The Institute of Internal Auditors
Elevating Impact

March 31, 2023

Financial Services Regulatory Authority (FSRA) of Ontario
25 Sheppard Avenue West, Suite 100
Toronto, ON
M2N 6S6

Re. FSRA's proposed Information Technology Risk Management Guidance

Dear Sir/Ma'am,

On behalf of The Institute of Internal Auditors (IIA), I am pleased to submit the following comments for consideration, in relation to FSRA's proposed **Information Technology Risk Management Guidance**. For over 80 years, The IIA and its now more than 230,000 members across the globe, with more than 7,000 members in Canada, have aided sound governance and risk management in public- and private-sector organizations, encouraging strong internal controls and an enterprise-wide approach.

The IIA appreciates the complexity of providing IT Risk Management Guidance for all FSRA's regulated sectors and individuals. For sectors required to comply with both the Principles and sector-specific guidance, we note that sector-specific guidance varies. In lieu of a harmonized approach across all sectors, the following recommendations are proposed to sufficiently addresses IT risks within each sector, and equitably across all sectors.

The proposed Guidance only recognizes internal audit as an independent oversight function for credit unions and caisse populaires and references potential external sources of IT Risk Management assurance which are typically limited in assurance scope. As IT Risk Management is a key element of effective governance, risk, and controls and is broader than just cybersecurity or financial reporting controls; we recommend expanding Guidance references to include internal audit for other sectors.

- **Recommendation re: Practice 1 - *Governance*** *should reference internal audit as a source for independent assurance on IT risk management, where the regulated entity or individual has proper governance and oversight of its IT risks and receives independent assurance from an internal audit function on IT risk management.*

Furthermore, while principles in the Guidance are largely consistent with widely recognized IT Risk frameworks and standards, we recommended that the Guidance reiterate the importance of alignment with a recognized IT Risk framework/standard. In alignment with such frameworks and standards, guidance related to logical access controls should be separate and distinct from data management requirements.

- **Recommendation re: Practice 2 - *Risk management*** *should reference a recognized IT Risk framework/standard to demonstrate due diligence in managing IT-related risks.*

Lastly, Incident Reporting requirements include subjective terms such as 'material' and 'significant' when describing incidents. To ensure appropriate interpretation and application, it may be beneficial to broaden the list of Examples of IT risk incidents listed in Appendix 1 of the Guidance with input from stakeholders and/or from similar guidance such as OSFI'S August 16, 2021 Technology and Cyber Security Incident Reporting Advisory.

- **Recommendation re: Guidance on Incident Reporting - *The Guidance*** *should be reviewed to minimize use of vague/subjective terminology and examples should be enhanced based on practical input from IT practitioners and auditors.*

The IIA welcomes further engagement with FSRA regarding the proposed Information Technology Risk Management Guidance and/or any other matters related to governance in Ontario's financial services industry. If you have any questions regarding this letter or issues related to internal audit or organizational governance, I'd kindly ask you to please contact me at jillian.fernandez@theiia.org.

Sincerely,

Jillian Fernandez
Director, Advocacy (Canada)
The Institute of Internal Auditors, Canada