Draft guideline

Title	Operational Resilience and Operational Risk Management - Draft guideline (2023)
Category	Sound Business and Financial Practices
Date	October 31, 2023
Sector	Banks Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies
Number	E-21

Table of Contents

Consultation status: Closed

Consultation closed February 5, 2024. We'll keep this draft on the site until the final guideline is released.

A. Overview

Federally regulated financial institutions (FRFIs) operate in a complex risk environment, with increasing threats posed to their critical operations from events such as control failures, third-party disruptions, infrastructure outages, technology failures, cyber incidents, geopolitical incidents, pandemics, and natural disasters. A robust and concerted approach to operational resilience can enhance the ability of the FRFI to withstand, adapt to, and recover from such events while continuing to deliver its critical operations.

FRFIs can achieve operational resilience by:

- identifying the FRFI's critical operations and mapping the internal and external dependencies (e.g., people, systems, processes, third parties, facilities, etc.) required to support critical operations;
- establishing tolerances for disruption in respect of a FRFI's critical operations;
- conducting scenario testing to gauge the ability of the FRFI to operate within its tolerances for disruption across a range of severe but plausible scenarios; and
- establishing a culture that promotes and reinforces behaviours that support operational resilience and proactively managing culture and behaviour risks that may influence resiliency.

A1. Relationship between operational risk management and operational resilience

Effective operational risk management involves the identification, assessment, monitoring and reporting of operational risks, and implementing appropriate risk responses. Operational resilience is built on a foundation of effective operational risk management, which should include such areas as technology and cyber risk management, third-party risk management and business continuity management and, as appropriate, leverage existing risk and governance frameworks.

Operational resilience emphasizes the end-to-end performance of the FRFI's critical operations across the organization. As the FRFI's operational resilience approach matures, the operational risk management underpinning it should transition from a business-unit approach to one that focuses on the performance of operations end-to-end.

Operationally resilient organizations understand that disruptions can and will occur. They respond, adapt to, recover, and learn from such disruptive events.

A2. Purpose and scope

This Guideline sets out OSFI's expectations for operational resilience and managing operational risks. It is applicable to all FRFIs, including foreign bank branches and foreign insurance company branches to the extent it is relevant to their ability to meet applicable requirements and legal obligations.[1] OSFI's expectations for branches are set out in Guideline E-4 on Foreign Entities Operating in Canada on a Branch Basis.

A3. Application and proportionality

OSFI's expectations for operational resilience and managing operational risks are principles-based and intended to be applied on a proportionate basis, for example, relative to a FRFI's interconnectedness to the financial system.

Larger and more complex FRFIs, including but not limited to those that OSFI has designated as systemically important, often carry out operations that, if disrupted, could cause harm to other financial institutions, the financial system, or the broader economy.

Smaller and monoline FRFIs typically have fewer services, products, or functions whose disruption would put the continued operation of the FRFI at risk. However, some small institutions offer unique products or carry out services or functions the unavailability of which could pose harm to other financial institutions, the financial system, or the broader economy.

In all cases, the design and implementation of the FRFI's operational resilience approach and operational risk management should be proportionate to the FRFI's size, nature, scope, complexity of operations, strategy, risk profile, and interconnectedness to the financial system.

A4. Definitions

"Operational resilience" is the ability of an institution to deliver operations, including critical operations through disruption. It is a prudential outcome of effective operational risk management. Operational resilience emphasizes preparation, responsiveness, recovery, learning and adaptation by recognizing that disruptions, including

simultaneous disruptions, will occur. Among other things, it includes resilience to technology and cyber risks.

"Operational risk" is the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events. It includes legal risk but excludes strategic and reputational risk. The management of operational risk encompasses the policies and procedures established to prevent loss resulting from people and events, including external or internal fraud, non-adherence to internal procedures/values/objectives, or unethical behaviour.

