Canadian Life & Health Insurance Association
Association canadienne des compagnies d'assurances de personnes

Submission to the

FINANCIAL SERVICES REGULATORY AUTHORITY OF ONTARIO ON ITS PROPOSED IT RISK MANAGEMENT GUIDANCE

March 31, 2023

EXECUTIVE SUMMARY

The Canadian Life and Health Insurance Association (CLHIA) members support the Financial Services Regulatory Authority of Ontario (FSRA)'s intent to provide guidance that will help the sectors and individuals it regulates effectively manage threats to their IT systems, infrastructure and data. We believe it is important that proper protocols are in place to prevent and mitigate any financial losses and harm to consumers.

However, we have some concerns with the draft Guidance, including:

1. Some sections within the Guidance are overly prescriptive and not principles-based.

2. While we appreciate that FSRA has oversight over a wide range of stakeholders, the expectations within the draft Guidance are duplicative of existing guidance from other regulators for life and health insurers within Canada and could create harmonization and compliance issues.

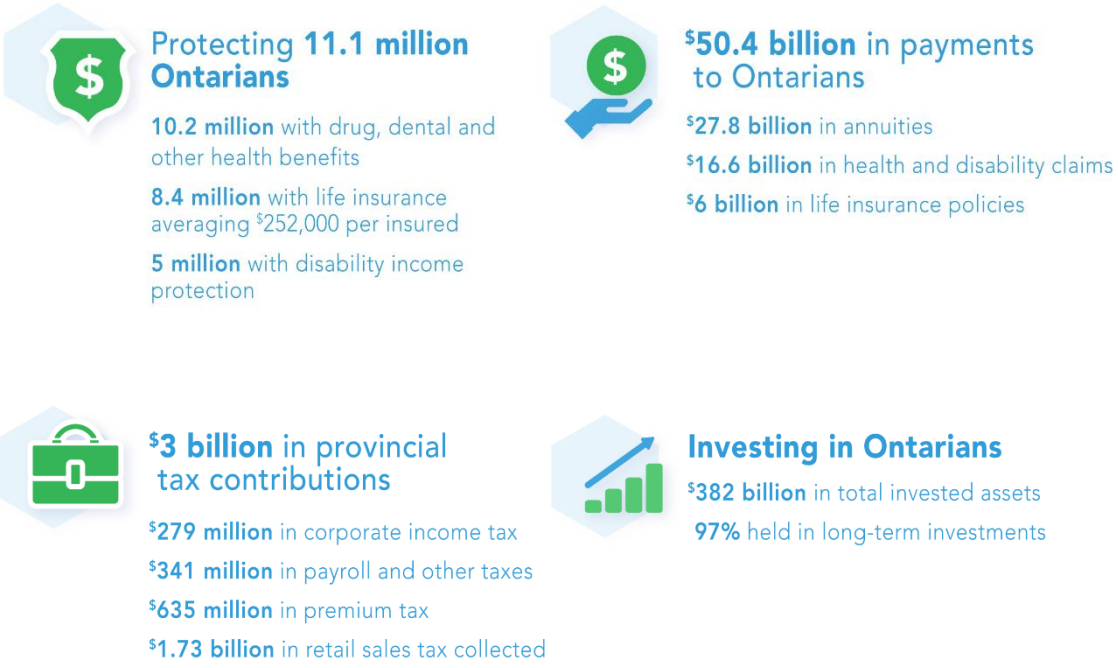
3. There needs to be greater collaboration and information sharing between regulators with respect to incident reporting.

4. Some of the expectations within the draft Guidance associated with independent advisors will be difficult for CLHIA members to meet and should be the responsibility of FSRA as a regulator and not delegated to insurers to enforce.

In this submission, we have provided comments on the sections within the Guidance that impact the life and health insurance industry. Our comments are divided into five sections. The first section summarizes our overarching comments. The second section provides comments on the section related to all sectors. The third section provides detailed comments on the section that applies to non-Ontario incorporated insurance companies, insurance agents, insurance adjusters, adjuster forms, and insurance agencies. The fourth section provides comments on the section that applies to Ontario-incorporated insurance companies and reciprocals. The fifth section provides comments on the two appendices in the Guidance.

