FSRA
Financial Services Regulatory Authority of Ontario

Guidance

☒ Interpretation ☒ Approach ☒ Information ☐ Decision

Effective Date: [TBD]
Identifier: No. PC0050INT

Proposed Guidance: Operational Risk and Resilience for Ontario-incorporated Insurance Companies and Reciprocal Insurance Exchanges

Purpose

The Financial Services Regulatory Authority of Ontario's ("**FSRA's**") Operational Risk and Resilience Guidance (the "**Guidance**") for Ontario-incorporated Insurance Companies and Reciprocal Insurance Exchanges (collectively the "**Insurers**") provides:

i. FSRA's interpretation of the operational risk and resilience requirements for the Insurers under the Risk Management Requirement in the MCT Guideline (as defined below) under the *Insurance Act* (the "***Act***")

Ontario

ii. FSRA's approach for assessing how the Insurers effectively adhere to the requirements in the Interpretation section of this Guidance and achieve the intended outcomes identified in this Guidance

iii. information on Environmental, Social and Governance (**ESG**) risk management guidance/standards, that have been developed by other jurisdictions and standard-setters, and potential future implications for the Insurers

The Guidance aims to enhance operational risk identification, assessment, and management, and non-financial resilience by improving the Insurers' ability to monitor their current environment, anticipate future threats and opportunities, respond effectively to stress events, and learn from past failures and successes.

Amendment to FSRA MCT Guideline

Section 102(8) of the *Act* requires that "Every insurer licensed under this Act shall maintain capital or assets (in compliance with such requirements as may be prescribed by regulation governing the level of capital or assets to be maintained) in an amount that bears not less than a reasonable relationship to the outstanding liabilities, premiums and loss experience of the insurer." Ontario Regulation 259/04 - Minimum Capital Test establishes the requirements for the purpose of s. 102(8) and incorporates FSRA's Guidance No. PC0047INT, **Minimum Capital Test Guideline for Property and Casualty Insurance Companies and Reciprocals - January 2023** (the "**MCT Guideline**") by reference, making it mandatory for every Insurer required to comply with s. 102(8) to maintain capital in compliance with the requirements set out in the MCT Guideline. FSRA can amend the MCT Guideline incorporated into O. Reg. 259/04 from time to time pursuant to s. 1(1) of O Reg. 259/04.

The MCT Guideline has been amended to include the following additional provision (the "Risk Management Requirement"):

> **Risk Management Requirement**
> Senior Management of an Insurer shall establish, develop, update, and implement, and the Board of the Insurer shall oversee and approve:
>
> **(i)** A risk management framework, which

a. provides a reasonable basis for Senior Management and the Board to understand and manage the Insurer's risks and potential liabilities

b. facilitates and protects the Insurer's stability and viability, through the identification, assessment, management and monitoring of all risks which may arise from the business and operations of the Insurer and its subsidiaries and have a potentially material impact on the Insurer's financial performance, capital, liquidity, stakeholders, reputation, operations or viability, and includes an enterprise-wide risk appetite framework which is appropriate relative to the risk profile of the Insurer on an enterprise-wide basis, its long-term strategic plan and its operating environment

c. strategies, procedures, policies, and processes to understand and evaluate all such risks, and to facilitate direct reporting to the Board of the Insurer by the Senior Management

The Approach section of this Guidance sets out FSRA's processes and practices for assessing Insurers' operational risk and resilience in accordance with FSRA Approach Guidance No. PC0045APP, **Risk Based Supervisory Framework for Ontario-incorporated Insurance Companies and Reciprocals** ("RBSF-I") and may have implications for Insurers' Overall Risk Rating (ORR). The impact of operational risk and resilience measures on the ORR is two-fold: (1) operational risk identification, assessment, and management will be considered when assessing inherent risks and quality of controls and oversight as part of the determination of the Prudential Summary Residual Risk (PSRR); and (2) resilience of the Insurers' will be assessed and reflected in the Resilience Rating, which will be used to modify the Summary Residual Risk Rating (SRR) to determine the Overall Risk Rating (ORR).

The Information section of this Guidance acknowledges that some Insurers have begun considering ESG factors in their risk management practices, summarizes some of the guidance/standards relating to ESG risk management that have been developed by other jurisdictions and standard-setters, and outlines potential future implications for the Insurers.

