



**Submission to the Financial Services
Regulatory Authority on its Proposed Guidance
for IT Risk Management**

Manulife

March 31, 2023



Thank you for the opportunity to comment on the Financial Services Regulatory Authority of Ontario's (FSRA) proposed Guidance for IT Risk Management.

Manulife is a leading international financial services group with global headquarters in Toronto and Canadian headquarters in Waterloo. At the end of 2022, we had more than 40,000 global employees working with 116,000 agents and thousands of distribution partners around the world to provide financial solutions to 34 million customers.

In Canada, we are a leading financial services provider, offering insurance products, insurance-based wealth accumulation products, and banking solutions. We also work with 26,000 employers across the country to provide group life, health, and disability solutions to five million Canadians.

Managing Emerging IT Risk is Critical

Our ambition is to be the most digital, customer-centric company in our industry. We continue to add innovative, customer-centric enhancements and advance our digital capabilities across our businesses to stay connect with our clients. While these ambitions may involve some element of risk taking, a strong risk culture and a common approach to risk management is central to our approach, and we have developed substantial governance processes to manage these risks, in both the IT-specific and broader third-party fields.

Manulife has been actively involved in efforts by the Office of the Supervisor of Financial Institutes (OSFI) to create new guidance specific to technology and cloud risks (B-13) and update existing third-party expectations (B-10).

A principles-based, technology neutral approach to managing technology and cyber-risk is essential to success. As technology continues to develop and grow, an agile approach that is focused on outcomes over process will provide the regulatory flexibility to keep pace with innovation, consumer expectations, and ever-evolving risks.

For this reason, we support the efforts of FSRA to develop clear guidance on risks related to technology. Our comments below focus on points of clarification and suggested amendments that will create greater operational effectiveness for the proposed guidance.

Alignment with Other Regulators

Manulife is a federally regulated financial institution (FRFI) whose operations at a group level are overseen by OSFI. As a FRFI, we are already subject to the technology, cyber and third-party risk expectations outlined by OSFI, including Guidelines B-10 and B-13 mentioned above.

We appreciate FSRA's stated intentions to align with the existing expectations from other regulators and agree that FSRA's proposed Guidance is generally harmonized with other regulatory guidelines. However, even with the best intentions, additional regulation has the potential to create unintended additional burdens and risks, particularly around reporting and compliance oversight.

Given this alignment, we would suggest that in lieu of subjecting FRFI's like Manulife to duplicative guidance, FSRA consider accepting and recognizing the oversight of counterpart

regulators.

Incident Reporting Coordination

As noted above, additional regulation, even those aligned with similar guidance by another regulator, has the potential to create unintended risk: regulatory requirements overtaking resources and capacity from managing the specific cyber incident.

In its consultation “Achieving Greater Convergence in Cyber Incident Reporting” released in October 2022, the Financial Stability Board notes that financial institutions operating in several jurisdictions are increasingly required to report in different forms and varying timelines to both insurance regulators as well as other oversight bodies, including law enforcement, cyber authorities, customers, and other stakeholders. At the same time, financial institutions must also focus on the immediate threat of addressing the incident, minimizing impact and recovering operations as soon as possible (Sec 2.1, FSB Consult Document).

It is clear that FSRA is sensitive to this concern, and we appreciate the proposed approach of allowing financial institutions to submit reporting forms developed by other regulators. However, this will still require reporting to multiple regulatory authorities while trying to manage a material incident.

To address this, insurance regulators in Canada should consider developing a “lead regulator” approach to cyber incident reporting. Similar to the lead state approach used by NAIC members in the United States, a financial institution’s lead regulator would be responsible for managing the regulatory response to incidents and would proactively share incident reporting received on a confidential basis with other impacted regulators across the country.

To operationalize this, FSRA could lead work by the Canadian Council of Insurance Regulators to establish an information sharing mechanism that allows companies to report once to their lead regulator (OSFI, FSRA or other provincial insurance authorities), and then return to devoting company resources to managing the cyber incident.

Third Party IT Risk Oversight

In the section applying specifically to Non-Ontario Incorporated Insurance Companies, Insurance Agents, Insurance Adjusters, Adjuster Firms, and Insurance Agencies, FSRA states that the proposed approach applies to both federally incorporated insurance companies as well as the other parties listed above.

However, later in the same section, FSRA states that it “considers insurers to be ultimately responsible for ensuring that IT risks are being effectively managed through all of its distribution channels and outsourced functions.”

We agree with the principle that insurers should ensure that third party providers providing outsourced functions, such as cloud services, have appropriate risk management practices in place. We would note, however, that in many cases these providers operate globally across jurisdictions and industries, and often individual entities who contract with them will have little influence on the details of risk management process (which also might be subject to specific regulatory requirements from other jurisdictions).

Regulator Responsibility for IT Risk Oversight in Distribution Channels

More concerning than outsourced services, is FSRA's proposal that insurers are ultimately responsible for IT risks within distribution partners.

Insurer oversight of IT risk management in various distribution channels is neither operationally practical nor contractually feasible.

For example, insurers have no insight into the third-party relationships that Managing General Agencies, Third Party Administrators or independent advisors enter. These organizations are independent entities with their own regulated corporate responsibilities (e.g., taxes, employee relations, etc.).

Manulife and other insurers do not have the legal authority or ability to influence which technology or cyber companies or solutions independent distributors choose to contract with.


Relatedly, MGAs have contractual relationships with multiple insurers, who each will have different standards, reporting processes, timelines, etc. Insurer oversight of MGA operations will create unnecessary confusion and poor allocation of resources when managing incidents and creating strong risk governance. Ultimately, making insurers responsible for the operations of independent, separately regulated third parties will force insurers to reduce interaction with third parties and create a strong preference for distribution through proprietary networks which will reduce consumer choice and competition in the market.

Conclusion

Thank you for the opportunity to provide comment. We would also like to note that Manulife has provided input into the CLHIA response and support many of the points raised therein.

We would also like to request the opportunity to meet to discuss in more detail the points raised in this letter and will follow up with FSRA in the coming weeks. Alternatively, please feel free to reach out directly to lindsay_walden@manulife.com

Sincerely,



Lindsay Walden
Director, Regulatory and Government Affairs
Manulife