WHO WE ARE

The CLHIA is the national trade association for life and health insurers in Canada. Our members account for 99 per cent of Canada's life and health insurance business. The industry provides a wide range of financial security products such as life insurance, annuities, and supplementary health insurance.



The industry is also a major contributor to the Ontario economy, employing more than 77,000 Ontarians and providing an important source of stable capital for the Ontario government through investments and tax contributions.

SECTION ONE: KEY RECOMMENDATIONS

The CLHIA is pleased to provide its comments to FSRA on its proposed Information Technology ("IT") Risk Management Guidance ("Guidance").

Take a more principles-based approach

Generally, CLHIA members believe that the Guidance is principles-based but there are some sections that have prescriptive requirements. We believe that for these particular sections, the Guidance should be revised to ensure that it is more principles-based. We have provided specific examples in the sections that follow.

Place reliance on the primary regulator for all non-Ontario regulated insurers who have similar guidance in place

CLHIA members support the intended purpose of the proposed Guidance. We appreciate that FSRA has oversight over a wide range of stakeholders. However, we believe that the scope of the Guidance should exclude companies that are already subject to robust guidance and oversight from other regulators. For example, federally regulated financial institutions (FRFIs) are already subject to robust guidance and oversight through the Office of the Superintendent of Financial Institutions (OSFI)'s *Guideline B-13: Technology and Cyber Risk Management*. Similarly, Quebec based companies are subject to the Autorité des marchés financiers (AMF)'s *Guideline on Information and Communications Technology Risk Management (ICT Guideline),* which includes similar expectations to FSRA's draft Guidance.

We believe that the draft Guidance is largely aligned with other regulators' guidelines on IT risk management. Therefore, it would be an administrative burden and duplication of effort to maintain additional compliance management and reporting programs across multiple regulators. This duplication of effort is costly and ultimately, the consumer bears these costs through increased product prices. We therefore believe that FSRA should place reliance on other regulators' due diligence to supervise and enforce the expectations within its guidelines where applicable.

Further to this, we understand that other provincial regulators are considering similar guidance on IT risk management. For instance, the BC Financial Services Authority (BCFSA) released its Information Security ("IS") Guideline in October 2021, which outlines principles for the effective management of IS risks and subsequently consulted on an Information Security Incident Reporting Rule in 2022. Following the 2022 consultation, the BCFSA committed to working with federal and other provincial regulators to explore better harmonization of IS incident reporting across the country. We recommend that all regulators work together to ensure harmonization of standards and that oversight be coordinated.

Work with other regulators to harmonize incident reporting expectations with material incidents only needing to be reported to the primary regulator

Convergence of Incident Reporting Frameworks

Aligned with the proposed recommendations set out by the Financial Stability Board (FSB), we recommend that FSRA explore ways for greater convergence in cyber incident reporting.

The life and health insurance industry understands that regulators are looking for ways to ensure that insurers properly manage reporting of incidents. Many CLHIA members have business operations and provide services to consumers across the country. Having different incident reporting expectations in each province, and federally, will be very burdensome for companies. This is especially true when reporting requirements are required in a short time frame. Insurers need to focus on addressing the incident with the first number of days being critical. We understand the need for regulators to be in the loop, however, we strongly prefer a coordinated approach by regulators in Canada.

Report IT Incidents to Primary Regulator

We support greater collaboration and information sharing between FSRA and other regulators. It is important to note that since August 2021, FRFIs have been required to report material technology and cyber events to OSFI, including analysis of root cause, impact, and lessons learned. Similarly, authorized insurers within Quebec are required to report incidents as part of the ICT Guideline. Having separate and disparate reporting requirements in each jurisdiction creates a duplication of effort and undue burden on companies and could lead to unnecessary delays in managing the incident.