FSRA will apply this Guidance and consider potential consequences resulting from non-compliance, in a proportional manner, based on the size, complexity, and risk profile of the Insurer.

Scope

This Guidance affects the following entities regulated or registered by FSRA:

- insurers incorporated under the *Corporations Act* (Ontario) and licensed by FSRA under the *Act*
- reciprocal insurance exchanges licensed by FSRA under the *Act*

This Guidance complements and should be read in conjunction with the forthcoming FSRA Guidance PC0051INT, **Corporate Governance Guidance for Ontario-incorporated Insurance Companies and Reciprocal Insurance Exchanges** (spring/summer 2024) and other FSRA Guidance and supporting publications found on FSRA's webpages.

Rationale and background

Insurers increasingly rely on technology, data, and third parties in their daily operations. As such, FSRA is placing a high degree of importance on operational risk identification, assessment, and management, as well as operational resilience.

Operational Risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risks. Reputational risk is a consequence that may arise from operational risk materialization.

Operational Resilience is an outcome that benefits from Insurers' effective treatment of operational risk during business-as-usual (BAU) or under stress and contributes to Insurers' safety and soundness. Insurers that have a high degree of resilience are more likely to incur shorter lapses in their operations and experience smaller losses from operational disruptions, thus lessening incident impact on critical operations and related services, functions, and systems. Achieving operational resilience may require Insurers to adopt a new mindset with an added perspective, develop preparedness and awareness plans, and implement effective strategies when moving from BAU to a stress environment.

This Guidance supports FSRA's statutory objects, as set out in ss. 3(1) and 3(2) of the *Financial Services Regulatory Authority of Ontario Act*, *2016*, including:

- to regulate and generally supervise the regulated sectors
- to contribute to public confidence in the regulated sectors
- to promote high standards of business conduct
- to foster strong, sustainable, competitive, and innovative financial services sectors

FSRA supervises the Insurers to assess how effectively they consider and manage their operational risk and implement resilience measures to promote high standards of business conduct. This helps Insurers operate in a sustainable manner when faced with operational risks and adverse events (including natural disasters and catastrophic loss), thereby contributing to public confidence in the insurance sector.

Definitions

Terms used in this Guidance, unless otherwise defined in this Guidance, have the meaning given to these terms in the *Act*. In this Guidance:

"**Board**" means an Insurer's board of directors or a reciprocal insurance exchange's advisory board.

"Senior Management" means an officer as defined s. 1(2) of but does not include individuals excluded form that definition in s. 1(3) of Ont. Reg. 123/08, *Corporate Governance – Part II.2 of* the *Act*.

Interpretation

Insurers that must comply with the MCT Guideline and the 2023 Office of the Superintendent of Financial Institutions ("**OSFI**") MCT guideline adopted by FSRA in the MCT Guideline must comply with the Risk Management Requirement because it has the force of law pursuant to s. 2 of O. Reg. 259/04: **Minimum Capital Test**.

Insurers are required to prudently manage their capital to maintain financial strength, absorb losses to withstand adverse conditions (financial and non-financial), allow for growth and meet other risk and business objectives, and policyholder obligations. As part of prudently managing their capital, Insurers should have practices in place to identify, assess and manage their enterprise-wide risks, which include operational risk. Due to the interdependency between risk management and capital management, FSRA views the Risk Management Requirement in the MCT Guideline as requiring the Insurers to implement effective operational risk management. The Risk Management Requirement, as interpreted below, supports prudent risk and capital management.

Adherence to the Risk Management Requirement should be done in a manner consistent with the principles set out in the Interpretation section of this Guidance which is in the best interest of Insurers and their policyholders. The principles describe FSRA's intended outcomes that, when achieved by Insurers, demonstrate effective operational risk identification, assessment, and management as well as resilience upon materialization of operational risk events. FSRA will monitor and assess how effectively the Insurers adopt these principles as part of its supervisory approach, which is outlined in the Approach section of this Guidance.

