FSRA
Financial Services Regulatory Authority of Ontario

Guidance

☒ Interpretation ☒ Approach ☒ Information ☐ Decision

Effective Date: March 1, 2024
Identifier: No. CU0088APP

Operational Risk and Resilience

Purpose

The Financial Services Regulatory Authority's (FSRA's) Operational Risk and Resilience Guidance (the "Guidance")[1] provides:

i. FSRA's Interpretation of the operational risk and resilience requirements for Ontario Credit Unions and Caisses Populaires (CUs) under the *Credit Unions and Caisses Populaires Act, 2020* (the "*Act*") and Rule 2021 – 001 Sound Business and Financial Practices (the "*SBFP Rule*")

ii. FSRA's Approach for assessing how CUs effectively adhere to the principles and achieve the outcomes identified in the Interpretation section of 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 CUs

The Guidance aims to enhance operational risk identification, assessment, and management, and non-financial resilience[2] by improving CUs' ability to monitor their current environment,

anticipate future threats and opportunities, respond effectively to stress events, and learn from past failures and successes.

The Interpretation section of this Guidance sets out FSRA's interpretation of applicable requirements under the *Act* and the *SBFP Rule* to identify where non-compliance may lead to supervisory or enforcement action. This may include requiring remediation and reporting by CUs, and/or issuing orders, and in some cases, placing CUs under supervision or administration in accordance with the provisions of the *Act*.[3]

The Approach section of this Guidance sets out FSRA's processes and practices for assessing CUs' operational risk and resilience in accordance with the Risk Based Supervisory Framework (RBSF) and may have implications for CUs' Overall Risk Rating (ORR). The impact on the ORR is two-fold: (1) operational risk identification, assessment, and management will be considered when assessing the inherent risk and quality of controls and oversight as part of the determination of the Prudential Summary Residual Risk (PSRR); and (2) resilience of CUs will be assessed and reflected in the resilience rating, which will be used to modify the Summary Residual Risk Rating (SRR) in order to determine the ORR.

The Information section of this Guidance acknowledges that some CUs have begun considering ESG 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 CUs.

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 CUs.

Scope

This Guidance affects the following entities regulated by FSRA:

- Credit Unions and Caisses Populaires incorporated under the *Act*

This Guidance complements, and must be read in conjunction with, other FSRA guidance and supporting publications on FSRA's website on the "Guidance – Credit Unions and Caisses Populaires" and "Rules" webpages.

Rationale and background

CUs 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.

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: CUs' effective treatment [4] of operational risk during business-as-usual (BAU) and under stress contributes to CUs' safety and soundness, and operational resilience. CUs 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 CUs 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), 3(2) and 3(4) of the *Financial Services Regulatory Authority of Ontario Act*, 2016 (the "*FSRA Act*"), 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
- to promote and otherwise contribute to the stability of the CU sector in Ontario with due regard to the need to allow CUs to compete effectively while taking reasonable risks

- to pursue the objects for the benefit of persons having deposits with CUs and in such manner as will minimize the exposure of the Deposit Insurance Reserve Fund (the DIRF) to loss

Interpretation

This section sets out FSRA's view of the requirements for CUs effective operational risk identification, assessment, and management, as well as operational resilience set out under:

- Particular provisions contained in ss. 4, 5, 6, 10, 11, 12, and 15 of the *SBFP Rule*, which outline principles-based and outcomes-focused requirements, with respect to:
    - board composition and responsibilities
    - the responsibilities of senior management
    - the status, authority and independence of CUs oversight functions
    - CUs' internal audit function
    - CUs' risk management function
    - CUs' operational management
- Section 109(1) of the *Act*, which articulates requirements on how the powers and duties of directors, officers, and committee members of CUs must be exercised and discharged

Adherence to the principles set out below is in the best interest of CUs and their members and helps to demonstrate how effectively CUs are complying with the provisions in the *SBFP Rule* and the *Act* noted above. The principles describe FSRA's expected outcomes, which must be achieved by Ontario CUs to demonstrate effective operational risk identification, assessment, and management as well as resilience upon materialization of operational risk events. FSRA will monitor adherence to these principles as part of its supervisory approach, outlined in the Approach section of this Guidance.

