IBC · BAC
Insurance Bureau of Canada
Bureau d'assurance du Canada

Kim Donaldson
Vice-President, Ontario
Vice-président, Ontario

416.362.2031
kdonaldson@ibc.ca

777 Bay Street, Suite 1900
P.O. Box 121, Toronto, ON M5G 2C8

March 31, 2023

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

Submitted via: https://www.fsrao.ca/engagement-and-consultations/consultation-proposed-guidance-it-risk-management

---

Re: IBC response to FSRA proposed guidance on IT risk management

On behalf of its member property and casualty ("P&C") insurers, Insurance Bureau of Canada ("IBC") thanks the Financial Services Regulatory Authority of Ontario ("FSRA") for the opportunity to provide comment on its Consultation on Proposed Guidance on IT Risk Management (the "Guidance"), which was released on January 23, 2023.

IBC is the national industry association representing Canada's private home, auto, and business insurers. Our member companies make up a vast majority of the P&C insurance market in Canada. For more than 50 years, IBC has worked with governments and regulators across the country to help make affordable home, auto, and business insurance available for all Canadians.

Technology and IT risk management is of critical importance to the P&C insurance industry. The P&C insurance industry plays an important role in underwriting economic and financial risks for Canadians and businesses. Insurance is an enabling sector that supports new ventures that innovate and contribute to the country's prosperity. In today's digital global economy, insurers use data and related information to more accurately underwrite risk, price risk, incentivize risk reduction, create operational efficiencies, facilitate better claims processing, and more. The P&C insurance industry therefore welcomes the opportunity to provide comments on any potential private sector legislation, regulations, or guidelines to ensure that Canadian companies are well-equipped to participate in a competitive data-driven digital global marketplace with all the necessary safeguards in place, including safeguards for information systems.

Comments

This submission addresses key concepts raised in the Guidance.

Scope

IBC agrees with FSRA's principles-based and risk-based approach to regulatory oversight, which recognizes the importance of ensuring flexibility to achieve the outcomes in a manner that is suitable for the size and nature of a business. Such an approach allows for the balancing of safeguards and consumer protections with regulatory oversight which allows the financial sector to take reasonable risks and compete effectively. It follows that rules that affect insurers' operations without added value to the protection of the public and consumers should be avoided.

It is therefore imperative that any potential new regulatory action is well-coordinated and consistent among different regulatory bodies (i.e., with market conduct, systemic risk, privacy regulators) and across industries (i.e., banks, insurers, and other financial institutions), such that insurers with operations in both Ontario and other jurisdictions can comply with regulations and reporting requirements in an effective, efficient, and seamless manner.

Existing guidance

IBC appreciates FSRA acknowledging that insurance companies that are incorporated outside of Ontario may be subject to similar guidance by another regulator, such as the Office of the Superintendent of Financial Institutions (OSFI)'s Technology and Cyber Risk Management Guideline. It should be noted that similar guidance has been issued by the Autorité des marchés financiers' ("AMF") in Quebec. Further, it should be noted that, last year, the British Columbia Financial Services Authority ("BCFSA") had proposed applying its Information Security Incident Reporting Guideline incident reporting guidance to both BC incorporated and extra-provincial entities. However, due to stakeholder feedback, the BCFSA opted to not include extra-provincial entities in scope of its guideline to avoid creating expectations that may conflict with those established by the extra-provincial entity's primary regulator. The BCFSA is expected to release extra-provincial applicable draft Guidelines for consultation later this year.

IBC's view is that non-Ontario incorporated companies that are subject to similar guidance by another federal or provincial financial regulator should only be required to report their primary regulator. However, if a provincial financial regulator, such as FSRA, intends to apply its provincial cyber incident reporting requirements to extra-provincial entities, IBC supports the alignment of the practices and desired outcomes set out in this Guidance with existing guidance on the same subject matter in order to reduce regulatory burden on companies that operate across Canada. Accordingly, IBC supports the pragmatic approach taken by FSRA in accepting comparable forms issued by other financial services regulators thereby lessening the burden on regulated entities that are required to submit multiple forms. IBC also thanks FSRA for confirming by email on March 7, 2023 that FSRA would consider the OSFI Technology and Cyber Incident Report Form to be comparable and propose accepting it. As such, IBC recommends revising the Guidance to name the OSFI report as an example of a comparable form. It would also be helpful to include a process for organizations to verify with FSRA whether a form or reportable information (if a form does not exist) as required by another provincial financial services regulator would be considered comparable.

Supervisory approach for non-Ontario incorporated insurance companies

IBC support's FSRA's risk-based supervisory approach for non-compliance including remedies ranging from education and remediation to regulatory discipline and intervention. However, IBC does not support FSRA's

statement that "Although this guidance also applies to insurance agents, insurance adjusters, adjusters, adjusting firms, and insurance agencies, FSRA considers insurers to be ultimately responsible for ensuring that IT risks are being effectively managed through all of its distribution channels and outsourced functions." Pursuant to OSFI Guideline B-10, insurers are accountable for outsourced activities and business activities, functions and services performed through a third-party arrangement. Insurers remain accountable by contractually requiring brokers, agents, and other vendors to adhere to specific privacy, confidentiality and systems requirements with contractual audit rights to monitor compliance. In our view, it would be inappropriate to require P&C insurers to assume a regulatory oversight function of the IT controls of regulated third party professional services. Accordingly, IBC recommends that FSRA revise the statement as follows "Although this guidance also applies to insurance agents, insurance adjusters, adjusters, adjusting firms, and insurance agencies, FSRA, expects insurers to remain accountable for its service providers through contractual means.