The MCT Guideline does not apply to Insurers that are reciprocal insurance exchanges pursuant to s. 4 of O. Reg. 259/04. Mutual insurance corporations that are members of the Fire Mutuals Guarantee Fund ("FMGF") do not need to comply with s. 102(8) of the *Act* and, by extension, with the MCT Guideline incorporated into O. Reg. 259/04. For these insurers, all references to "must", "shall", and "requires" and similar words that state a requirement under Principles 1 to 3 of the Interpretation section of this Guidance are deemed to say "may", "should", or "can" or similar words. For these Insurers, Principles 1 to 3 indicate common industry practices that FSRA will assess against under the RBSF-I. Not meeting the intended outcomes of the principles may result in an elevated level of supervisory engagement.

S. 169(4)(a) of the *Act* allows FSRA the discretion to specify further amounts of assets that the FMGF must maintain beyond $1 million in book value. Under s. 169(3) of the *Act*, the purposes of the FMGF include paying the insurance claims of policyholders of members of FMGF, if a member of the FMGF is unable to meet its obligations. Weak operational risk management practices can increase an Insurer's exposure to losses from operational risks. A loss from an operational risk increases the risk that a claim of a policyholder of an FMGF member will not be paid. Hence, for a mutual insurance corporation that is a member of the FMGF, FSRA may consider the Insurer's adherence to the Principles in the Interpretation section of this Guidance to help determine the further amount of assets that the FMGF must have pursuant to s. 169(4)(a) of the *Act*.

Principles

Principle 1: Governance

Ultimate accountability and responsibility of operational risk oversight rests with the Insurer's Board and Senior Management.

Sound operational risk management and resilience reflects the effectiveness of an Insurer's Board and Senior Management in administering the Insurer's portfolio of products, activities, processes, and systems, resulting in reduced frequency and impact of operational risk events.

Under the Risk Management Requirement, the Board is responsible for establishing the necessary strategies and governance structures, overseeing and approving Insurers' operational risk management program, as well as ensuring that there are adequate resources to carry out their operational risk management activities, and meet policyholder obligations. FSRA's interpretation is that for a Board to fulfill its obligations under the Risk Management Requirement, it is required to periodically review and approve the Insurer's Operational Risk Management Framework (**ORMF**) and supporting frameworks (e.g., third-party risk management framework, information technology framework, incident management framework) or similar construct according to the Insurer's size, complexity, and risk profile, which will include the Insurer's operational risk appetite, tolerance, and limits. The Board is also required to review the Insurer's business continuity plan

("**BCP**") and disaster recovery plan ("**DRP**"). To define the Insurer's risk appetite and review the ORMF's alignment with it, the Board must clearly articulate the nature, types, and levels of operational risk that Insurers are willing to assume and ensure that they are providing adequate and effective oversight on that basis.

Under the Risk Management Requirement, Senior Management is responsible for developing, updating, and implementing the policies, processes, and systems used to manage operational risk and enhance operational resilience effectively at all decision levels and ensuring that it is understood among staff, third parties, and other relevant stakeholders based on the level of their involvement in managing the risks. FSRA's interpretation of the Risk Management Requirement is that to fulfill its obligations, Senior Management must establish the respective roles and responsibilities necessary to effectively identify, assess, manage, and oversee operational risk. As the Board is responsible for the oversight and governance of risks, under the Risk Management Requirement, an Insurer's operational risk profile in relation to the Board-approved risk appetite and tolerance must be measured by Senior Management and presented to the Board to confirm alignment.

Governance structures with well-defined accountabilities and responsibilities, reporting lines, and decision-making authorities support the management of operational risk and Insurers' resilience. FSRA's view is that compliance with the Risk Management Requirement necessitates that Insurers establish an organizational structure where operational risk management activities are conducted by operational management (first line of defence), are reviewed and challenged by risk management (second line of defence), and independent assurance is then provided by internal audit (third line of defence), facilitating effective governance, oversight and risk management.

Principle 2: Operational risk identification and assessment

Comprehensively identifying, assessing, and understanding the operational risk inherent in all of the Insurer's products, activities, people, processes, and systems, as well as in its external environment, enables the development and implementation of corresponding risk response strategies.