We therefore recommend that FSRA work with other regulators on an information sharing protocol that will allow information sent to a company's primary regulator to be shared with FSRA. Designating a lead reporting authority to receive incident reports and disseminate this information to other regulators, as appropriate, would ensure regulators get the information they require while minimizing the reporting

requirements on insurers, thus allowing them to focus the maximum possible time on addressing an event.

Common Format for Incident Reporting

We were pleased to see in the draft Guidance that FSRA is willing to accept being notified of an incident with a comparable form issued by another financial services regulator. This greatly reduces the regulatory burden on companies as they will only be required to complete one form.

However, in keeping with the proposed FSB recommendations, we would strongly recommend a common format to allow for incident reporting exchange across Canada.

Insurers should not have ultimate responsibility for independent advisors

Within the Guidance, it is noted that there is an expectation that insurers be ultimately responsible for ensuring that IT risks are being effectively managed through all of its distribution channels. It is unclear what is meant by "ultimately responsible". As written, it could be interpreted to mean that the insurer is responsible for defining the IT risk management practices of independent MGAs and advisors.

While insurers are responsible for regulated individuals who are considered employees (e.g., in-house advisors), insurers are not responsible for the business practices of independent advisors. Independent advisors are responsible and liable for their own risk management practices, including IT risk management. Insurers would not have the authority to have this level of oversight. This is ultimately the responsibility of FSRA as the regulator to these entities.

Allow companies sufficient time for implementation

We recommend a period of two years for implementation of the Guidance as some companies will need to adjust existing internal processes and may need to hire new staff to meet the new requirements. We also request that the transition period be clearly defined when the final Guidance is issued.

SECTION TWO: INDUSTRY COMMENTS ON ALL SECTORS

Purpose and scope

CLHIA members support the intended purpose of the proposed Guidance. However, as noted above, we believe that the scope of the Guidance should exclude non-Ontario incorporated insurance companies who are already subject to similar guidance. Any supervisory oversight or enforcement action taken on a company's non-compliance should come from the company's primary regulator (e.g., OSFI, AMF).

We understand that other provincial regulators, where IT risk management guidelines do not exist, are considering similar guidance on IT risk management. We recommend that all regulators work together to ensure harmonization with the expectations within guidance, including expectations when there is an IT risk incident, and that oversight be coordinated so that companies are only supervised by one entity.

Rationale and background

CLHIA members believe the Guidance combines multiple operational risk categories under the umbrella of IT risk. For example, it includes security, information management, business continuity, and organizational change management in addition to IT risk. We recommend that the Guidance focus on elements solely under IT risk. We believe the scope of FSRA's guidance should be consistent with that of other regulators in order to support harmonization and coordination amongst regulators.

Interpretation

While we support the proposed guidance and risk management expectations in FSRA's requirements, as noted above, we believe that it is duplicative to require companies that are already subject to robust guidance and oversight from other regulators to comply.

Information

Generally, CLHIA members support the seven "practices" identified in the Guidance for effective IT risk management. However, we believe that the "desired outcomes" under the practices are not principles-based and are overly prescriptive. For example, under "practice 1", there is a desired outcome that requires that "clear responsibilities for the management of IT risks are assigned to an individual or individuals with sufficient seniority and expertise".

Companies should be allowed to have the flexibility to achieve the seven practices based on their own internal systems and procedures. It should be made clear in the Guidance that the "desired outcomes" are not requirements from a compliance standpoint.

This is especially important for smaller organizations, such as individual agents and agencies, as they may have difficulty in applying the "desired outcomes".

CLHIA members have provided additional comments on the practices for consideration:

- There is overlap between *Practice 5: Incident preparedness* and *Practice 7: Notification of material IT risk incidents*. We believe that these practices can either be combined or clarified as to why they are different.

- Under *Practice 4: Outsourcing*, the definition of "outsourced" and "co-sourced" includes all third-party arrangements. This is inconsistent with the approach taken by OSFI in its draft *Guideline B-10: Third party risk management*. We would recommend that FSRA update the terminology, once OSFI has finalized its guideline, in order to ensure alignment and harmonization between regulatory guidance.

Approach

We support the approach that companies have an IT risk management framework in place that aligns with its size, the nature, scope, and complexity of its operations, and risk profile.