Notification of material IT risk incidents

To facilitate consistent, timely, and robust reporting, triggers and definitions should be standardized and aligned with those already in place (such as existing triggers and definitions established by OSFI in its security incident reporting advisory) to address other types of security incidents in addition to privacy/data breaches. Accordingly, IBC would like to recommend revisions to some parts of the FSRA Guidance to better align with OSFI requirements in order to provide more certainty to federally regulated entities.

First, with respect to the criteria for reporting, OSFI's Technology and Cyber Security Advisory states "A reportable incident may have **any one or more** of the following characteristics" and provides a detailed list of criteria. The OSFI list of criteria does not include the indicator listed in the FSRA Guidance where the incident requires non-routine measures or resources. We note that a particular indicator may not be significant on its own, although in combination with others, it could take on more significance or have greater impact. The fact that non-routine measures or resources may have been required would need to be reviewed in light of other factors in order to determine materiality, including factors such as length of time the measures needed to be in place, volume of additional resources, impact or materiality of non-routine measures, etc. As such, IBC recommends replacing the preamble "Indicators that a material incident has occurred could include but are not limited to the following, If the incident:" with the following "Indicators that a material incident has occurred could include, but are not limited to, any one or more of the following, as determined by the regulated entity or individual, materially impacts its business, operations and consumers."

Second, one of the indicators in FSRA's Guidance for determining a material incident appears broader and less clear than a similar criteria in OSFI's Advisory. While OSFI's Advisory would capture an incident whose impact has potential consequences to other federally regulated financial institutions or the Canadian financial system, FSRA's Guidance would capture incidents that could potentially affect the other entities or individuals regulated by FSRA or an incident that is likely to reoccur with other entities or individuals regulated by FSRA [emphasis added]. In our view, it is not reasonable to require an entity to assess and make a determination regarding whether an incident is likely to occur at another entity as they cannot know what IT risk management practices other entities have implemented.

In terms of the trigger for Ontario-incorporated insurance companies to report, the proposed 48-hour window to notify FSRA of any material IT risk incident should be qualified to begin after the organization has determined that the materiality threshold has been met. Consideration should be given to allowing some latitude for

organizations to determine when a matter becomes material and therefore reportable that is proportionate to a company's size, complexity, and type of activities. Incidents frequently evolve over time, making it difficult to ascertain when a report to the regulator ought to be made. Such a standard would also have the benefit of ensuring that the essential work of containing and remedying a security incident remains an organization's paramount priority.

We recommend that any required report should be made through a secure FSRA-established reporting method (i.e., avoid regular emails).

In terms of the proposed requirement for affected entities to provide updated reports (under Phase 2 of FSRA's Protocol for IT Risk Incidents), it would be helpful for FSRA to specify the reporting intervals and also clarify when an affected organization may cease reporting. For non-Ontario incorporated insurers, FSRA should align expected reporting intervals and subsequent reporting requirements with the updates that the insurer is required to provide to OSFI or other provincial financial services regulator. For example, FSRA's proposed ongoing reporting requirements appear more prescriptive and extensive than what is required by OSFI. FSRA is proposing to require continuous engagement until FSRA has received confirmation about certain things (including confirmation that all affected stakeholders, including clients and relevant privacy regulators, have been notified) and has a complete understanding and knowledge of certain things (including if any confidential data has been breached and what information was accessed). It should be noted that some information, for example, what data was actually accessed by a hacker, can be difficult to determine with absolute certainty. Further, FSRA's Guidance should make it clear that regulated entities have the discretion to determine, based on applicable law, whether any stakeholders, such as any privacy regulators, should be notified. On the other hand, OSFI's requirements are less prescriptive. It requires federally regulated financial institutions to provide situation updates, including any short term and long term remediation actions and plans, until the incident is contained/resolved. Further, following incident containment, recovery and closure, OSFI requires a report on post-incident review and lessons learned. Aligning such expectations with OSFI and other provincial financial regulators would provide the needed clarity to encourage fair and effective compliance and eliminate unnecessary, costly, and burdensome administrative efforts. In addition, with a view to ensuring an appropriate level of compliance, FSRA should provide the reporting entity with a written confirmation that the incident has been resolved to FSRA's satisfaction and that no further reporting is therefore required.

FSRA has further proposed that, following containment, recovery, and resolution of an IT risk incident, financial institutions would be required to report to FSRA on its post-incident review, including its plan to prevent a similar incident in the future (Phase 3 of FSRA's Protocol for IT Risk Incidents). The Guidance also states that the engagement continues until FSRA has "a complete understanding and knowledge of the safeguards that have been put in place to ensure the regulated entity or individual is protected from similar incidents." It should be noted that such safeguards may take extended periods of time to implement, and therefore this may lead to an indefinite and uncertain engagement time frame. Further, disclosing to FSRA the exact security safeguards that an entity has implemented can create security risk for the entity in the event that an unauthorized party accesses this information. Accordingly, IBC recommends that FSRA align this requirement with the subsequent reporting requirements in OSFI's Technology and Cyber Security Incident Reporting Advisory.

Conclusion

We thank FSRA for the opportunity to provide feedback on the Guidance. It is important to insurers that there not be overlap or duplication of regulatory burden caused by FSRA, the OSFI, and/or any other regulator issuing

guidance or rules on the same issues. A harmonized cross-regulator approach to compliance is therefore recommended. To this end, rules and regulatory oversight that affect insurers' operations without adding value to the protection of the public and consumers should be avoided.

We welcome all opportunities for further discussion with FSRA. Please reach out to Diana Lee, Director, Legal & Chief Privacy Officer at dlee@ibc.ca should you have any questions.

Sincerely,

Kim Donaldson
Vice-President, Ontario