March 31st, 2023

Mr. Mark White
Chief Executive Officer
Financial Services Regulatory Authority of Ontario
5160 Yonge Street, 16th Floor.
Toronto, Ontario M2N 6L9

Re: Proposed guidance on Operational Risk and Resilience and IT Risk Management

Dear Mr. White,

On behalf of the Desjardins Group, I am pleased to respond to your request for comments regarding Financial Services Regulatory Authority of Ontario's (FSRA) proposed guidance on Operational Risk and Resilience and IT Risk Management.

Desjardins is the leading cooperative financial group in Canada serving over 7.5 million members and clients across the country. For over 120 years, Desjardins has listened and responded to its members' needs and adapted to changes. We provide Canadians with banking, wealth management, life & health insurance, property & casualty insurance, personal, business, and institutional financial services. In Ontario, the Desjardins Ontario Credit Union (DOCU) is the second largest credit union in the province with 132,000 members, 48 branches, and just shy of 10 billion in assets. Desjardins General Insurance Group (DGIG) is a subsidiary of Desjardins Group and proud to be the leading personal use auto insurer in Ontario. Desjardins Financial Security (DFS) is the fifth largest Life and Health insurer in the country.

We take operational risk, resilience and IT risk management seriously and believe a proper regulatory framework will only reinforce the strength and stability of the financial industry in Ontario. As such, we support FSRA's objectives to protect consumer from harm and mitigate any financial loss. Our comments are intended to help FSRA in achieving this objective.

1) General comments on the proposed Guidance on Operational Risk and Resilience

Recognizing the DOCU's relationship with the Desjardins Group

It is important for us to reiterate that DOCU is an integral part of the Desjardins Group, and the interconnectedness of Desjardins Group's integrated business model allows for many activities to be centralized to the benefit of the entire Desjardins ecosystem.

Since 2013, the Desjardins Group is designated as a "domestic systemically important financial institution'' (D-SIFI) per the criteria set out by the Basel Committee on Banking Supervision. The D-SIFI status results in greater supervision and a specific bail-in regime, as well as added capitalization and disclosure requirements.

As a result, the DOCU, with its activities in Ontario and thus regulated and supervised by FSRA, benefits from a strict regime of requirements and enhanced supervision due to the combination of the D-SIFI designation of the Desjardins Group, and the legislative and regulatory framework in place in Ontario. This realty contributes to the DOCU's financial stability and low risk profile, which in turn benefits the entire Ontario credit union and *caisse populaire* sector.

Accordingly, we reviewed the Operational Risk and Resiliency Guideline with the understanding that FSRA recognizes the existence of the DOCU model within Desjardins Group and that it follows a principles-based approach to analyzing DOCU compliance with the Guideline. Indeed, the guideline indicates a large number of means and practices to be put in place by DOCU. However, we are certain that the measures and practices put in place at the Desjardins Group level and adopted by DOCU will allow us to achieve the outcomes set forth by FSRA in its guidance.

Third party risk management

We would appreciate clarifications on FSRA's expectations regarding the management of third-party risk. We understand the level of oversight, control and supervision required of DOCU when it outsources the production of goods or services to a third party rather than doing them in-house must vary in accordance with the material importance and criticality of the service provided.

For example, a financial institution outsources its clearance and settlement activity to a third party. What checks does the Board need to perform on this third party to achieve a level of due diligence?

The same is true when it comes to products. If the credit union offers a credit card, how can it be responsible for the operational risk of that product and the systems that support it? Are regulated entities supposed to have alternative solution for every service provider? While we agree to the importance of establishing exit plans for third party arrangements, proving exhaustive exit strategies for each critical individual third party arrangement would be extremely costly to a regulated entity. Furthermore, this may put an undesired strain on the relation with the vendor.

More importantly, DOCU's relationship with Desjardins Group is too deeply integrated to be treated as a standard relationship with a third-party service provider. We hope this relationship will be treated accordingly when FSRA asses DOCU third party risk management.

2) General comments on the proposed Guidance on IT Risk Management

Keeping a principle-based approach

We believe the proposed guidance follows a principle-based approach, but certain section and the structure could be improved to make it more comprehensively principles-based.

For example, the *Practices for effective IT Risk management* presented to regulated entities are set forth in a section classified as "Information". The guidance states that this type of content does not create a compliance obligation for regulated entities; however, in the credit union interpretation and approach, it is stated that FSRA expects all regulated entities to follow the *Practices for effective IT Risk management* and their desired outcomes in order to satisfy the Sound Business and Financial Practices Rule (“SBFP Rule").

This illustrates an opportunity to review the structure of the guidance, as well as the approach to drafting it to ensure that the principles that inform it retain their intended character and do not become prescriptive requirements.

Harmonization

It is desirable to aim for and develop an interrelated and consistent prudential system among FSRA’s guidance to avoid overlap by topic within the guidance as well as overlap with expectations expressed in other guidance already in place by other Canadian regulators regarding other risks to be managed by reporting entities. Additionally, the guidance includes, in its specialized subject of information technology risks, other equally specialized subject (data risk, third party risks, operational risk, business continuity). In addition to the necessary references and cross-references, these should also be developed in detail in other specialized guidance, different from the one currently under public consultation.