FSRA considers that adherence with the Risk Management Requirement necessitates that an Insurer regularly perform environmental scans of its operations to support the Insurer's

ability to comprehensively identify, assess, and manage operational risk inherent in all their products, activities, people, processes, and systems, as well as those in the external environment. Activities, processes, and systems subject to the environmental scan include information technology used to support the Insurer's business operations. Understanding these inherent risks will facilitate informed decision-making and enable effective risk management.

Principle 3: Operational risk management

An effective operational risk management framework enables a stable operational environment for the Insurer's businesses, reduces the probability of disruption, and minimizes the risk of loss to policyholders.

In accordance with the Risk Management Requirement, an Insurer must implement a robust operational risk management program to reduce the frequency of risk materialization and the impact of operational risk events on the Insurer's policyholders and other stakeholders. An Insurer's approach to managing operational risk must be carefully considered, adequately documented, and periodically updated to reflect changes in the Insurer's operating environment, risk appetite and tolerance, and/or advancements in risk management capabilities.

FSRA interprets the Risk Management Requirement to necessitate that an Insurer develop and implement frameworks and supporting policies and procedures to facilitate reasonable treatment, including identification, assessment, mitigation, monitoring, and reporting of its operational risk exposures commensurate with the Insurer's size, complexity, and risk profile. An Insurer's ORMF, and any supporting frameworks or similar construct, are aligned and integrated with the Insurer's enterprise-wide risk management program.

Principle 4: Resilience

The Board and Senior Management plan for adverse scenarios and ensure that the Insurer is crisis ready. The Insurer achieves resilience during BAU through enhancing crisis preparedness and improving its ability to monitor and anticipate any escalation of risks. Upon operational risk materialization, the Insurer responds and adapts by taking feasible and timely actions and leveraging pre-determined processes and protocols to facilitate streamlined and effective recovery. The Insurer will also review

and re-evaluate processes and protocols in light of past failures and successes, aiming for continuous improvements to resiliency.

Operational Resilience is a key component of an effective operational risk management framework and an outcome that benefits from the Insurer's effective treatment of operational risk during BAU or under stress and contributes to the Insurer's safety and soundness. Achieving operational resilience may require the Insurer to adopt a new perspective, develop awareness, and implement effective strategies when transitioning from BAU to a stress environment. Effective governance (Principle 1) along with robust identification and assessment (Principle 2) and management (Principle 3) of operational risk improve the Insurer's ability to achieve this outcome.

Operationally resilient Insurers can deliver critical operations through disruption and are less prone to experiencing operational risk events. If operational risk materializes, resilient Insurers are more likely to incur shorter lapses in their operations and experience smaller losses from disruptions, thus lessening incident impact on critical operations and related services, functions, and systems.

Approach

Processes and practices

This section of the Guidance describes FSRA's approach to the assessment of the Insurer's operational risk management framework and resilience practices and describes the processes and practices which FSRA will use to assess the Insurer's adoption of the principles identified in the Interpretation section of this Guidance to meet intended outcomes. Refer to FSRA's RBSF-I for details on the Risk Assessment Process.

FSRA uses the RBSF-I to identify imprudent or unsafe business practices that may impact policyholders, subscribers, and customers of Insurers and will intervene on a timely basis if warranted. FSRA will exercise supervisory judgement and assess the most important risks posed by the Insurer to supervisory objectives and the extent to which the Insurer can identify, assess, and manage these risks as well as achieve resilience.

FSRA's assessment of the Insurer's operational risk as an Inherent Risk

When assessing an Insurer under **Principle 2: Operational risk identification and assessment**, FSRA will assess operational risk as an Inherent Risk intrinsic to the Insurer's significant activities (e.g., a line of business, business unit, or enterprise-wide process such as Information Technology). FSRA evaluates Inherent Risk before any mitigation and considers the probability and impact of an adverse event to the Insurer's capital and earnings.

Operational risk could originate from the Insurer's products, activities, people, processes, systems, and external environment. The Insurer considers the complexity of its products and services, delivery channels, and level of automation when identifying the nature and complexity of operational risk at the organization.

Operational risk is a broad concept and includes various sub-risks such as, but not limited to, third-party risk, cyber risk, data risk and climate risk (physical and transition):

- Third-party risk arises when an Insurer engages a third party for the provision of a product or service and the third-party fails to deliver the product/service as a result of the risks inherent to its own activities.

