Proposed Operational Risk and Resilience Guidance & Corporate Governance Guidance

for Ontario-incorporated insurance companies and reciprocal insurance exchanges ("Insurers")

Information Webinar

Financial Services Regulatory Authority of Ontario

Date: **June 5, 2024**

Speakers:
Victoria Lesau, Director, Credit Union, Insurance Prudential and Pension Policy
Amber McNair, Senior Manager, Credit Union and Insurance Prudential Policy
David Maxwell, Head, Regulation and Strategic Initiatives, Credit Union and Insurance Prudential (CUIP)

Ontario

Agenda

- Introductions
- Land acknowledgement
- Background
- Overview of the Proposed Operational Risk and Resilience Guidance
- Overview of the Proposed Corporate Governance Guidance
- Summary
- Questions

FSRA
Financial Services Regulatory Authority of Ontario

Ontario

Introductions

Victoria Lesau, Director – Credit Union, Insurance Prudential and Pensions Policy

Amber McNair, Senior Manager – Credit Union and Insurance Prudential Policy

David Maxwell, Head – Regulation and Strategic Initiatives

Land Acknowledgement

We acknowledge the land we are on is the traditional territory of many nations including the Mississaugas of the Credit, the Anishnabeg (ah-nish-naw-bek), the Chippewa, the Haudenosaunee (hoodt-en-oh-show-nee) and the Wendat peoples and is now home to many diverse First Nations, Inuit and Métis peoples. We acknowledge that Toronto is covered by Treaty 13 with the Mississaugas of the Credit and the Williams Treaties signed with multiple Mississaugas and Chippewa bands.

Principles Based Regulation (PBR)

What is Principles Based Regulation (PBR)?

- PBR is a regulatory approach that relies on high level**, broadly stated principles that are outcomes focused**, as opposed to just prescriptive rules.

Benefits

- Gives regulators and stakeholders the **flexibility** to respond to market changes, innovation and actual market practices and apply the requirements on a **proportional** basis.
- PBR makes use of **qualitative and evaluative terms** (e.g. “fair”, “reasonable”, “suitable”) to facilitate compliance, adherence or alignment as it allows entities to honour the spirit of the law.

Proposed Operational Risk and Resilience and Corporate Governance Guidance

- The Operational Risk and Resilience & the Corporate Governance Guidance are both consistent with **FSRA’s principles-based and outcomes-focused regulatory approach**.
  - Both pieces of guidance set out high level principles that are consistent with industry practices to achieve FSRA’s intended outcomes.
  - If Ontario Insurers meet and demonstrate the intended outcomes commensurate to their size and complexity, they are more likely to operate in a sustainable manner.

Overview of RBSF-I

Knowledge of Business

RBSF-I is predicated on gaining a thorough understanding of each Insurer's business including specific structures, processes, governance frameworks, staff and the board.

Proportionality

Given the unique nature of Ontario Insurers, the level and extent of supervision under the RBSF-I will depend on the **size, complexity, and risk profile** of the Insurer, and the potential consequences of an Insurer's failure including systemic impact.

Transparent, open, and continuous communication between FSRA and the Board

Complementary Guidance for Insurers

The Proposed **Operational Risk and Resilience Guidance** and **Corporate Governance Guidance** should be considered together

Operational Risk and Resilience Guidance

Principles for Effective Treatment* of Operational Risk and Achieving Resilience

1. Governance
2. Operational Risk Identification and Assessment
3. Operational Risk Management
4. Resilience

*Treatment of operational risk encompasses the identification, assessment, and management of operational risk. The management of operational risk may include mitigation, monitoring, and reporting of operational risk.

Corporate Governance Guidance

Practices for Effective Corporate Governance

1. Defined roles and responsibilities
2. Board independence and composition
3. Effectiveness of oversight structures
4. Integrity in reporting and disclosure
5. Corporate Culture
6. Effective subsidiary governance

Supporting FSRA's Statutory Objects

The two Proposed Guidance support FSRA's statutory objects, 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 protect the rights and interests of consumers
- to deter deceptive or fraudulent conduct, practices and activities by the regulated sectors
- to foster strong sustainable, competitive, and innovative financial services sectors

Relationship between Risk Management and Capital

- A key aspect that in both pieces of guidance is the linkage of risk management and the capital requirements set out in the 2023 Minimum Capital Test Guideline for Insurers (MCT Guideline).
- The MCT Guideline requires Insurers to prudently manage their capital to:
  - maintain financial strength
  - absorb losses to withstand adverse conditions (financial and non-financial)
  - meet other risk and business objectives
- To prudently manage capital, Insurers should have practices in place to identify, assess and manage their enterprise-wide risks, including **operational risk**. In addition, Insurers should implement appropriate **corporate governance** practices that include oversight of enterprise-wide risks.