With respect to incident reporting, we would recommend that FSRA harmonize with existing incident reporting requirements, such as the OSFI advisory. While the incident reporting criteria in the Guidance is largely consistent with OSFI's criteria, there are some indicators of a material incident that are unnecessarily broad and not included in OSFI's advisory.

We were pleased to see that FSRA will accept being notified with a comparable form issued by another financial services regulator. This will ensure consistency in reporting for FRFIs. However, for non-FRFIs, FSRA should align its incident reporting criteria with other regulators as much as possible.

As noted above, we also recommend that FSRA work with other regulators on an information sharing protocol that will allow information sent to a company's primary regulator to be shared with FSRA.

With respect to the timing of incident reporting, there is inconsistency within the draft Guidance. In one instance, the Guidance notes that incidents be reported on "as soon as possible". However, in another instance, the Guidance indicates that incidents be reported on within 48 hours. CLHIA members support the approach that incidents are reported "as soon as possible" versus providing a strict timeline. This gives companies the time to be able to determine the materiality of the incident.

SECTION THREE: INDUSTRY COMMENTS ON NON-ONTARIO INCORPORATED INSURANCE COMPANIES, INSURANCE AGENTS, INSURANCE ADJUSTERS, ADJUSTER FORMS, AND INSURANCE AGENCIES

Supervisory Approach

As noted above, we believe non-Ontario incorporated insurance companies subject to similar guidance should be excluded from the scope of the Guidance. We believe the Guidance would be a duplication of existing guidance and would place undue regulatory burden on companies. Any supervisory or enforcement action taken on a company's non-compliance should come from the company's primary regulator. Regulators should work together to ensure compliance with similar IT risk management expectations.

In addition, as noted above, CLHIA members are concerned with the expectation that insurers be ultimately responsible for ensuring that IT risks are being effectively managed through all of its distribution channels. Insurers do not have the authority to require independent advisors and agencies to have effective IT risk management practices in place. Some independent advisors and agencies outsource their IT functions, which would make it even more difficult for insurers to have oversight of these functions as companies would not have contractual relationships with these third parties. We believe that oversight of these entities rests with FSRA.

SECTION FOUR: INDUSTRY COMMENTS ON ONTARIO-INCORPORATED INSURANCE COMPANIES AND RECIPROCALS

Interpretation

Consistent with above, clarification is needed on the timing for incident reporting to FSRA. Under this section, the Guidance indicates that companies must notify FSRA of any material IT risk incident within

48 hours. However, in other instances in the Guidance, companies must report “as soon as possible”. We would recommend that FSRA maintain the “as soon as possible” for all entities required to report a material IT risk incident.

Criteria used to assess practice 1: Governance

CLHIA members would like clarification on the expectations for approval of policies for technology risk management and relevant standards. It is unclear whether these expectations need to be approved by the Board or by relevant management committees/senior leaders. We recommend that each individual company be able to assess the appropriate level of approval (e.g., Board versus senior management) based on their own internal structure of risk management programs.

It should be noted that in large organizations, governance elements, including frameworks, strategy reporting, and policy development fall within the purview of Enterprise or Operational Risk Management. The language in the Guidance suggests that companies must create a separate risk management stream for IT assets. We believe that companies should have the flexibility to manage IT risks based on their own internal practices.

Criteria used to assess practice 2: Risk management

We believe that the use of the word “practices” and “desired outcomes” is confusing. It is unclear what the expectations are for compliance with the “desired outcomes”. We believe that expectations need to be clearly defined to ensure companies are able to comply with the Guidance.

Further, we believe that risks associated with record retention and data quality fall under operational risks. Companies should be allowed to incorporate IT risk management practices within existing internal operational risk management practices rather than creating separate practices.

Criteria used to assess practice 3: Data management

CLHIA members believe that the criteria outlined in this section does not align with the desired outcome for practice 3. The criteria is more focused on the type of data (e.g., ensuring it is fit for purpose) rather than on ensuring the successful management and security of the data, as is the intended purpose of practice 3. We believe that FSRA should not dictate the type or quality of data that companies are collecting.