- Cyber risk is the risk of financial loss, operational disruption or damage from the unauthorized access, use, disclosure, disruption, modification, or destruction of an Insurer's information technology systems and/or data.

- Data risk arises when inadequate data governance and data infrastructure are in place to ensure data integrity and availability to support an Insurer's day-to-day operations, internal risk reporting, and decision-making. Data risk often intersects with other risk areas such as cyber risk, third-party risk, and advanced analytics. Data risk materialization can occur when Insurers have inadequate processes and cyber security controls to safeguard confidential consumer data from a potential privacy breach.

- Physical climate risk arises from a changing climate increasing the frequency and severity of wildfires, floods, storms, wind events and rising sea levels, among other events. Climate events could disrupt critical operations when physical assets owned by the Insurer or its third-party service providers are damaged, such as real estate and infrastructure. Physical risk can also amplify underwriting risk through potential

increases in insurance claims for property damage in respect of a wide range of assets, including real estate, infrastructure, and natural resources.

FSRA's consideration of the Insurer's information technology as a significant activity of the Insurer

The use of information technology has been a key enabler of the effective delivery of an Insurer's products and services but may also result in significant operational risks. Operational risks associated with information technology emerge from a broad range of functional areas and business operations. Systems and infrastructure could become inadequate (due to, for example, obsolescence, insufficient upgrades, poor system conversions, unsuccessful/ineffective integration between systems after a merger with another Insurer) or could be misused (due to, for example, misaligned fit for purpose, unauthorized access), which may contribute to operational risks of the Insurer.

In leveraging information technology to support digitization and better meet the evolving demands of policyholders, Insurers have been increasingly relying on third-party providers, including cloud service providers, in their business models. This reliance has resulted in new opportunities for Insurers but has also exposed Insurers to new risks and vulnerabilities.

FSRA's assessment of the Insurer's Quality of Controls and Oversight ("QCO") in managing operational risk

FSRA will assess the extent to which the level of controls and oversight at the Insurer is adequate to mitigate its inherent risks. FSRA's assessment will evaluate the extent to which the Insurer adopts practices set out under **Principle 2: Operational risk identification and assessment** and **Principle 3: Operational risk management** in the Interpretation section of this Guidance. For each of the Insurer's significant activities, FSRA will consider both QCO characteristics and performance in the context of the Insurer's size, complexity, and risk profile.

When assessing the Insurer's operational risk management, FSRA will evaluate the extent to which the Insurer's operational management has identified the potential for material losses originating from activities and whether adequate processes and controls are in place to mitigate those operational risks when materialized. Among other things, this would include an

assessment of the effectiveness of an Insurer's operational risk management tools (e.g., operational risk taxonomy, risk and control assessments, loss data collection) to identify, assess, and manage its operational risks. FSRA will also evaluate an Insurer's Oversight Functions (i.e. Actuarial, Compliance, Risk Management, Internal Audit, Senior Management, and Board) in order to assess the extent to which they provide effective independent enterprise-wide oversight to operational management and whether the Insurer's operations and risk exposures are consistent with its operational risk appetite and tolerance. As part of this assessment FSRA will also consider how effectively Insurers are adopting the practices described under **Principle 1: Governance in the Interpretation section of this Guidance**. For smaller Insurers, independence may be achieved through separation of functional duties between individuals and independent review of processes and functions.

FSRA's approach in assessing the Insurer's information technology (including cyber) risk management

In assessing the Insurer's QCO functions as they relate to the management of information technology (IT) risks, FSRA will evaluate the extent to which an Insurer's information technology and cyber risks are managed through clear accountabilities and reporting structures (**Principle 1: Governance**). It is important for an Insurer's technology strategies and cyber plans to be commensurate with its size, and complexity, and risk profile.