Principles

Principle 1: Governance

Ultimate accountability and responsibility of operational risk oversight rests with CUs' Board[5] and Senior Management.[6]

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

The Board, composed of directors who have the appropriate skills and expertise[7], is responsible for establishing the necessary strategies and governance structures, overseeing and approving CUs' operational risk management program, as well as ensuring that there are adequate resources[8] to carry out their operational risk management activities[9] and protect members' deposits. The Board is required to periodically review and approve CUs' 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 CU's size, complexity, and risk profile, which will include the CU's operational risk appetite, tolerance, and limits[10]. The Board is also required to review the business continuity plan (BCP)[11] and disaster recovery plan (DRP).[12] The Board must clearly articulate the nature, types, and levels of operational risk that CUs are willing to assume.[13]

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[14] based on the level of their involvement in managing the risks. Senior Management establishes and governs the respective roles and responsibilities necessary to effectively identify, assess, manage, and oversee operational risk.[15] As the Board is responsible for overseeing and approving risk management, CUs' operational risk profile in relation to the Board-approved risk appetite and tolerance needs to be measured by Senior Management and presented to the Board to confirm alignment.[16]

Governance structures with well-defined accountabilities and responsibilities, reporting lines, and decision-making authorities support the management of operational risk and CUs' resilience. CUs must establish an organizational structure where operational risk management activities are

conducted by Operational Management[17] (first line of defence), are reviewed and challenged by Risk Management[18] (second line of defence), and independent assurance is then provided by Internal Audit[19] (third line of defence), facilitating effective governance, oversight and risk management.[20]

Principle 2: Operational Risk Identification and Assessment

Comprehensively identifying, assessing, and understanding the operational risk inherent in all of a CU's products, activities, people, processes, and systems, as well as in its external environment, enables the development and implementation of corresponding risk response strategies.[21]

Regularly performing environmental scans of CUs' operations supports CUs' 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 may include information technology used to support CUs' 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 a CU's businesses, reduces the probability of disruption, and minimizes the risk of loss to depositors.[22]

A robust operational risk management program reduces the frequency of risk materialization and the impact of operational risk events on the CU's members and other stakeholders. CUs' approach to managing operational risk must be carefully considered, adequately documented[23] and periodically updated to reflect changes in CUs' operating environment, risk appetite and tolerance, and/or advancements in risk management capabilities.[24]

Commensurate with CUs' size, complexity, and risk profile, CUs must develop and implement frameworks and supporting policies and procedures to facilitate reasonable treatment, including identification, assessment, mitigation, monitoring, and reporting of their operational risks exposures.[25] The ORMF and any supporting frameworks or similar construct must be aligned and integrated with their enterprise-wide risk management program.[26]

Principle 4: Resilience

The Board[27] and Senior Management[28] plan for adverse scenarios and ensure that CUs are crisis ready. CUs achieve resilience during BAU through enhancing crisis preparedness and improving their ability to monitor and anticipate any escalation of risks.[29] Upon operational risk materialization, CUs respond and adapt by taking feasible and timely actions, leveraging pre-determined processes and protocols, to facilitate streamlined and effective recovery.[30] CUs also review and re- evaluate processes and protocols in light of past failures and successes, aiming for continuous improvements to resiliency.[31]

Operational Resilience is an outcome that benefits from CUs' effective treatment of operational risk during BAU or under stress and contributes to CUs' safety and soundness. Achieving operational resilience may require CUs' to adopt a new perspective, develop awareness, and implement effective strategies when moving 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 improves CUs' ability to achieve this outcome. Operationally resilient CUs are able to deliver critical operations through disruption and are less prone to experiencing operational risk events. In the event that operational risk materializes, resilient CUs 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 the processes and practices which FSRA will use to assess CUs' adherence to the provisions of the *SBFP Rule* and *Act* which are noted above, as informed by the principles identified in the Interpretation section of this Guidance. Refer to FSRA's Risk Based Supervisory Framework Guidance (No. CU0083APP) for details on the Risk Assessment Process.

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

FSRA's assessment of CUs' operational risk as an Inherent Risk category

When assessing CUs' compliance with the *SBFP Rule* as interpreted by **Principle 2: Operational Risk Identification and Assessment** in the Interpretation section of this Guidance, FSRA will assess operational risk as an Inherent Risk category intrinsic to CUs' Significant Activities[32] (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 CUs' capital and earnings.

Operational risk could originate from CUs' products, activities, people, processes, systems, and external environment. Among other things, FSRA will consider the complexity of CUs' products and services, delivery channels, and level of automation when assessing the level of operational risk at CUs.

Operational risk is broad and includes various sub-risks such as, but not limited to, third-party risk, cyber risk, and data risk:

- Third-party risk arises when CUs engage a third party for the provision of a product or service and the third party fails to deliver the product/service in accordance with the contractual agreement.