"Operational risk event" is an unintended outcome resulting from operational risk, including actual and potential operational losses and gains, as well as near misses (i.e., where the FRFI did not experience an explicit loss or gain resulting from an operational risk event).

"Critical Operations" are the services, products, or functions of a FRFI which, if disrupted, could put at risk the continued operation of the FRFI, its safety and soundness, or its role in the financial system.

"Data risk" refers to the potential harm or negative impact that can result from the collection, storage, processing, use, sharing, or disposal of data. Data risk encompasses the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events impacting data.

"Tolerance for disruption" is the limit of disruption from any type of operational risk that a FRFI is willing to accept given a range of severe but plausible scenarios (e.g., outage time, diminishment of service, loss of data, extent of customer impact, etc.). Tolerances should be established for each critical operation, taking into account the compounding impact of related services, products or functions being disrupted simultaneously.

"Scenario testing" uses a hypothetical state of the world to define changes in risk factors affecting the FRFI's operations. This will normally involve changes in a number of risk factors, as well as ripple effects that are other impacts that follow logically from these changes and related management and regulatory actions. Scenario testing is typically conducted over the time horizon appropriate for the business and risks being tested. As it pertains to operational resilience, scenario testing would assess the effectiveness of the FRFI's ability to operate within tolerances for disruption in a range of severe but plausible scenarios.

A5. Outcomes

This Guideline presents four outcomes FRFIs are expected to achieve related to operational resilience and managing operational risks.

1. The FRFI can deliver critical operations through disruption.
2. Operational risk management is integrated within the FRFI's enterprise-wide risk management program and supports operational resilience.
3. Operational risks are managed within the FRFI's risk appetite.
4. Operational resilience is underpinned by operational risk management subject areas, including business continuity management, disaster recovery, crisis management, change management, technology and cyber risk management, third-party risk management, and data risk management.

A6. Related guidance

This Guideline should be read in conjunction with applicable legislation and relevant OSFI guidance, including but not limited to the Corporate Governance Guideline, Guideline B-10 on Third-Party Risk Management, Guideline B-13 on Technology and Cyber Risk Management, Guideline E-13 on Regulatory Compliance Management, Guideline E-18 on Stress Testing, and Guideline E-4 on Entities Operating in Canada on a Branch Basis.

1. Governance

Principle 1: The operational resilience approach and operational risk management framework are implemented, governed, and reported through the appropriate structures, strategies, and frameworks.

1.1 Senior management is responsible for operational resilience and managing operational risks

Senior management is responsible for developing, implementing, and sustaining the FRFI's operational resilience approach and for its operational risk management framework, and for ensuring the allocation of adequate financial, technical and organization resources for these purposes. There should be clear ownership and accountabilities for operational resilience and management of operational risk across the business and central functions, risk and compliance oversight, and internal audit. Senior management should ensure significant deficiencies are addressed rapidly and appropriately and provide timely reports to the board of directors. Senior management should promote and reinforce behaviours supporting operational resilience and proactively manage culture and behaviour risks influencing resiliency, as an institution's culture can impact its ability to withstand and mitigate operational disruptions.

Please refer to OSFI's Corporate Governance Guideline for expectations of FRFI boards of directors regarding the business plan, strategy, risk appetite, culture, and the oversight of senior management and internal controls.

1.2 Operational resilience and management of operational risks are integrated into the FRFI's enterprise risk management program and reporting

OSFI expects the FRFI's operational resilience approach to be fully integrated with its enterprise risk management program, which includes operational risk, technology and cyber risk, third-party risk, and data risk, as well as business continuity management, disaster recovery, crisis management, and change management.

As part of enterprise risk management, appropriate, accurate and timely reporting on the current status and outlook of the FRFI's operational risk profile and its operational resilience approach should be provided to senior management. Effective escalation mechanisms should also be in place to report operational events and significant deficiencies with the potential to impact the FRFI's delivery of critical operations.