FSRA will assess the Insurer's ability to identify, assess, and manage IT risks against **Principle 2: Operational risk identification and assessment** and **Principle 3: Operational risk management** as set out in the Interpretation section of this Guidance, as well as FSRA Guidance No. GR0016INT, **Information Technology ("IT") Risk Management** **FSRA's IT Risk Management Guidance**. FSRA will evaluate the extent to which the Insurer's IT risk management program consists of, but is not necessarily limited to, the following:

- processes to identify and assess significant IT risks based on the likelihood and impact of IT risk events

- adequate controls in the IT control environment to prevent, detect, and manage unauthorized access to the Insurer's network and systems (e.g., by establishing identity and access management controls, audit trail, encryption, firewalls, and server

hardening)

- identification, classification, and maintenance of technology assets to ensure integrity

- monitoring, logging, managing, resolving, and reporting IT incidents to ensure service standards and business objectives are met, with associated risks sufficiently mitigated within Insurer's risk appetite. It is important that Insurers provide FSRA with timely notification of material IT risk incidents as described in FSRA's **IT Risk Management Guidance**.

- monitoring and managing currency of technology (including safe disposal of end-of-life technology assets) to support a robust, secure, and resilient operating environment for business activities

- managing and implementing IT projects and technological changes or updates effectively with sufficient processes to minimize potential disruptions

- implementing cyber security awareness training

FSRA will assess the extent to which the Insurer safeguards the confidentiality, integrity, and availability of its own information technology assets and understands the magnitude and impact of weaknesses in the IT control environment which could potentially be exploited by both external and internal threat actors. As part of this, FSRA will look for evidence that the Insurer's IT security controls are adequate to protect, detect, respond, recover, and learn from IT incidents. For situations where the Insurer is outsourcing these activities, FSRA will assess the Insurer's review and understanding of the controls put in place by its third-party providers to manage these risks. In addition, it is important for the Insurer to enhance its resilience characteristics and performance in preparation for, and in the event of, technology service disruptions.

FSRA will evaluate the extent to which the Insurer periodically reviews and updates its BCP/DRP to reflect its current operations, risks, and threats, as well as regularly test these plans against severe but plausible scenarios that could impact the Insurer's critical business operations to ensure plans remain effective. FSRA will consider the extent to which the

Insurer's BCP/DRP articulate roles and responsibilities, define thresholds/ triggers for plan activation, incorporate quantitative/qualitative impact assessments or business impact analyses, establish recovery objectives, and include incident response and communication plans (**Principle 4: Resilience**).

FSRA's approach in assessing the Insurer's third-party risk management

Insurers are increasingly relying on third-party providers to innovate, provide technology services, and/or fulfill operational needs. While these third-party providers may increase organizational efficiency and reduce costs, they also may expose the Insurer to additional risks. Irrespective of the arrangement, the Insurer retains accountability and ownership of all risks including those introduced by engaging third parties. As such, the Insurer should establish a third-party risk management framework, or similar construct, and ensure the dedication of adequate resources with the necessary skills/expertise to implement the framework because these are essential to support effective management of risks borne by engaging these third-party providers (**Principle 1: Governance**).

FSRA will evaluate the extent to which the Insurer's third-party risk management framework supports a consistent and sound approach to managing third-party risks throughout the third-party lifecycle. Among other things, FSRA will assess the extent to which the Insurer performs due diligence prior to onboarding a third-party and on an ongoing basis. This includes understanding concentration risk and the implications in the event of a material disruption at a dominant third-party provider (e.g., contagion risk). In addition, FSRA will assess the effectiveness of procurement/contracting processes and the appropriateness of contract provisions to manage the risks associated with the arrangement. This may include requirements to notify the Insurer of material incidents or use of subcontractors, rights to access information and audit, or requirements to operate within established risk and performance measures. FSRA will also assess the extent to which the Insurer is continuously monitoring and reporting on its third-party risk to ensure that products/services are delivered in accordance with contractual arrangements and whether risks are appropriately managed and aligned with the Insurer's risk appetite (**Principle 2: Operational risk identification and assessment** and **Principle 3: Operational risk management**).

As it relates to the Insurer's BCP/DRP, FSRA will also look for evidence that the Insurer has considered concentration risk as well as the interconnections between, and

interdependencies of, its third-party providers. FSRA will assess the appropriateness of the Insurer's plans and measures (e.g., conducting scenario testing, establishing redundancies) for ensuring business continuity in the event of an outage or disruption at a third-party (**Principle 4: Resilience**).