Interrelation between Risk, Capital and Governance

- Risk-based capital adequacy
- Insurers' own internal capital target should be above supervisory target and MCT requirement

- Operational risk is a component of the MCT calculation
- Effective oversight and treatment of operational risk contributes to:
  - operational resilience
  - safety and soundness

Insurer's Senior Management and Board are critical to meeting intended outcomes with respect to effective risk management and governance

Proposed Corporate Governance Guidance

Proposed Corporate Governance Guidance – Background

Rationale

- Corporate governance is a foundational and critical factor through which the objectives of the Insurer are set and the means of attaining those objectives and monitoring performance.

- Insurers that demonstrate sound corporate governance practices are more likely to achieve and maintain long-term sustainable business performance.

Corporate Governance – Definition

Corporate Governance

- Corporate governance is a set of relationships between a company's management, its Board, and other stakeholders.
- The Board's overall role includes providing leadership, as well as approving and overseeing the implementation of the Insurer's strategic direction and overall business objectives, taking into account the need to protect members, policyholders, subscribers and other stakeholders.
- Boards are responsible for ensuring their organization has the necessary resources, policies, and practices in place to meet its objectives and effectively measure performance against them.

The Proposed Guidance sets out:

- Practices for effective corporate governance to achieve the outcomes
- The role of the Board in setting the tone from the top and achieving effective corporate governance
- The role of the Board under Principles Based Regulation (PBR)
- The important relationship between regulator and the Board

Overview of Proposed Corporate Governance Guidance

Interpretation

FSRA's **Interpretation** under the *Insurance Act* and Regulations for **Principles of Corporate Governance**

1. Defined Roles and Responsibilities
2. Board Independence and Composition
3. Effectiveness of Oversight structures
4. Integrity in Reporting and Disclosure
5. Corporate Culture
6. Effective Subsidiary Governance

Approach

Describes the **processes and practices** which FSRA will use to assess how effectively Insurers adhere to principles and **achieve outcomes**

- The delegation of roles and responsibilities is clearly understood and consistently applied
- Potential conflicts of interest or lack of independence are acknowledged and addressed
- Board effectively directs and challenges the Insurer's senior management and assumptions
- Board can articulate the linkages between strategic plans, financial and capital plans, and the Insurer's risk appetite statement
- Insurer's compensation program promotes desired behaviours and culture that is in the best interests of members, subscribers, policyholders, and the long-term viability of the Insurer
- Objective assessments of critical functions, including oversight functions and structures

Role of the Board

Intended Outcomes for an Insurer's Board include:

- The Board is able to **act independently** in the best interests of members and the Insurer itself
- The Board's collective skillset and experience are appropriately **aligned with business strategies and associated risks**
- Board responsibilities and those delegated to management support **effective oversight** of all material aspects of the Insurer
- Reporting supplied by senior management fosters **informed decision making** by the Board
- The Board has confidence that issues requiring their attention will be escalated to them by senior management

Role of the Board

Accountability

vs

Responsibility

Accountabilities are discharged by ensuring that something is done

Responsibilities are discharged by actually doing something

Role of the Board

- Complex market conditions and high-profile governance breakdowns have driven a common understanding of the broader accountabilities and responsibilities of Boards of Directors
- The Board delegates responsibility and authority to subcommittees and to the management team, but accountability cannot be delegated and remains with the Board
- There are certain elements for which the Board is both accountable and responsible
- Clearly defined roles and responsibilities and an effective culture will help directors achieve a level of comfort that the responsibilities they have delegated are being fulfilled

Role of the Board

The Proposed Guidance sets out corporate governance **principles** that the Board should adopt to effectively discharge its duties. Boards have a duty to act in the best interests of their members/subscribers/policyholders, and are, among other things, responsible for:

- Setting the **strategy** of the Insurer and establishing limits on the risks that can be taken in pursuit of that strategy
- **Directing management** to operationalize the strategy and risk appetite by establishing appropriate policies, processes, and systems and ensuring that staff have appropriate skillsets and experience
- **Fostering a culture** at the Insurer that promotes the flow of relevant information to decision makers at all levels
- Providing **oversight** and **challenge** by seeking assurances that the Insurer continues to be aligned with the principles it has set and approved

