Toronto Corporate Office
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON M8X 2X3
(416) 597-4400
MeridianCU.ca

March 31, 2023

Financial Services Regulatory Authority of Ontario ("FSRA")
5160 Yonge Street, 16th Floor
Toronto, Ontario
M2N 6L9

Re: Proposed Information Technology ("IT") Risk Management Guidance

Meridian Credit Union Limited ("Meridian") welcomes this opportunity to comment on the proposed Information Technology ("IT") Risk Management Guidance (the "Guidance").

With more than 75 years of banking history, Meridian is Ontario's largest credit union and the second largest in Canada, helping to grow the lives of 375,000 Members and customers. Meridian has $30.0 billion in assets under management (as at December 30, 2022) and delivers a full range of financial services online, by phone, by mobile and through a network of 89 branches across Ontario, and business banking services in 15 locations. Meridian respectfully offers the following comments on this proposed Guidance.

General Comments:

Meridian commends FSRA for seeking to strengthen the information technology risk management practices in its regulated sectors. Meridian agrees with FSRA that IT risks constitute a large and growing risk category that requires both careful regulation and diligence on behalf of credit unions across the sector. This is why Meridian has long placed IT risk management at the heart of our enterprise risk management policies and we take IT security very seriously.

As the 2016 article by McKinsey titled "The ghost in the machine: Managing technology risk"[1] notes:

> *Technology is synonymous with the modern bank. From the algorithms used in proprietary trading strategies to the mobile applications customers use to deposit checks and pay bills, it supports and enhances every move banks and their customers make.*
>
> *While banks have greatly benefited from the software and systems that power their work, they have also become more susceptible to the concomitant risks. Many banks now find that these technologies are involved in more than half of their critical operational risks, which typically include the disruption of critical processes outsourced to vendors, breaches of sensitive customer or employee data, and coordinated denial-of-service attacks.*
>
> *…*

[1] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-ghost-in-the-machine-managing-technology-risk

Toronto Corporate Office
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON M8X 2X3
(416) 597-4400
MeridianCU.ca

Meridian™

Exposure to these IT risks has grown in lockstep with the rapid increase in digital services provided directly to customers.

This same article recommends six principles to guide best-practice IT risk management and we are pleased to see that these principles are reflected in the Guidance, just as they are reflected in the current IT security and risk management practices of Meridian.

Specific Comments/Request for Clarification:

Incident Reporting Detail:

In our read of the Guidance, it is unclear what level of detail FSRA might be looking for when an incident is reported. Meridian has a mature IT incident management program, with policies and standards that classify incidents on risk and impact to the business. Our program is based on the COBIT 2019 framework, a globally recognized standard set by ISACA – an international professional association focused on IT governance. Using COBIT 2019, some aspects of our incident management reports are very detailed; some other data fields are at a higher level, with less detail. Our concern is that FSRA may in future be looking for the detail that our framework and systems do not generate, and the reason we do not generate the information is that it does not fit with the COBIT 2019 criteria upon which the system is built. We are also concerned that FSRA's idea of an IT Risk Framework and Meridian's idea – again, based on COBIT 2019 standards – could be very different and unless there is alignment, it could force Meridian to significantly change its risk framework, without significant added value.

We suggest further dialogue to refine what FSRA is looking for in its incident reports and recommend that FSRA allow Meridian and other credit unions to adopt industry standards such as COBIT 2019, rather than trying to create a new framework for Ontario's credit unions that is custom to FSRA.

Alignment with Overall Credit Union Risk Management Framework

In the Guidance, it is stated: "*Credit unions must establish an organizational structure where IT risk management activities are conducted by IT Operational Management (first line of defence), are reviewed and challenged by IT Risk Management (second line of defence) …"* Is this second line of defense a new requirement specific to IT, separate from the overall Risk Management second line of defense? For example, the Risk Committee of the Board meets in camera with the CRO as the second line of defense. Does the CRO also act as the IT Risk Management second line of defense?

The Guidance goes on to state:

- *"The risk oversight function/person(s) within the credit union has developed an enterprise-wide approach to the management of IT risk, which includes the following elements:*
    - *o The credit union's board-approved IT risk appetite, tolerances and limit.*
    - *o A process to report to the board regularly and consistently on the credit union's performance against its IT risk appetite."*

Meridian has a well-developed enterprise risk-management framework. Our question is whether this "IT risk appetite, tolerances and limit" is a new requirement, that is separate from the overall risk management framework, or whether it should be integrated (in the same way as all other identified risks are managed.)

Toronto Corporate Office
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON M8X 2X3
(416) 597-4400
MeridianCU.ca

There is some assurance in this document that it will be integrated where it states: *"The management of IT risk is also a factor in assessing a credit union's operational risk and resilience, as described in the 'Operational Risk and Resilience Guidance'"* In our view, there is a difference between being "a factor" and being fully a part of the overall risk management framework.

In our view, the IT Risk Management Framework should be seamlessly integrated with the overall risk management framework and our concern is that, as presently constructed, this Guidance could become duplicative in effort if it is separate and could in fact work at cross-purposes with the overall risk management framework.

Summary Conclusion:

As noted, overall, we are pleased that FSRA is taking a hard look at modernizing its approach to IT risk management. Inadequate IT risk management is a vulnerability for the sector, though we believe firmly that Meridian already stands as a leader in this respect. Looking ahead, we offer the following suggestions to improve the Guidance:

- Align the standard with other federal and provincial regulators and use internationally recognized standards:
    - FSRA should consider collaborating and working with other federal and provincial regulators and the sector to align guidance, expectations, and processes for incident reporting across regulators. There are internationally accepted standards of IT governance that can be used as a template. Following these standards would streamline processes for Ontario credit unions, allowing for less complexity and a consistent approach for reporting.

- Make reporting requirements less prescriptive:
    - Reporting requirements on what constitutes material IT risk should not be prescriptive for Ontario credit unions but align to the credit union's own risk appetite with higher level guidance from regulators on critical criteria, ensuring reporting processes are efficient and effective.

- Clarify that a credit union's overall risk management framework applies to IT risks:
    - The IT Risk Management Framework should be seamlessly integrated with the overall risk management framework and our concern is that, as presently constructed, this Guidance could become duplicative in effort if it is separate and could in fact work at cross-purposes with the overall risk management framework.

- FSRA should consider building in a regular consultation with the sector to further refine the Guidance as it evolves.
    - As the information technology landscape evolves quickly, so should FSRA and the Guidance. We recommend a yearly review by FSRA in consultation with IT managers and Chief Risk Officers at Ontario credit unions.
    - The current Guidance states that it will be reviewed "no later" than June 2027. We believe there will be benefit with consultation sooner and more frequently to refine the Guidance as credit unions and FSRA use it over the coming few years.

Toronto Corporate Office
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON M8X 2X3
(416) 597-4400
MeridianCU.ca

We appreciate the opportunity to engage with FSRA on this important topic and look forward to continued dialogue as refinements are made.

Sincerely,

Sunny Sodhi
Chief Legal & Corporate Affairs Officer