FSRA's approach in assessing the Insurer's data management and governance

FSRA will evaluate the extent to which the Insurer's data governance is supported through clear accountabilities and reporting structures. FSRA will assess the Insurer's data governance framework (or similar construct) to determine the extent to which they clearly define roles and responsibilities (**Principle 1: Governance**) and sufficiently identify, assess, and manage data risk (**Principle 2: Operational risk identification and assessment** and **Principle 3: Operational risk management**).

FSRA will assess whether the Insurer has sufficient data capabilities to support informed decision-making, not only in BAU but also in stress conditions (**Principle 4: Resilience**).

FSRA's approach in assessing Operational Risk and Resilience as it relates to the Insurer entering new business activities

When the Insurer is entering into any new business activity, either itself or through a subsidiary or affiliate, which involves technological innovation and new uses, or sharing of policyholder data or information, FSRA will assess the extent to which the Insurer has robust governance and effective operational risk identification, assessment, and management in the undertaking of new business activities. FSRA will also evaluate the extent to which the Insurer has:

- established policies, procedures, and practices to manage the risks introduced by entering new business activities, such as data risk and IT risk (see Approach section above)

- demonstrated reasonable care in handling consumer financial data with sufficient security measures, including the way confidential and sensitive data is safeguarded

and policyholders are appropriately compensated for, and protected from, future loss

- considered possible liability, privacy, and security issues when handling policyholder data

FSRA's resilience assessment of the Insurer

FSRA will assess the Insurer's resilience in accordance with **Principle 4: Resilience**. FSRA will also assess whether an Insurer follows market practices on how Insurers should plan for adverse scenarios and operational risk materialization. During supervisory monitoring, FSRA may direct an inquiry to require that the Insurer present its BCP, DRP, or any relevant report to demonstrate its stress and scenario testing activities, and overall resilience during stress environments.[1]

Overall resilience of the Insurer is assessed holistically through financial and non-financial factors and considers BAU and post-stress event conditions. Financial resilience factors include capital and liquidity on a current state and forward-looking basis. Non-financial factors are generally governance and operational based but also require adequate human capital and supporting resources while focusing on crisis preparedness. Some key indicators of resilience characteristics and performance are the strength of an Insurer's capital management policy; adequacy and implementation of Recovery Plan; Contingency Funding Plan; Business Continuity Plan and Disaster Recovery Plan during stress.

In assessing an Insurer's resilience, FSRA will consider the way the Insurer operates both in a BAU environment and when it is forced into a stress (non-BAU) environment. FSRA will consider the Insurer's ability to respond and recover effectively from disruption after an operational risk or crisis has materialized.

FSRA will assess resilience from a characteristic and performance perspective. Resilience characteristics are demonstrated during a BAU environment; at which time the Insurer enhances its crisis preparedness through improving its ability to monitor and anticipate any escalation of

[1] Para. 442.1(1) 1 of the Act.

risks. Resilience performance of the Insurer is demonstrated by its ability to respond and adapt to stress by taking feasible and timely action, leveraging pre-determined processes under pre-established protocols to facilitate streamlined and effective recovery. FSRA will also consider the extent to which the Insurer learns from past failures and successes for continuous improvements towards achieving resiliency.

The following are some specific areas on which FSRA will focus its assessment of an Insurer's resilience characteristics and resilience performance. These areas reflect the principles set out in the Interpretation section of this Guidance:

- governance
- crisis and incident preparedness via contingency, continuity, and recovery planning
- operational risk management, especially the management of IT, third-party, and data risks
- environmental, social and governance considerations (see Information Guidance below)

In assessing the Insurer's resilience rating, FSRA will look for evidence of an Insurer's ability to monitor and anticipate escalating risks during BAU, demonstrating its resilience characteristics. This includes but is not limited to, the extent to which:

- the Board has periodically reviewed reporting of actual Insurer metrics, as measured against the management/board triggers, describing the Insurer's holistic state of financial health
- there is evidence of periodic communication between the Board and Senior Management
- the strength and adequacy of the Insurer's capital management, including the number, severity, and overall quality of stress scenarios used to assess capital adequacy
- the quality of the Insurer's business contingency plans, and if they are adequate, given

its size, complexity, and risk profile

FSRA will look for evidence of an Insurer's ability to respond to and learn from stress events, demonstrating resilience performance. For example, FSRA will consider the extent to which:

- actions have been taken by Senior Management and the Board based on protocols and criteria described in the Insurer's business continuity plans, disaster recovery plans, contingency plans, and upon activation of these plans, and the effectiveness of such actions

- there have been continuous improvements to the Insurer's operations and practices based on lessons learned

The above examples are non-exhaustive and have been provided only for illustrative purposes.

