DUCA
Do more. Be more. Achieve more.
5255 Yonge Street, 4th Floor, Toronto, ON M2N 6P4 • 416-223-8838 • www.duca.com

March 31st, 2023

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

Attention: Sreejith Lal, Relationship Manager

Dear Sreejith,

Re: Information Technology Risk Management – guidance for consultation

DUCA Financial Services Credit Union Ltd ("DUCA" or "we") appreciates the opportunity to comment and respond to the public consultation surrounding FSRA's Information Technology Risk Management Guidance ("the Guidance"). FSRA's willingness to have a conversation around our concerns is helpful and we appreciate your openness for dialogue.

We support the intent and principles behind the Guidance and understand the opportunity at hand for the Guidance to further strengthen our sector. As such we are providing this feedback with the desire to assist in arriving at a final version of the Guidance that achieves the outcomes intended.

Below is a summary of key issues that DUCA has determined to be of particular importance. Additional questions / comments are included in Appendix A.

From a broad perspective, the Guidance is open to interpretation in terms of the classification of an event as "Material and/or Significant". While we fully support a principles-based regulation, a high-level criteria would be helpful for the credit union sector and for ensuring consistency in reporting to FSRA. Also, we trust that in the final Guidance FSRA will ensure that the reporting requirements do not impede the ability of credit unions to resolve the issues and requests for event data / information and that this will not breach any data privacy covenants.

The Guidance requires significant changes in the broader Information Technology Risk Management infrastructure and practices. As such we trust that credit unions will be given appropriate time to implement the changes necessary for compliance with the new regulations.

Sincerely,

RAhmad

Riz Ahmad, Chief Risk Officer

cc: Michael Hatch, CCUA

DUCA Executive Leadership Team

Appendix A

Practice/Page Number / Requirement	DUCA's Comments
Practice 7: Notification of material IT Risk Incidents – The regulated entity or individual notifies its regulator(s) in the event of a material IT risk incident	Notifying FSRA of IT risk incidents is mentioned many times throughout the IT Risk Guidance document. Notifying FSRA of such an incident may trigger the FSRA Protocol for IT Risk Incidents which involves continuous engagement to provide them with a "complete understanding and knowledge" and confirmation of actions. During an IT incident, the primary focus MUST BE to resolve the incident, as the priority rather than information briefs to the regulatory authority. We feel the incorporation of this critical prioritization of effort needs to be incorporated into the practice. It is important to note that some incidents (depending on the nature) may take time to completely understand. It will be important to avoid inefficiency that could be created through having to re-explain to the regulatory authority an understanding of an incident as it unfolds if initially the understanding may not be full and complete. Also 48 hours may not be sufficient to resolve the incident. Our strong preference is to modify the language to ensure it is practicable, that it recognizes the prioritization in management efforts toward resolving the incident versus providing updates to the regulatory authority and avoids inefficient use of time in providing versions of "complete understanding and knowledge" for incidents that may be evolving.
Page 9: Criteria used to assess practice 1: Governance – The board has ensured an appropriate organizational structure is established and resources (both people and financial) are available to effectively manage IT risk.	While we agree that the IT Strategy should be documented and approved by the Board, implementing the strategy including establishing an appropriate organizational structure and adequate resourcing should be the responsibility of the Senior Management.