Further to this, we believe that the Guidance needs to be clearer on what is considered “confidential data”. We believe that the level of risk associated with the data will determine the level of confidentiality needed. Confidentiality should be prioritized for high risk data.

Criteria used to assess practice 4: Outsourcing

For this section, we would recommend that FSRA align its Guidance with the soon to be released OSFI *Guideline B-10: Third-Party Risk Management,* which is expected to be finalized in late Q1 2023/early Q2 2023.

We recommend that companies take a risk-based approach when applying the criteria to third-party activities. We do not believe that applying the same criteria to a low risk outsourcing arrangement will provide additional value. Companies should be focusing their efforts on high risk third-party arrangements.

For instance, the criteria includes the rights to audit and access information in its third-party contracts. This implies that all third-party contracts require the inclusion for rights to audit the third-party. We believe that the need to secure audit rights should be based on the nature of services that the third-party is providing, as well as the risk associated with the arrangement.

CLHIA members also believe that the requirement to establish an exit plan is too prescriptive. Instead, we recommend that third-party strategies are developed based on the level of risk and the nature of services being provided.

Criteria used to assess practice 5: Incident preparedness

The criteria states that companies must conduct periodic "independent reviews" of incident management processes and controls to ensure their effectiveness. It is unclear what is considered "independent". It is also unclear what the expectations are around the frequency of independent reviews. CLHIA members are seeking further clarity on this point.

Criteria used to assess practice 6: Continuity and resiliency

CLHIA members believe that continuity and resiliency are not unique to IT risks. We believe that these concepts are already being managed within existing internal risk management practices for all risks.

Further, we recommend that the Guidance include a definition of Project Management and its scope.

Criteria used to assess practice 7: Notification of material IT risk incidents

Comments on this section are consistent with what has already been noted regarding harmonization of reporting expectations amongst regulators and ensuring there is clarity around timing for reporting of incidents. As noted above, we are recommending that FSRA work with other regulators on an information sharing protocol that will allow information sent to a company's primary regulator to be shared with FSRA.

SECTION FIVE: INDUSTRY COMMENTS ON APPENDICES

Appendix 1: Examples of IT risk incidents

With respect to internal data breaches, as written it could be interpreted to include all internal incidents, including those that are not material. We would recommend including the following text:

> "An employee or contractor has either purposefully or unintentionally caused the exposure of confidential data **that results in a real risk of significant harm to individuals**."

With respect to internal systems malfunction, as written, the materiality of the incident is solely based on the length of time of the outage and not on the impact to a company's business. If the ability to provide essential services to customers is not impacted, we would not consider this to be a material IT risk incident. We recommend using the example similar to the one used by OSFI:

> **"Technology failure at data center. Critical online service is down and alternate recovery option failed. Extended disruption to critical business systems and operations."**

Appendix 2: IT Risk Notification Form

As noted above, we were pleased to see in the draft Guidance, FSRA is willing to accept being notified of an incident with a comparable form issued by another financial services regulator. This greatly reduces the regulatory burden on companies as they will only be required to complete one form. We would strongly recommend that FSRA align its form as much as possible with the ones developed by other regulators, such as OSFI. This will ensure consistency of reporting incidents across regulators.

Should FSRA decide to proceed with its own reporting form, we believe that the "scale" within the form needs to be clearly defined to ensure consistency in the value being placed using the scale (e.g., what does a 1 versus 10 mean in the scale?).

CONCLUSION

Thank you for the opportunity to provide our comments on the draft proposed *Information Technology ("IT") Risk Management Guidance*. Should you have any questions or wish to discuss further, please do not hesitate to contact Devika Prashad, Vice-President and Chief Actuary, at dprashad@clhia.ca.

Canadian Life & Health Insurance Association

Association canadienne des compagnies d'assurances de personnes

79 Wellington St. West, Suite 2300
P.O. Box 99, TD South Tower
Toronto, Ontario M5K 1G8
416.777.2221
info@clhia.ca