Information

Climate change and the global response to the threats it poses have the potential to significantly impact the safety and soundness of Insurers and the financial system more broadly. "Climate-related risks" are broadly categorized as physical and transition risks. Physical and transition risks can also lead to liability risks, such as the risk of climate-related claims under liability policies, as well as litigation and direct actions against financial institutions for failing to manage their climate-related risks. They can drive financial risks, such as credit, market, insurance, and liquidity risks for Insurers. They can also lead to strategic, operational, and reputational risks. In severe instances, climate-related risks can threaten the long-term viability of an Insurer's business model and the stability of the sector.

Regulators around the world and standard-setting bodies such as the Financial Stability Board[2], International Financial Reporting Standards ("IFRS"), and the International Association of

[2] Financial Stability Board

Insurance Supervisors[3] have been developing regulatory responses to the physical and transition risks of climate change in recent years.

In June 2023, the International Sustainability Standards Board ("ISSB") issued its first two IFRS Sustainability Disclosure Standards: **IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information** and **IFRS S2 Climate-related Disclosures**. IFRS S2 sets out the requirements for companies to disclose information about their climate-related risks and opportunities, while building on the requirements in IFRS S1. IFRS S2 integrates and builds on the recommendations of the Task Force on Climate-related Financial Disclosures and requires the disclosure of information about both cross-industry and industry specific climate-related risks and opportunities. In alignment with this, the Canadian Sustainability Standards Board announced its first proposed Canadian Sustainability Disclosure Standards on March 13, 2024, setting a new benchmark for the disclosure of sustainability-related information, and facilitating a more consistent and comparable approach.[4]

Some Insurers have already started working towards developing and meeting ESG objectives. FSRA recognizes these efforts and encourages Insurers to continue progress towards further incorporation of ESG goals and climate risk management into their corporate strategies and business activities.

Going forward, FSRA will consider the integration of ESG goals into its regulatory and supervisory frameworks, which may include issuing additional guidance to address climate-related risks, aspects relating to natural disaster and catastrophe risk, and governance practices that are aligned with the *FSRA Act* and the *Insurance Act*. In the interim, Insurers are encouraged to develop and implement plans to include ESG considerations in their corporate strategies, business plans, and business activities to ensure positive contributions towards ESG goals.

Other Canadian financial services regulators have released guidance/standards relating to ESG risk management; in particular, addressing the following areas:

---

[3] International Association of Insurance Supervisors
[4] Canadian Sustainability Disclosure Standards

- climate-related physical and transition risks requiring frameworks, policies, disclosures, metrics, targets, as well as establishment of a complete understanding of the supply chain
- social risks requiring a focus on human and labour rights, diversity, community, and customers
- governance risk requiring appropriate mitigation frameworks

Currently, FSRA assesses Insurers' ESG (especially climate risk) initiatives under the RBSF-I as part of their Resilience Rating. FSRA may issue observations to Insurers through their supervisory process, but any observations on ESG will not punitively contribute to Insurers' ORR rating until, and if, future guidance is issued.

Effective date and future review

This Guidance will be effective as of **[TBD]** and will be reviewed on or before **[TBD]**.

About this Guidance

This document is consistent with FSRA's Guidance Framework. As Interpretation guidance, it describes FSRA's view of requirements under its legislative mandate (i.e., legislation, regulations, and rules) so that non-compliance can lead to enforcement and/or heightened supervisory action. As Approach guidance, it describes FSRA's internal principles, processes, and practices for supervisory action and application of CEO discretion where applicable. The Approach section of this Guidance may refer to compliance obligations but does not in and of itself create a compliance obligation. The Information section of this guidance describes FSRA's views on certain topics without creating new compliance obligations for regulated persons.

Effective date: TBD