FSRA's Principles and Approach to Drive Outcomes

FSRA Financial Services Regulatory Authority of Ontario

Ontario

Principles for Effective Corporate Governance

Roles and Responsibilities	Independence and Composition	Effectiveness of Oversight Structures	Integrity in Reporting and Disclosure

ROLES AND RESPONSIBILITIES / INDEPENDENCE

OUTCOMES

- The Insurer establishes committees with clear mandates, tenure, duties, and terms of reference
- Directors provide oversight over the Insurer's business plan, strategy, and risk appetite/framework
- Separation of roles/responsibilities between Board and Senior Management
- Board oversees CEO performance

RISK GOVERNANCE AND OVERSIGHT

OUTCOMES

- Independence from management of the risks overseen
- Three lines of defence
- Adequate stature, expertise, and unfettered access to the Board
- Robust processes to monitor, identify, and report on the Insurer's risks and effectiveness

REPORTING AND DISCLOSURE

OUTCOMES

- Board has access to unfiltered information from the audit committee and other oversight functions
- Board determines the level of assurance it requires for the Insurer's financial and corporate reporting to be considered credible

WHEN ASSESSING BOARD EFFECTIVENESS, THE INSURER CONSIDERS OUTCOMES ABOVE

FSRA's Principles and Approach to Drive Outcomes cont.

Principles for Effective Corporate Governance

Culture and Behavioural Risk

RISK CULTURE

OUTCOMES

- Define a desired culture that supports the Insurer's purpose, strategy, effective oversight of risks and resilience
- Foster a culture that encourages openness and constructive challenge of judgments and underlying assumptions

Subsidiary Governance

SUBSIDIARY GOVERNANCE

OUTCOMES

- Maintain clear reporting lines to the parent Insurer
- Refrains from forming complex structures given the inherent risk of forming such structures
- Manages legal entity governance risk

WHEN ASSESSING BOARD EFFECTIVENESS, THE INSURER CONSIDERS OUTCOMES ABOVE

How Does an Insurer Achieve Independence?

- To effectively discharge its responsibilities, the Board must be **independent from senior management**. A director should be independent in conduct, character and judgment. This can be achieved by:

  - **Separating** the Board chair and CEO roles to ensure independent oversight
  - Ensuring the Board is comprised of directors who provide the appropriate **balance** and **mix** of skills, knowledge and experience to foster constructive debate and challenge senior management
  - **Adopting** processes which demonstrate integrity, such as regularly conducting in-camera sessions without the CEO and leveraging external expertise when appropriate
  - Developing and reviewing **conflicts of interest** policies**,** procedures and practices
  - Maintaining and updating **nomination**, **succession**, **onboarding** and training plans

Approach to Risk Management - three lines of defence

- Governance structures with well-defined accountabilities and responsibilities and decision-making authorities support effective governance, oversight, and risk management by the Board.
- Where an insurer lacks the risk management function or it does not have enterprise-wide responsibility, in applying proportionality, FSRA expects other functions to provide risk oversight.

FIRST LINE

Operational Management

OUTCOMES

- Operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks
- Executes risk and control processes on a day-to-day basis

SECOND LINE

Risk management

OUTCOMES

- Monitors and facilitates the implementation of effective risk management practices by operational management
- Assists risks owners in reporting adequate risk management across the Insurer

THIRD LINE

Internal Audit

OUTCOMES

- Provide independent assurance to the Insurer's Board and senior management
- Captures all elements of an Insurer's risk management framework and the interconnection to organizational objectives.

Example: Effectiveness of oversight structures

Intended outcome: The Board seeks independent assurances that risks are appropriately managed, and that the Insurer is in compliance with legal and regulatory requirements

Supervisory scenarios

- For Insurers that do not have independent and enterprise-wide second line functions, such as Risk Management or Compliance, FSRA may assess the Insurer's activities under Senior Management
- The Board through the Audit Committee is accountable and responsible for Internal Audit as it must be independent from Senior Management to provide objective assurances
- Insurers may outsource oversight responsibilities but not the ownership and accountability

Integrity of reporting and disclosure

The Board works to ensure that appropriate reporting processes are implemented to achieve quality and effectiveness in reporting

What is risk culture?