1.3 Business lines and central functions manage risk and are subject to independent oversight

The FRFI's business and central functions should be responsible for managing their operational risks and contributing to the FRFI's operational resilience approach. In turn, the FRFI should subject the judgement and risk management practices of the business and central functions to a documented process of independent and effective challenge by the risk and compliance oversight function. While the size and structure of the risk and compliance oversight function may vary according to the FRFI's nature, size, complexity, and risk profile, it should in all cases be able to challenge the risk management practices and decisions of the business lines and central functions without fear of reprisal.

1.3.1 Business and central functions are responsible for managing operational resilience and risks in their day-to-day activities

As the owners of operational resilience and the management of day-to-day operational risks, OSFI expects the business and central functions to:

- identify and assess operational risks inherent in all aspects of their business;
- escalate operational risk events in accordance with established escalation channels;
- establish appropriate mitigating controls and test the design and effectiveness of such controls;
- identify and mitigate risks to critical operations within established tolerances for disruption;
- manage operational risk in line with the FRFI's risk appetite framework and operational resilience approach;
- adhere to the FRFI's operational resilience approach, risk management framework, and related policies; and
- provide adequate and periodic training to staff on the management of operational resilience and risk.

1.3.2 Independent risk and compliance oversight of operational resilience and managing operational risks

To foster robust operational resilience and effective operational risk management throughout the FRFI, independent risk and compliance oversight should:

- establish and oversee adherence to, review, and continuous improvement of the FRFI's operational resilience approach and operational risk management policies and procedures, processes, and tools;
- establish effective reporting tools;
- confirm that appropriate escalation channels are established, monitoring of operational resilience and risk are adequately documented, and significant issues are escalated in a timely and accurate manner; and
- promote integration of operational risk management into the overall enterprise-wide risk management of the FRFI.

1.3.3 Independent assurance is provided

Internal audit or a similar function should provide independent assurance to senior management and the board of directors that the FRFI's operational resilience approach and operational risk management controls, processes, and systems, across the enterprise, function as intended.

2. Operational Resilience

Outcome: The FRFI can deliver critical operations through disruption.

An effective operational resilience approach involves the FRFI understanding and documenting its critical operations on an end-to-end basis and being prepared to deliver those operations through severe but plausible circumstances within established tolerances for disruption.

2.1 Identify and map critical operations

Principle 2: The FRFI should identify its critical operations and map internal and external dependencies.

2.1.1 Identify and assess critical operations

The FRFI should identify and document the services, products, and functions that, if disrupted, could imperil its continued operation, its safety and soundness, or its role in the financial system. The designation of critical operations depends on the strategy and risk profile of the FRFI, and to a certain extent the size, nature, scope, and complexity of the FRFI, as well as its interconnections to other financial institutions.

Critical operations should be assessed for their capability to withstand disruption and operational losses. Quantifications for direct financial losses (e.g., the cost of remediating and resolving technology failures and other disruptions) and indirect financial losses (e.g., reputational damage and forgone business) may be useful in these assessments. Based on the results of such assessments and taking into consideration the FRFI's enterprise-wide risk appetite, senior management may decide to add or enhance existing controls or accept the residual risk.

The identification and assessment of critical operations should be reviewed and updated regularly.

2.1.2 Holistic, end-to-end mapping of critical operations

The FRFI should engage in a holistic, end-to-end assessment of critical operations to comprehensively map internal and external dependencies. The mapping should be sufficiently granular to identify and document the people, technology, processes, information, facilities, third parties[2], and the interconnections and interdependencies among them, on which the FRFI relies to deliver critical operations. The level of granularity of the mapping should be sufficient to identify vulnerabilities and to support scenario testing and analysis (see Section 2.3). The FRFI should review and update the mapping of critical operations on a regular basis.

2.2 Establish tolerances for the disruption of critical operations

Principle 3: The FRFI should establish tolerances for the disruption of critical operations.