- Cyber risk is the risk of financial loss, operational disruption or damage from the unauthorized access, use, disclosure, disruption, modification, or destruction of CUs' 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 CUs' day-to-day operations, internal risk reporting, and decision-making. Data risk often intersects other risk areas such as cyber risk, third-party risk, and advanced analytics. Data risk materialization can occur when

CUs have inadequate processes and cyber security controls to safeguard confidential consumer data from a potential privacy breach.

The following are some examples, but not an exhaustive list, of potential operational risk events (OREs) to illustrate how operational risks may materialize and associated outcomes. These events could result in actual losses or near misses and may fall under multiple operational risk types (as illustrated in brackets).

- **Example #1:** A cyber attack has compromised a CU's core banking system and also resulted in a data breach at the data warehouse hosted by a third-party vendor. Data has been corrupted. The system was shut down by the third-party vendor for investigation in order to clean and restore the data, causing major operational disruptions for the CU. (An ORE illustrating cyber risk, third-party risk, and data risk)

- **Example #2:** A CU fails to adequately identify, capture, and record details for different deposit account types, in part due to its outdated banking system. There are instances where beneficiary information on some trustee accounts were missing. Members were dissatisfied after uncovering many issues and decided to withdraw their deposits. (An ORE illustrating information technology risk and data risk)

- **Example #3:** A CU has erroneously transferred confidential member information in an Application Programing Interface (API) call to a financial technology company (FinTech) without first securing the member's consent. The privacy breach resulted in legal liability and reputational damage for the CU. (An ORE illustrating data risk and legal risk)

- **Example #4:** A CU relies on a third-party consultant without understanding the underlying model assumptions. As a result, poor risk management decisions were made by the CU, which ultimately led to financial losses. (An ORE illustrating third-party risk and model risk)

- **Example #5:** A CU does not incorporate emerging climate-related risks into its business strategies, corporate governance and internal control frameworks, resulting in future financial and reputational losses. (An ORE illustrating environmental under ESG risk)

FSRA's consideration of CUs' information technology as a Significant Activity at the CU

The use of information technology has been a key enabler to effective delivery of CUs' 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 CU) or could be misused (due to, for example, misaligned fit for purpose, unauthorized access), which may contribute to operational risks at CUs.

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

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

FSRA will assess the extent to which the level of controls and oversight at CUs is adequate in order to mitigate their inherent risks. FSRA's assessment will evaluate the extent to which CUs' practices are compliant with legislative and regulatory requirements (e.g., those set out in the *SBFP Rule* and the *Act*) and FSRA's interpretation of such requirements (in particular those 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 CUs' Significant Activities, FSRA will consider both QCO characteristics and performance in the context of the CUs' size, complexity, and risk profile.

When assessing CUs' operational risk management, FSRA will evaluate the extent to which CUs' 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 CUs' operational risk management tools (e.g., operational risk taxonomy, risk and control assessments,loss data collection) to identify, assess, and manage their operational risks. FSRA will also evaluate CUs' Oversight Functions (i.e., Compliance, Risk Management, Internal Audit, Senior Management, and Board of Directors) in order to assess the extent to which they provide

effective independent enterprise-wide oversight to Operational Management and whether CUs' operations and risk exposures are consistent with their operational risk appetite and tolerance. As part of this assessment, FSRA will also consider how effectively CUs are adhering to **Principle 1: Governance in the Interpretation section of this Guidance**. For smaller CUs, independence may be achieved through separation of functional duties between individuals and independent review of processes and functions.

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

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

FSRA will assess CUs' 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's IT Risk Management Guidance**. FSRA will also consider the extent to which CUs have adopted risk management practices informed by industry frameworks and standards. FSRA will evaluate the extent to which CUs' 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 CUs' 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 CUs' risk appetite. It is important that CUs 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 CUs safeguards the confidentiality, integrity, and availability of CUs' own information technology assets and understand 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 CUs' IT security controls are adequate to protect, detect, respond, recover, and learn from IT incidents. For situations where CUs are outsourcing these activities, FSRA will assess CUs' review and understanding of the controls put in place by their third-party providers to manage these risks. In addition, it is important for CUs to enhance their resilience characteristics and performance in preparation for, and in the event of, technology service disruptions.

FSRA will evaluate the extent to which CUs periodically review and updates their BCP/DRP to reflect their current operations, risks, and threats, as well as regularly test these plans against severe but plausible scenarios that could impact CUs' critical business operations to ensure plans remain effective. FSRA will consider the extent to which CUs' BCP/DRP articulate roles and responsibilities, define thresholds/ triggers for plan activation, incorporate quantitative/ qualitative impact assessments or business impact analysis, establish recovery objectives, and include incident response and communication plans (**Principle 4: Resilience**).