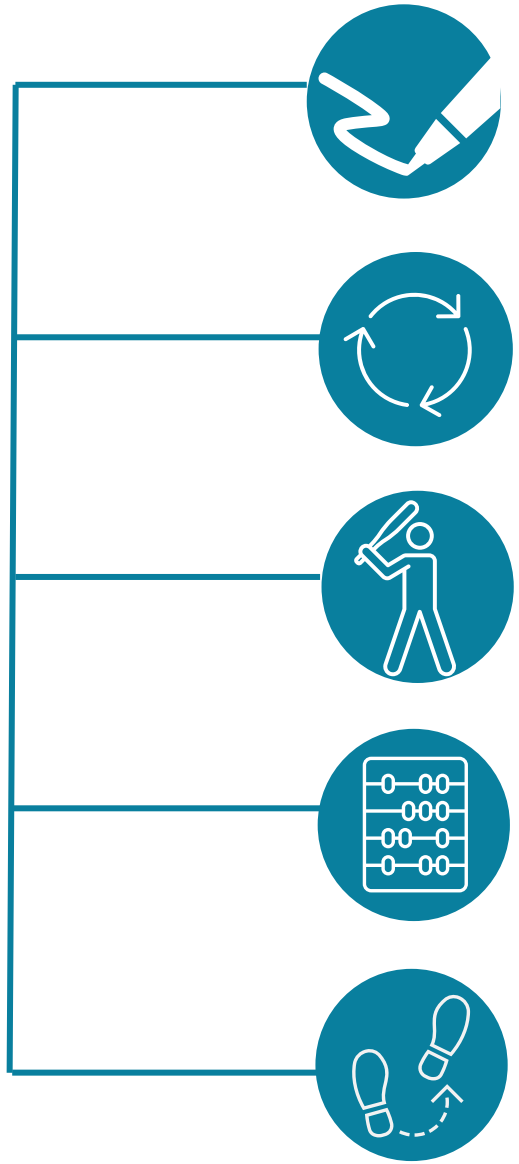
Culture in this context: An Insurer's articulation of its commonly held values and the behaviours expected of its employees and Directors

Culture as a driver of effective governance

- Culture can act as a reinforcing mechanism for an Insurer's information flows, aligning risk appetite and strategy, and driving meaningful conversations between management and the Board
- A sound risk culture can identify and remedy behaviour risks such as complacency, excessive risk-taking, poor communication or lack of speaking up
- When organizations do not adopt a sound risk culture, it can render well-designed frameworks, robust systems, and experienced people completely ineffective

Achieving desired behaviours and culture

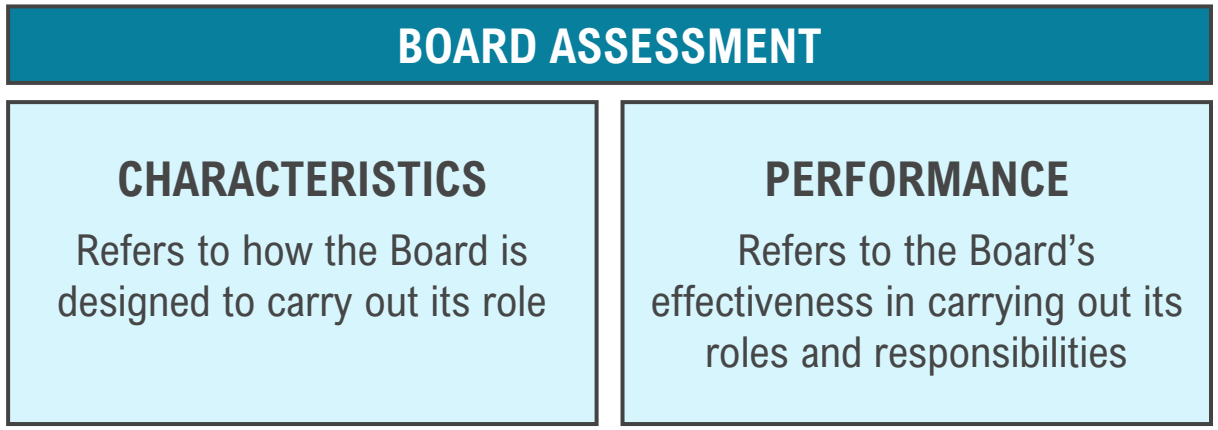
Tone from the top



- Articulate desired behaviours
- Reinforce desired behaviour with management and staff
- Seek assurances that supporting mechanisms are in place
- Ensure alignment with compensation, rewards and incentives
- Lead by example