2.2.1 Tolerances for disruption should be established for each of the identified critical operations

The FRFI should set out the maximum amount of disruption it is willing to tolerate for each critical operation across a range of severe but plausible threat scenarios and risk events. Tolerances for disruption are separate from and should typically be set higher than the operational risk appetite (see Section 3.2 below). Disruption to critical operations can be measured as a duration or unit of time, and then nuanced with other measures and variables, such as the volume of transactions, the number of customers impacted, or the value of the financial loss.

2.2.2 Tolerances for disruption should be holistic and account for internal and external dependencies

When establishing tolerances for disruption, particular attention should be paid to the holistic, end-to-end mapping of the internal and external dependencies required to deliver critical operations. The FRFI should consider the impact of disruptions to other related critical operations, which rely on the same resources, as well as the potential for the failure of systems, facilities, and third-party suppliers on which critical operations rely.

2.3 Scenario testing and analysis

Principle 4: The FRFI should develop and regularly conduct scenario testing on critical operations to gauge its ability to operate within established tolerances for disruption across a range of severe but plausible operational risk events.

2.3.1 Scenario testing should be forward-looking and assess the impact of severe risk events

Effective scenario testing and analysis exercises for operational resilience are forward-looking, enabling institutions to assess the potential impact of severe risk events and evaluate their ability to deliver critical operations within established tolerances for disruption.

These exercises should be conducted across a range of severe but plausible threats, hazards and operational risk events of differing nature, scale, and duration. Such events could include, but would not be limited to:

- large-scale technology failures and power outages;

- critical third-party service interruptions;
- cyber incidents; and
- pandemics and natural disasters.

The FRFI should also contemplate the potential for overlapping, simultaneous, and prolonged disruptive events in developing their scenario testing and analysis exercises.

Scenario testing is an iterative process that will mature and become more sophisticated over time. To this end, the FRFI should consider the results of previous tests, past events (internal and external) and near misses when designing scenario tests.

2.3.2 Scenario testing should be holistic and enterprise-wide in scope

Scenario testing typically applies an end-to-end (or holistic) approach to determining the aggregate impact of a severe disruption across multiple operations, including the internal and external dependencies of critical operations and critical third parties. Business and central functions may engage with risk and compliance oversight and internal audit to consider the relevant risks for each scenario, and coordinate with critical third parties to conduct broader exercises. The FRFI should also consider the results of business continuity plan (BCP) testing where relevant (see Section 4.1.3).

2.3.3 Frequency and intensity of testing is proportionate to risk and criticality

The design of scenario testing should be commensurate with the size, complexity, business, and risk profile of the FRFI, as well as its level of interconnectedness to the financial system. In most cases, testing should occur at least annually and in response to a significant change in the risk environment.

2.3.4 Metrics should be implemented to monitor level of disruption

The FRFI should monitor its critical operations and assess whether it is performing within established tolerances for disruption during scenario tests. To that end, the FRFI should establish metrics to monitor, assess and take necessary remediation actions to address disruptions to critical operations. Such metrics should be regularly evaluated for their appropriateness and comprehensiveness.

2.3.5 Reporting on scenario testing and analysis is provided to senior management

Reporting should include assessments of resilience and whether critical operations performed within established tolerances for disruption, as well as analysis of deficiencies, opportunities to improve the management of operational risk events, and plans to address shortcomings in a timely manner.

2.4 Continue to strengthen operational resilience

Critical operations should be the FRFI's initial focus when developing and implementing its operational resilience approach. Recognizing that risk landscapes, economic environments, and business strategies are constantly evolving, the FRFI should continuously improve and strengthen its approach. The FRFI should also consider that levels of criticality may shift, and risk impacts may accumulate across multiple areas. A mature operational resilience approach extends beyond critical operations to include other activities, processes, functions, and services that could have a significant impact on the FRFI or its depositors, policyholders, or customers.

3. Operational risk management

Outcome: Operational risk management is integrated within the FRFI's enterprise-wide risk management program and supports operational resilience.