FSRA's approach in assessing CUs' third-party risk management

CUs 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 CUs to additional risks. Irrespective of the arrangement, CUs retain accountability and ownership of all risks including those introduced by

engaging third parties. As such, establishing a third-party risk management framework or similar construct and ensuring the dedication of adequate resources with the necessary skills/expertise to implement the framework 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 CUs' 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 CUs 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 CUs 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 CUs are continuously monitoring and reporting on their 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 CUs' risk appetite (**Principle 2: Operational Risk Identification and Assessment** and **Principle 3: Operational Risk Management**).

As it relates to CUs' BCP/DRP, FSRA will also look for evidence that CUs have considered concentration risk as well as the interconnections between, and interdependencies of, their third-party providers. FSRA will assess the appropriateness of CUs' 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 CUs' data management and governance

FSRA will evaluate the extent to which CUs' data governance is supported through clear accountabilities and reporting structures. FSRA will assess CUs' 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 evaluate CUs' approach to managing and safeguarding their data and the extent to which they have implemented processes and controls to manage their data risk throughout the data lifecycle (from data creation/collection to deletion) and protect consumer privacy. In addition, FSRA will look for evidence that CUs' data architecture and IT infrastructure adequately support their risk data aggregation[33] and risk reporting capabilities, as well as evidence of appropriate data identification, classification, ownership, and authorization of use. Robust processes and procedures with adequate staff training to create awareness can contribute to ensuring accuracy, completeness, consistency, timeliness, availability, confidentiality, traceability, non-repudiation, and fit-for-use of data. For CUs leveraging advanced analytics (i.e., more complex data analysis techniques such as artificial intelligence) to gain deeper insights, improve forecasting, and drive decision-making, FSRA will assess the extent to which appropriate mechanisms are in place to ensure robust data governance and mitigate the risks of harm and bias in their models.

FSRA will assess whether CUs have sufficient data capabilities to support informed decision-making, not only in BAU but also in stress conditions (e.g., generate off cycle and more granular reports related to assets and deposits, produce ad hoc reporting) (**Principle 4: Resilience**).

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

When a CU is entering into any new business activity, either itself or through a subsidiary, which involves technological innovation and new uses, or sharing of customer data or information (e.g., participating in open banking, setting up an insurance brokerage subsidiary), FSRA will assess the extent to which CUs have 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 CUs have:

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

- demonstrated reasonable care in handling consumer financial data with sufficient security measures, including the way confidential and sensitive data is safeguarded and consumers are appropriately compensated for, and protected from, future loss

- considered possible liability, privacy, and security issues when handling consumer data
- ensured that data provided by a consumer for one purpose is not used for another purpose unless informed consent is obtained

FSRA's resilience assessment of CUs

FSRA will assess CUs' resilience against their adherence to **Principle 4: Resilience** in the Interpretation section of this Guidance, which interprets requirements set out in the *SBFP Rule*.

Overall resilience of CUs is assessed holistically through financial and non-financial factors and considers BAU and post-stress event conditions. Financial resilience factors include capital and liquidity. 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 performance and characteristics are the strength of a CU's Internal Capital Adequacy Assessment Process; adequacy and implementation of Recovery Plan, Contingency Funding Plan, Business Continuity Plan and Disaster Recovery Plan during stress.

In assessing CUs' resilience, FSRA will consider the manner in which CUs operate both in a BAU environment and when they are forced into a stress (non-BAU) environment. FSRA will consider CUs' 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 CUs enhance their crisis preparedness through improving their ability to **monitor** and **anticipate** any escalation of risks. Resilience performance of CUs is demonstrated based upon their 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 CUs learn 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 CUs' 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[34]
- Operational risk management, especially the management of IT, third-party, and data risks
- Environmental, social and governance considerations (see Information Guidance below)

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

- the Board has periodically reviewed reporting of actual CU metrics, as measured against the management/board triggers, describing CUs' holistic state of financial health
- there is evidence of periodic communication between the Board and Senior Management
- the quality of CUs' business contingency plans are adequate, given their size, complexity, and risk profile

FSRA will look for evidence of CUs' 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 CUs' recovery plan or contingency plans, upon activation of these plans, and the effectiveness of such actions
- there have been continuous improvements to CUs' practices based on lessons learned

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

Information

Over the last decade there have been significant developments and rising awareness of ESG issues across industries in global economies. The Sustainable Development Goals (SDG) were introduced by the United Nations as an important part of its 2030 Agenda for Sustainable Development. Increasing evidence from studies has also emerged on the growing threat of

climate change and the impact that it could have on the safety and soundness of financial institutions, including CUs.