Approach – FSRA's Assessment of Board Effectiveness

- FSRA currently applies, and will continue to apply under the Proposed Guidance, proportionality when assessing an Insurer's Board under the RBSF-I
- The performance assessment is more important than the characteristics assessment. Consequently, the performance assessment will carry more weight when determining the rating of the Board
- FSRA assesses the extent to which the Board meets the **intended outcomes set out in the Proposed Guidance**



The Board's level of engagement with FSRA is an indication of effectiveness and factors into FSRA's assessment of the Board

Relationship between Regulator and Board

As your regulator FSRA won't act unilaterally for those who are committed to achieving the identified outcomes. **This doesn't mean agreement on every point; it means a commitment to collaboration and finding effective solutions.**

When intended outcomes are aligned

- Ongoing work to build consensus and understanding
- Insurer-led enhancements where they are needed, with the Board as the agent of change
- Free flow of information drives a truly risk-based supervisory approach that is less intrusive and time and resource intensive

When collaboration breaks down

- A lack of good information may require FSRA to make conservative assumptions and act accordingly
- Prescriptive requirements reduce a regulated entity's autonomy
- Increased supervisory intensity resulting from higher risk

Questions

Proposed Operational Risk and Resilience Guidance

Proposed Operational Risk and Resilience Guidance – Background

Rationale

- Insurers are increasingly relying on technology, data, and the third-party ecosystem in their daily operations. As such, FSRA is placing a higher degree of importance on operational risk identification, assessment, and management, as well as operational resilience.

- The objective of the Operational Risk and Resilience Guidance is to enhance non-financial risk management and non-financial resilience by improving the Insurer's ability to monitor its current environment, ability to anticipate future threats and opportunities, ability to respond effectively to any stress event, and ability to learn from past failures and successes.

Operational Risk and Resilience – Definitions

Operational Risk

- 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

- Insurers' effective treatment of operational risk during business-as-usual (BAU) and under stress contributes to their safety and soundness, and operational resilience
- 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

Overview of Proposed Operational Risk and Resilience Guidance

Interpretation

FSRA's **Interpretation** under the *Insurance Act* and Regulations for **Principles for Effective Treatment of Operational Risk and Achieving Resilience**

1. Governance
2. Operational Risk Identification and Assessment
3. Operational Risk Management
4. Resilience

Approach

Describes the **processes and practices** which FSRA will use to assess how effectively Insurers adhere to principles and **achieve outcomes**

- IT (including cyber) risk management
- Third-party risk management
- Data management and governance
- Entering new business activities
- Assessment of an Insurer's Resilience

Information

Information on **Environmental, Social and Governance** (ESG) risk management

Examples of Operational Risk Events

An **operational risk event** (ORE) is an unintended outcome resulting from operational risk materialization. The below are some of the ORE categories that Insurers are exposed to:

Exposure to cyber risk, third-party risk, and data risk

Exposure to data risk and legal risk

Exposure to third-party risk and model risk

FSRA's Principles and Approach to drive Outcomes

FSRA Financial Services Regulatory Authority of Ontario

Ontario

Principles for Effective Treatment of Operational Risk and Achieving Resilience

Governance	Operational Risk Identification and Assessment	Operational Risk Management	Resilience

IT (INCL. CYBER) RISK MANAGEMENT OUTCOMES

- The Insurer is safeguarding and protecting IT assets to ensure confidentiality, integrity, and availability
- The Insurer is resilient in the event of technology service disruptions

THIRD-PARTY RISK MANAGEMENT OUTCOMES

- The Insurer retains accountability and ownership of all risks, including those introduced by engaging third parties
- The Insurer is resilient in the delivery of critical operations. Third-party risks are sufficiently mitigated to minimize disruptions and financial losses

DATA MANAGEMENT AND GOVERNANCE OUTCOMES

- The Insurer protects consumer privacy
- The Insurer ensures accuracy, completeness, consistency, timeliness, availability, confidentiality, traceability, non-repudiation, and fit-for-use of data for decision making and other purposes
- The Insurer minimizes harm and bias when leveraging advanced data analytics

WHEN CONDUCTING ITS ENTERPRISE-WIDE RISK ACTIVITIES, THE INSURER CONSIDERS OUTCOMES ABOVE

Example: Effective Governance of Operational Risk

Intended outcome: Ultimate accountability and responsibility of operational risk oversight resides with the Insurer's Board and Senior Management