Operational risk is inherent in all products, activities, processes, and systems. As such, operational risk management is fundamental to an effective risk management program and operational resilience approach.

3.1 Operational risk management framework (ORMF)

Principle 5: The FRFI should establish an enterprise-wide operational risk management framework.

OSFI expects the FRFI to establish an ORMF scaled for proportionality. A comprehensive ORMF would typically include the following elements:

- operational risk appetite statement, including measurable limits/thresholds for risk acceptance;
- operational risk management policies and procedures that are regularly reviewed and revised through continuous improvement;
- standard operational risk taxonomy to ensure consistent use of operational risk terms across the enterprise;
- operational risk assessment tools and methodologies, which include evaluation of inherent risk and the relative strength of controls, and the estimation of residual risk; and
- operational risk monitoring tools.

3.2 Operational risk appetite

Principle 6: The FRFI should set a risk appetite for operational risks.

The operational risk appetite statement should be integrated into the FRFI's enterprise-wide risk appetite framework as described in OSFI's Corporate Governance Guideline.

3.2.1 Operational risk appetite articulates types of risks and sets quantifiable limits for risk acceptance

The risk appetite should articulate the nature and types of operational risk the FRFI is willing to accept within business-as-usual circumstances and should include a measurable component with limits/thresholds for risk acceptance.

3.2.2 Operational risk appetite is regularly reviewed

The operational risk appetite, its limits and thresholds should be regularly reviewed to ensure appropriateness to the risk profile and risk exposure of the FRFI. Such reviews may consider:

- changes in the external environment;
- significant increases/decreases in business or activity volumes;
- the quality of the control environment;
- the effectiveness of risk management or mitigation strategies;
- the FRFI's operational risk event experience; and

- the frequency, volume, or nature of breaches of risk appetite limits/thresholds.

3.3 Operational risk management practices

Outcome: Operational risks are managed within the FRFI's risk appetite.

Principle 7: The FRFI should ensure comprehensive identification and assessment of operational risk using appropriate operational risk management practices.

3.3.1 Risk Identification and assessment

3.3.1.1 Tools are applied to determine a FRFI's risk profile

The FRFI should regularly identify and assess its critical products, activities, processes, and systems to ensure it remains within its operational risk appetite.

The FRFI should have in place effective tools and practices to understand and manage their day-to-day operational risk profile and exposure and thereby promote operational resilience. Such tools include:

- Risk and control assessments (RCAs);
- Key risk indicators (KRIs);
- Operational risk event (ORE) data analysis.

While these are the most common tools used to identify, assess, and monitor operational risk, it should not be seen as a complete list. The size, nature, complexity of operations, strategy, risk profile and risk environment of the FRFI should be taken into account when determining the appropriate tools to apply.

3.3.1.2 RCAs are performed

To ensure the FRFI understands the operational risk inherent in all its critical products, activities, processes, and systems across the enterprise, it should use a self-assessment tool, such as the RCA, to effectively manage

operational risks. The self-assessment should be applied at various levels, where appropriate, while taking into consideration proportionality and criticality.

The FRFI should use RCAs to assess operational risks and the design and effectiveness of mitigating controls. RCAs should reflect the current environment and be forward-looking in nature. RCAs should be reassessed when the FRFI is undertaking significant change (see Section 4.4) or when there has been a significant operational risk event.

Completing RCAs should help the FRFI determine whether residual risk exposure is within its relevant limits and thresholds, as set out in its operational risk appetite. In cases where residual risk exceeds the limits and thresholds for operational risk, the FRFI should undertake corrective measures or formally accept the risk (i.e., document the rationale and approval for risk acceptance) and consider revisiting or adjusting limits and thresholds in line with the FRFI's operational risk appetite. The FRFI should track, monitor, and subject to independent challenge any action plans resulting from completed RCAs to ensure required enhancements are appropriately implemented and effective. Action plans addressing significant residual risks, key control weaknesses, or significant breaches should be given higher priority.

