provide for a reasonable implementation period following the proposed effective date of June 2023, during which regulated entities could assess and, if appropriate, adjust, their organization's IT infrastructure, having regard to the Practices.

Reporting of IT Risk Incidents

With respect to Practice 7 and the reporting of IT risk incidents specifically, we suggest that FSRA clearly indicate the source of its authority under the PBA for the collection of IT risk incident information. This would help users identify the nature of the requested reporting. FSRA may also wish to consider whether mandatory reporting of this nature would fall within the ambit of section 98.1 of the PBA (which is not yet in force), relating to disclosable events to be prescribed.

To the extent that FSRA intends to require reporting of IT risk incidents, it is our suggestion that the scope of this regime should be narrowed. More specifically, the Guidance should recognize that where there is no direct impact to a plan administrator's ability to pay benefits

[3] The Guidance indicates that "[f]ailure to follow the Practices for Effective IT Risk Management to properly protect their assets, operations and the confidential information of their plan members will likely result in a breach of sections 22 (1) and 30.1 (2) of the PBA."

or where sensitive plan member data is not compromised externally, FSRA does not require reporting.

Harmonization of Pension Regulation

The draft CAPSA guidance also exemplifies a principles-based approach to managing IT risks, which we believe is ideally suited to this complex area. CAPSA recently undertook a consultation on IT risk following the issuance of draft guidance.[4] It would be helpful to await the completion of CAPSA's work in this area before further consulting on and finalizing the Guidance. Doing so would provide the opportunity to ensure consistency between any CAPSA and FSRA guidance and afford plan administrators more time to review and implement any changes to their practices. This also appears to be aligned with the approach that the federal pension regulator and CAPSA member, the Office of the Superintendent of Financial Institutions Canada (**"OSFI"**), is taking.[5]

Conclusion

The OBA appreciates the opportunity to provide this submission in response to FSRA's consultation. We also appreciate the collaborative approach FSRA has taken with stakeholder engagement, and we would welcome the opportunity to arrange a call to discuss any of our comments if that would be helpful. If there are particular categories of information that more guidance on would be helpful, we can work with FSRA on providing that guidance.

[4] Cyber Risk for Pension Plans, draft dated June 9, 2022.
[5] We note that OSFI issued IT risk guidance for financial institutions but not for pension plans. In InfoPensions 27 (November 2022), OSFI indicated that IT risk guidance for financial institutions "could be a good reference for plan administrators" until CAPSA's is completed. OSFI also advised that it is working with CAPSA on finalizing its guidance.