Supervisory scenarios

- The Board periodically reviews and approves the Insurer's Operational Risk Management Framework (ORMF) and supporting frameworks
- Insurers establish a structure with adequate separation between functions or individuals that manage vs. oversee operational risk
- The Board effectively integrates ORMF into the Enterprise Risk Management (ERM) program and other enterprise-wide initiatives
- The Board ensures that there are adequate resources to carry out operational risk management activities

FSRA's RBSF Approach – Overview

- FSRA's integrated **Risk-Based Supervisory Framework** (RBSF-I) articulates the approach used to identify imprudent or unsafe business practices that may impact members, policyholders, and subscribers of Insurers
- FSRA exercises supervisory judgement and assesses the most important risks posed by Insurers to supervisory objectives and the extent to which Insurers can identify, assess, and manage these risks as well as achieve resilience

Operational Risk as an Inherent Risk category

Quality of Controls & Oversight in managing operational risk

Information Technology as a Significant Activity

FSRA RBSF RISK MATRIX | INSURERS

Significant Activities	Inherent Risks							Quality of Controls and Oversight							Residual Risk		
	Credit	Market	Insurance	Operational	Compliance	Strategic	Market Conduct	Operational Management	Actuarial	Compliance	Risk Management	Internal Audit	Senior Management	Board	MC	Prudential	Importance
								Enterprise-Wide Oversight Ratings							MCSRR	PSRR	
															SRR		

RBSF RATINGS

IR | RESIDUAL RISK | MCSRR | PSRR | SRR | ORR
Low • Low-Moderate • Moderate • Moderate-High • High

QCO | CAPITAL (INCL. EARNINGS) | LIQUIDITY | RESILIENCE
Strong • Adequate • Needs Improvement • Inadequate • Weak

IMPORTANCE
Low • Medium • High

INTERVENTION LEVEL
1 • 2 • 3 • 4 • 5

Resilience under BAU and stress conditions

Capital (incl. Earnings)	
Liquidity	
Resilience	

Overall Risk Rating	ORR
Intervention Level	IL

Resilience Assessment

FSRA assesses an Insurer's resilience from a characteristic and performance perspective

CHARACTERISTICS
demonstrated during **business-as-usual**

Crisis preparedness through improving ability to **monitor** and **anticipate** any escalation of risks

EXAMPLES

- Robustness of Insurer's operational risk management
- Extent of Board review of risk reports and frameworks
- Extent and quality of communication between the Board and Senior Management on improving contingency, continuity, and recovery plans

PERFORMANCE
demonstrated during **stress**

Respond and adapt to stress/incident, take feasible and timely action, leverage pre-determined processes to facilitate streamlined and effective recovery

Learn from past failures and successes

EXAMPLES

- Effectiveness of actions taken by Senior Management and the Board upon activation of contingency, continuity, and recovery plans when in stress
- Extent of continuous improvements

Information – ESG

- Insurers have already started working towards developing and meeting ESG objectives. FSRA encourages Insurers to continue progress towards further incorporation of ESG goals into their corporate strategies and business activities

- ESG and Sustainable Development Goals (SDG) goals can be addressed in parallel

- Other jurisdictions and standard-setting bodies have released guidance/standards relating to ESG risk management; in particular, addressing the following areas:

Environmental	Social	Governance
Climate-related physical and transition risks requiring frameworks, policies, disclosures, metrics, targets, as well as establishment of a complete understating of the external environment	**Social risks** requiring a focus on human and labour rights, diversity, community, and customers	**Governance risk** requiring appropriate mitigation frameworks

Recent development on ESG initiatives

ESG disclosures and natural catastrophe risk has been an increasing area of importance for:

International Sustainability Standards Board (ISSB)/ International Financial Reporting Standards (IFRS)

Financial Stability Board (FSB)

International Association of Insurance Supervisors (IAIS)

Summary

Summary and Next Steps

- Insurers are increasingly relying on technology, data, and the third-party ecosystem in their daily operations. Operational risk represents a significant and growing threat to Insurers' businesses and operations. As such, FSRA is placing a higher degree of importance on operational and operational risk identification, assessment, and management, as well as operational resilience

- Strong corporate governance is crucial to ensure that Insurers are managed in a safe and sound manner and are able to appropriately adapt and respond to the emerging risks affecting their operations

- FSRA looks forward to working with Insurers in achieving effective corporate governance, including enhancing operational risk management practices, through RBSF-I Assessments and ongoing dialogue

- The consultation on FSRA's website for both the Proposed Operational Risk and Resilience and the Corporate Governance Guidance closes **June 17, 2024**.

- FSRA will consider feedback in revising the Guidance, as appropriate.

Questions