3.3.1.3 KRIs are established and acted on

KRIs are metrics used to assess and monitor the main drivers of exposure to operational risk. Leading and lagging indicators are typically developed using data from risk assessments, such as RCAs, internal and external events. Lagging indicators should provide insight into control weaknesses, while leading indicators are used for risk exposures and emerging risks. KRIs should have associated escalation protocols to identify risk trends and warn when risk levels approach or exceed limits or thresholds. These warnings should prompt the FRFI to take the appropriate mitigating action.

The FRFI should have KRIs in place at appropriate levels within the organization to support the proactive management of operational risk.

3.3.1.4 Operational risk event data is captured and analyzed

The FRFI should have systems and processes in place to capture data and analyze significant internal operational risk events (e.g., those that exceed an appropriate internal threshold), with controls (i.e., segregation of duties,

verification) established to maintain data integrity.

For significant operational risk events, OSFI expects the FRFI to identify the root cause as well as any required remedial action such that similar future events are prevented or sufficiently managed. Reporting and analysis should be subject to appropriate signoff and escalation, effective challenge, and be based on the potential or observed impact of the event. It should determine:

- whether the exposure is an actual, potential, or near-miss event;
- the underlying operational risk category exposure as defined within the risk taxonomy;
- deficiencies and control failures that can be mitigated; and
- the corrective actions to be taken to address the deficiencies and control failures.

3.3.2 Monitoring and reporting

Principle 8: The FRFI should conduct ongoing monitoring of operational risk to identify control weaknesses and potential breaches of limits/thresholds, provide timely reporting, and escalate significant issues.

3.3.2.1 Ongoing risk-based monitoring of operational risks

As part of its management of operational risk, OSFI expects the FRFI to conduct ongoing monitoring activities to help the FRFI prepare for and respond to potential threats and changes in the risk landscape. Such monitoring activities should:

- be risk-based and subject high-risk areas to enhanced monitoring;
- take place regularly, as well as in response to changes in the FRFI's operating environment and risk landscape;
- include comprehensive metrics for measuring adherence to operational risk appetite and approved thresholds/limits;
- be forward looking; and
- be supported by data (e.g., residual risks, control deficiencies, actual events, and internal audits).

3.3.2.2 Comprehensive reporting on operational risk profile and issues are escalated as appropriate

Senior management should be provided with timely reports on the FRFI's ongoing monitoring of operational risks across the business units and functions as appropriate, particularly in cases where it discovers significant deficiencies. Reporting and analysis should include:

- comprehensive assessment of the FRFI's overall operational risk profile;
- monitoring outcomes, including formal metrics and/or measures to identify and report instances of breaches of operational risk limits/thresholds;
- significant issues, impacts and remedial actions taken;
- documented risk acceptance rationale and approvals; and
- timely escalation mechanisms particularly for significant risk exposures.

3.3.3 The FRFI continually enhances its operational risk management

As the risk environment evolves in a fast-paced and interconnected financial ecosystem, the FRFI should strive to continuously improve operational risk management practices. For example, if traditional manual practices no longer provide sufficient assurance, the FRFI may consider investing in innovation, automation, and real-time operational risk management activities to continuously strengthen operational resilience.

4. Operational risk management subject areas that strengthen operational resilience

Outcome: Operational resilience is underpinned by operational risk management subject areas, including business continuity management, disaster recovery, crisis management, change management, technology and cyber risk management, third-party risk management, and data risk management.

Operational resilience is built on a foundation of effective operational risk management. In addition to the core practices of operational risk management outlined above in Section 3, there are operational risk management

subject areas that strengthen operational resilience by emphasizing preparation, responsiveness, recovery, learning and adaptation. The areas that have an outsized impact on the achievement of operational resilience include business continuity management, disaster recovery, crisis management, change management, technology and cyber risk management, third-party risk management, and data risk management.