The Desjardins Group already complies with the guidance on managing IT risks from the Office of the Superintendent of Financial Institutions (OSFI) (B-13 - Technology and Cyber Risk Management) and the one of the Autorité des marchés financiers (AMF) (Guideline on Information and Communications Technology Risk Management). We commend FSRA efforts to harmonize its requirements and approach. Certain elements could, however,–be further integrated. Of note, OSFI should soon release its definitive version of guideline *B-10 – Third-party Risk Management*. We expect FSRA will continue to ensure its own expectation regarding third-party risk management closely match with OSFI’s to ensure harmonization.

As with many large organisations operating across Canada, most of Desjardins Group’s IT services, protocols and risk management is undertaken by a central unit for the group. As such, most of the IT expertise does not reside within the entities’ governance structure. As FSRA recognises that the AMF and OSFI’s respective guidance are aligned with FSRA’s guidance for the purpose of non-Ontario incorporated insurance companies, we hope this approach can be explicitly recognised not only for DGIG and DFS but also for DOCU. Considering the DOCU’s affiliation to the Desjardins Financial Group, duplicating these processes and functions would impose an unnecessary burden on DOCU.

Definitions

The guidance does not provide many definitions beyond “IT risk”. We believe FSRA should define technical terms susceptible to cause differing interpretations among regulated entities. For example, does FSRA intends to include personal data protection incident with the term “data breach”? Definitions should include provisions that the interpretations and application are subject to the regulated entity’s size, complexity, and risk profile, which will include its IT risk appetite, tolerance and limits.

Notification of material IT risk incidents

We are pleased that FSRA accepts reception of any comparable form issued by a financial service regulator to report cyber incidents. However, we encourage FSRA to work with other regulators to ensure that regulated entities are not burdened with multiple lines of communication with regulators should a cyber event affect clients and operations across multiple jurisdictions. This is especially crucial given the short timeframe afforded for incident reporting and the importance of the first few days in addressing incidents. We also believe a more principle-based requirement of notifying all stakeholders, including the regulator, as soon as possible when an incident reaches the appropriate materiality threshold would be optimal in allowing regulated entities the latitude to deal with the incident and notify every stakeholder according to the specific criticality of the incident.

Effective date and implementation

Although most elements required by this guidance are already in place within Desjardins Group, there will be considerable time constraints and resource requirements to make updates, adjust, and shift reporting across various teams and areas. We believe a two-year transitional period would allow those changes to be implemented without undue burden.

3) Specific comments

Guidance on Operational Risk and Resilience:

Section	Comment
The Board, composed of directors who have the appropriate skills and expertise, is responsible for establishing the necessary strategies and governance structures, overseeing and approving CUs' operational risk management program, as well as ensuring that there are adequate resources [8] to carry out their operational risk management activities and protect members' deposits.	DOCU can target a collective profile of the Board of Directors, but it cannot compel the democratic choice of members for the election of directors. Section 4 (2) of the Sound Business and Financial Practices Rule only provides for a power of recommendation, so the new Operational Risk Guideline should not be binding in this respect.
FSRA's Approach to Third Party Risk Management Assessment	The provisions of the agreements between Desjardins Group and third parties cover the reporting and performance measurement requirements of this guideline. We believe that the concept of risk transfer should be included in the assessment of third-party risk, particularly the concept of compensation for loss realization.

Guidance on IT Risk Management:

Section	Comment
Practice 1: Governance – The regulated entity or individual has proper governance and oversight of its IT risks. • Clear responsibilities for the management of IT risks are assigned to an individual or individuals with sufficient seniority and expertise.	This desired outcome is very prescriptive. It is advisable not to link expertise to seniority so as not to generate any type of discrimination and to be able to capitalize on the skills of the resources without considering any element other than the technical and/or conceptual ability necessary to carry out such a function within an entity.

Practice 5: Incident preparedness – The regulated entity or individual is prepared to effectively detect, log, manage, resolve, recover, monitor, and report on IT incidents in a timely manner. • The impact of IT risk incidents is minimalized.	We believe the desired outcome is to minimize the impact and not minimalize it.
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 (see Notification of Material IT Risk Incidents section) • Regulated entities and individuals assist FSRA in identifying high risk areas in a timely manner that can help prevent future incidents.	We believe this statement could be better explained. Is FSRA interested in emergent risk in the general business environment or risks specific to the regulated entities?

We thank you for giving us the opportunity to provide feedback on the proposed Operational Risk and Resilience and Information Technology Risk Management and welcome the opportunity to discuss our comments in greater detail.

Sincerely,

Giuseppina Marra
Regulatory Affairs
Desjardins Group

CC:
William Boucher, Chief Executive Officer, Desjardins Ontario Credit Union
Christian Jobidon, Vice-President, Actuarial & Underwriting Services, and Analytics, Desjardins General Insurance Group