Some CUs have already started working towards developing and meeting ESG objectives. FSRA recognizes these efforts and encourages CUs to continue progress towards further incorporation of ESG goals in their corporate strategies and business activities. It is important for CUs to proactively work towards supporting Canada's ESG and SDG goals, which can be addressed in parallel.

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 human and social rights, and governance practices that are aligned with the *SBFP Rule*. In the meantime, CUs are encouraged to develop and implement plans to include ESG considerations in their corporate strategies and business activities to ensure positive contributions towards ESG goals.

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

- climate-related physical and transition risks requiring frameworks, policies, disclosures, metrics, targets, as well as establishment of a complete understating 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 CUs' ESG (especially climate risk) initiatives under the RBSF as part of their Resilience Rating. FSRA may issue observations to CUs through their supervisory process, but any observations on ESG will not punitively contribute to CUs' ORR rating until future guidance is issued.

Effective date and future review

This Guidance will be effective as of March 1, 2024 and will be reviewed on or before March 1, 2029.

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 or 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: March 1, 2024

---

[1] This Guidance is being published as combined Interpretation, Approach, and Information Guidance under FSRA's Guidance Framework. Each component is labelled for clarity.

[2] Overall resilience of CUs is assessed holistically through financial and non-financial factors and considers "business as usual" and "post-stress event" conditions. Financial resilience factors include capital (including earnings) and liquidity; non-financial factors are generally governance and operational-based and focus on crisis preparedness. For the purpose of this Guidance, resilience is in reference to non-financial resilience.

[3] Credit Union and Caisses Populaires Act, 2020, S.O. 2020, C. 36, Sched 7, ss. 230 and 233 [CUCPA 2020].

[4] For the purpose of this Guidance, the treatment of operational risk encompasses the identification, assessment, and management of operational risk (as outlined in Principle 2 and Principle 3 in the Interpretation Section). The management of operational risk may include mitigation, monitoring, and reporting of operational risk (as described in Principle 3 in the Interpretation Section).

[5] Rule 2021-001 Sound Business and Financial Practices, s. 5(3)(i)(g) [*SBFP RULE*].

[6] Ibid at s. 6(2)(ii), s. 6(2)(iii).

[7] Ibid at s. 4(1).

[8] Ibid at s. 5(4)(ii).

[9] Ibid at s. 5(3)(i)(g).

[10] Ibid.

[11] O. Reg. 105/22, clause (18) of s. 36(1).

[12] Ibid.

[13] *SBFP RULE*, s. 5(3)(i)(g).

[14] Ibid at s. 6(1)(i)(b), s. 6(2)(iii).

[15] Ibid at s. 6(1)(i)(b)

[16] Ibid at s. 5(3)(i)(g).

[17] Ibid at s. 15(2)(iv), s. 15(2)(v).

[18] Ibid at s. 10(9)(i)(a)-(b), s. 10(11) and s. 12(1)(i).

[19] Ibid at s. 11(2).

[20] In accordance with s. 10(1) of the *SBFP Rule*, a CU must establish and maintain oversight functions such that these functions have sufficient resources, status, authority, and independence to perform their roles and responsibilities, proportionate to the CU's size, complexity, and risk profile.

[21] Ibid at s. 5(3)(i)(g), s. 6(1)(i)(b), s. 6(2)(ii), s. 6(2)(iii), s. 11(2), s. 12(1)(i), s. 12(1)(i), s. 15(2)(iv) and s. 15(2)(v).

[22] Ibid at s. 12(1)(i).

[23] Ibid at s. 12(1)(ii).

[24] Ibid at s. 12(1)(i).

[25] Ibid at s. 12(1)(i), s. 12(1)(ii).

[26] Ibid at s. 12(1)(i).

[27] Ibid at s. 5(3)(i)(g).

[28] Ibid at s. 6(2)(ii) and(iii).

[29] Ibid at s. 12(1)(i).

[30] Ibid at s. 12(1)(ii).

[31] Ibid.

[32] As defined in FSRA's Risk Based Supervisory Framework (No. CU0083APP).

[33] Risk data aggregation is defining, gathering, and processing risk data according to CUs' risk reporting requirements to enable CUs to measure their performance against their risk appetite and tolerance.

[34] Refer to Recovery Planning Guidance (CU0069INT).