4.1 Business continuity management (BCM)

The FRFI's BCM should be integrated with and serve to strengthen its operational resilience approach, such that the FRFI can holistically prepare for and respond to a disruptive event. OSFI's expectations for governance of BCM align with its expectations for governance of operational risk and resilience more generally. Specifically:

- senior management should ensure adequate financial and human resources are dedicated to the development, implementation, and oversight of BCM;
- responsibilities and accountabilities for BCM should be clearly assigned;
- reporting to senior management should include the implementation status of specific plans for business continuity, incident reports, testing results and analysis, and related action plans for strengthening the FRFI's BCM and its operational resilience approach; and
- BCM policies and procedures should be implemented on an enterprise-wide basis.

4.1.1 Business impact analysis (BIA)

BIA is an initial step in developing the FRFI's BCM. BIAs are used to identify critical areas and dependencies (i.e., functions, products, services, technology, systems, resources, third parties, infrastructure, etc.) and associated recovery objectives (timeframes, data, volumes, etc.). BIAs assess the risks and potential impacts of a range of disruptive events and should be regularly reviewed and updated. BIAs enable the identification and measurement of the impact of a disruption, and the maximum limits on recovery objective before severe consequences may occur.

4.1.2 Business continuity plans (BCPs)

Effective BCPs enable institutions to prepare, respond, recover, learn, and adapt to disruptive events. The FRFI's BCPs should support the continued delivery of services, products, and functions—particularly those identified as

critical operations—during a range of events, from relatively minor incidents to the most severe but plausible, including consideration of the potential for overlapping and simultaneous events.

Sound practices for BCPs include:

- internal decision-making protocols for invoking the BCP;
- internal and external communication protocols;
- roles and responsibilities for managing disruptions to critical operations;
- recovery objectives, including recovery levels (e.g., business-as-usual) and recovery times;
- procedures for addressing testing outcomes and making strategic enhancements to plans;
- event impact analysis and recovery strategies;
- initiatives to provide training and raise awareness so that staff can respond and adapt;
- precautions to ensure the safety of the FRFI's personnel during the event; and
- succession plans for unexpected absences or loss of key personnel during the execution of the plan or immediately following the risk event.

4.1.3 BCP testing

BCP testing provides assurance that a plan is well-designed to minimize the impact of a disruption, in accordance with its BCM and BIA recovery objectives. The frequency and type of BCP testing should be tailored to the potential impact per the BIA and the FRFI's risk appetite.

The FRFI should conduct testing to identify potential deficiencies and gaps within BCPs under a range of adverse circumstances. In addition to fostering continuous improvement, testing is vital for promoting the awareness and understanding of senior management and other key employees about their roles and responsibilities in the BCP during risk events.

BCP testing can also help to inform scenario testing and analysis, contributing to a holistic view of critical operations across the enterprise as part of the FRFI's operational resilience approach (see Section 2.3).

4.2 Disaster recovery

Disaster recovery planning helps to develop a posture of readiness and prepare potential actions for severe risk events, such as loss of technology infrastructure (e.g., data servers). The disaster recovery plan should include roles and responsibilities, and protocols for invoking the recovery plan.

Please refer to Guideline B-13 on Technology and Cyber Risk Management Guideline for OSFI's expectations related to disaster recovery.

4.3 Crisis management

The FRFI should establish a crisis management plan to ensure an effective, coordinated, and timely response to a potential crisis or significant emergency, which may originate from internal or external factors. To ensure effective communications, expedite recovery and respond decisively, the FRFI should consider designating a focal point of responsibility for managing a crisis, such as a crisis management team or equivalent structure.

The FRFI should also consider developing internal and external crisis communication protocols to ensure it communicates the best available information to the appropriate stakeholders in a timely manner. Effective communication during a crisis helps to keep employees safe, minimize the disruption of operations, meet recovery objectives, and maintain public confidence in the institution.

Escalation protocols should set out the criteria for escalating the crisis, or other significant emergency, to senior management and for invoking the crisis management plan.

The crisis management plan should be regularly tested and shared with applicable areas. Lessons-learned exercises should be undertaken following a crisis.

4.4 Change management

In general, the operational risk exposure of the FRFI evolves when it initiates change, such as developing new products or services, entering new markets, engaging in new activities, implementing new technological systems, or significantly modifying business processes. The FRFI should develop and document a change management process

that is comprehensive and monitors the evolution of the FRFI's operational risk exposure across the full lifecycle of the change it is initiating.

The FRFI should have change management policies and procedures, and contingency plans, to address the operational risk associated with new products, services, activities, markets, technological systems, and business processes.

When initiating significant change, the FRFI should undertake a change management process, accompanied by contingency plans, including:

- identifying and assessing inherent and residual risks;
- evaluating relevant controls;
- considering risks related to human resources, risk management, and technology;
- project management throughout the change lifecycle, including adequate pre- and post-implementation testing and the appropriate metrics;
- reviewing and making any necessary changes to operational risk appetite, limits, and thresholds, including any necessary changes to the assessment of operational risks associated with existing products, services, activities, markets, processes, or systems;
- identifying any new risks and measuring any changes to operational risk exposure, including unexpected changes; and
- conducting independent assessment and effective challenge of the change management process.

4.5 Technology and cyber risk management

A critical technology failure, infiltration of a critical system, or loss or corruption of data could imperil the FRFI's operational resilience. Sound technology and cyber risk management is therefore fundamental to bolstering operational resilience. OSFI's Guideline B-13 promotes the implementation of a technology architecture and systems that align with business needs and the FRFI's tolerance for disruption.

Please refer to Guideline B-13 on Technology and Cyber Risk Management Guideline for OSFI's expectations related to managing the risks associated with technology.

4.6 Third-party risk management

Risks can arise from critical third-party arrangements, including operational disruption at the third party or the loss or corruption of critical data, which can threaten the FRFI's operational resilience. Effective third-party risk management is therefore an important contributor to operational resilience.

Please refer to Guideline on B-10 Third-Party Risk Management Guideline for OSFI's expectations related to managing the risks associated with third-party arrangements.

4.7 Data risk management

Managing data risks is essential to ensure operational resilience in an interconnected and data-driven environment. Effective data risk management supports oversight and enhances decision-making by ensuring that data are accurate, complete, timely, secure, and protected. Effective data handling and processing can strengthen operational resilience by minimizing the likelihood and impact of data breaches, system failures, or disruptions, thereby safeguarding the FRFI's critical operations and reputation.

A risk-based approach to managing data risk should include:

- a robust data management framework, including policies, procedures, standards, assessments, and controls;
- a risk appetite and appropriate metrics to track and report on the management of data risk;
- clearly defined roles and responsibilities on the management and oversight of data;
- processes to classify and protect data, ensuring integrity, confidentiality, and availability throughout the data lifecycle, commensurate with assessed risks;
- ability to accurately collect, aggregate and report risk data across the enterprise in a timely manner;
- a well-defined strategy for data architecture and IT infrastructure that supports the collection, aggregation, and reporting of data across the enterprise for decision-making;
- incident management processes to respond to data breaches and other data-related incidents;
- providing adequate and periodic training to the people responsible for the management and oversight of data; and

- continuous monitoring and review of data risk management practices to identify areas for improvement and implementation of appropriate changes.

[1] ‘Foreign bank branches’ refers to foreign banks authorized to conduct business in Canada on a branch basis under Part XII.1 of the *Bank Act*. ‘Foreign insurance company branches’ refers to foreign entities that are authorized to insure in Canada risks on a branch basis under Part XIII of the *Insurance Companies Act*.

[2] Third parties are any type of business or strategic arrangement between the FRFI and an entity(ies) or individuals, by contract or otherwise, save for arrangements with FRFI customers (e.g., depositors and policyholders) and employment contracts, which are excluded from this definition. Please see Guideline B-10 on Third-Party Risk Management.