Guideline

Title	Operational Risk Management and Resilience – Guideline
Category	Sound Business and Financial Practices
Date	August 22, 2024
Sector	Banks Cooperative Credit Associations Foreign Bank Branches Foreign Insurance Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies
No	E-21

Table of Contents

A. Overview

- A1. Relationship between operational risk management and operational resilience
- A2. Purpose
- A3. Scope
- A4. Application
- A5. Definitions
- A6. Outcomes and expectations

1. Governance

- 1.1 Senior management
- 1.2 Business and central functions
- 1.3 Independent oversight
- 1.4 Independent assurance

2. Operational risk management

- 2.1 Operational risk management framework
- 2.2 Operational risk appetite
- 2.3 Operational risk management tools
- 2.4. Monitoring and reporting

3. Operational resilience

- 3.1 Identification and mapping
- 3.2 Establishing tolerances for disruption
- 3.3 Scenario testing

4. Key areas of operational risk management that strengthen operational resilience

- 4.1 Business continuity risk management
- 4.2 Disaster recovery risk management
- 4.3 Crisis management
- 4.4 Change management
- 4.5 Technology and cyber risk management
- 4.6 Third-party risk management
- 4.7 Data risk management

A. Overview

Financial institutions operate in a fast-paced, complex environment with increasing risks to their operations, notably their people, facilities, and systems. Robust operational risk management and resilience enhance their ability to prevent, detect, respond to, and recover from adverse events, while continuing to deliver critical operations.

A1. Relationship between operational risk management and operational resilience

Operational risk management is about identifying and managing risks that could impact the operations of financial institutions. The goal of operational risk management is to minimize the frequency and intensity of disruptions and losses from those risks.

Sound operational risk management is a cornerstone of operational resilience, enhancing the ability of financial institutions to withstand disruptions. Operational resilience, however, assumes that disruptions will happen. It focuses on the response of a financial institution and its recovery, by taking a holistic approach that considers all critical operations end to end.

A2. Purpose

Sets expectations for managing operational risks and resilience.

A3. Scope

Applies to all federally regulated financial institutions, including foreign bank branches and foreign insurance company branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada. Expectations for branches are set out in Guideline E-4 on Foreign Entities Operating in Canada on a Branch Basis.

A4. Application

This guideline applies on a risk-basis, proportional to the financial institution's:

- Size.
- Strategy.
- Risk Profile.
- Nature, scope, and complexity of operations.
- Interconnectedness, such that disruptions could harm other financial institutions, the financial system, or the broader economy.

A5. Definitions

Operational risk

"Operational risk" is the risk of loss resulting from people, inadequate processes and systems, or external events.

Operational resilience

"Operational resilience" is the ability to deliver operations, especially critical operations, through disruption.

Operational risk event

"Operational risk event" is an unintended outcome (loss or gain) resulting from operational risk. This includes near misses (that is, where the financial institution did not experience a loss or gain from an event).

Critical operations

"Critical operations" are services or products that, if disrupted, would put at risk the financial institution's continued operations or safety and soundness, or harm other institutions due to its interconnectedness to the financial system.

Crisis management team

"Crisis management team" is typically a senior group within a financial institution responsible for making decisions, coordinating, and providing oversight of the development and implementation of strategies to address and mitigate potential or actual crises that could affect operations, reputation, or financial stability.

Data risk

"Data risk" is the risk of loss that can result from the collection, storage, processing, use, sharing, or disposal of data. It could be caused by people, inadequate processes and systems, or from external events impacting data.

Scenario testing

"Scenario testing" is defined in Guideline E-18: Stress Testing. As it pertains to operational resilience, scenario testing is used to assess the ability to operate within tolerances for disruption under a range of severe but plausible scenarios.

Tolerance for disruption

"Tolerance for disruption" is the maximum disruption from an operational risk event a financial institution can withstand, under a range of severe but plausible scenarios. It includes things like outage time, diminishment of service, loss of data, or extent of customer impact.

Failover

"Failover" is the ability to switch automatically to a backup technology system when a primary system fails.

Third-party arrangement

"Third-party arrangement" is defined in Guideline B-10: Third-Party Risk Management.

A6. Outcomes and expectations

1. Operational risk management practices support operational resilience.
2. Operational risks are managed within approved risk appetite and risk limits.
3. Critical operations continue to be delivered through disruptions.

Outcome 1: Operational risk management practices support operational resilience.

1. Governance

Principle 1: An effective operational risk management framework and approach to operational resilience are properly governed, documented, and implemented.

1.1 Senior management

Senior management is ultimately accountable for the development, implementation and oversight of an effective operational risk management framework and approach to operational resilience.

This involves:

- Ensuring effective operational risk management and resilience programs are established.
- Ensuring ongoing scenario analysis and testing at both the business unit and, as appropriate, enterprise-wide levels are conducted.
- Defining clear roles and accountabilities and allocating adequate resources.
- Providing timely and accurate reporting to the board of directors.
- Ensuring operational deficiencies are assessed and addressed in a timely and sustainable manner.
- Ensuring breaches of tolerances for disruption are appropriately escalated and addressed.
- Promoting and reinforcing a supportive culture and behaviours.

- Empowering risk and compliance functions to challenge practices and decisions without fear of reprisal.

Refer to the Corporate Governance Guideline for expectations of boards of directors related to business plans, strategy, risk appetite, culture, and the oversight of senior management and internal controls.

1.2 Business and central functions

The business and central functions are accountable for managing operational risks and contributing to operational resilience. Their activities should be subject to independent, documented, and effective challenge.

Business and central functions:

- Adhere to the financial institution's operational risk management framework and operational resilience approach, along with their related policies and procedures.
- Identify and assess operational risks and maintain effective controls, leveraging appropriate tools.
- Manage operational risk in line with the risk appetite framework and operational resilience approach.
- Escalate operational risk events appropriately.
- Identify critical operations and set tolerances for disruption (see sections 3.1 and 3.2).
- Manage risks to critical operations within tolerances for disruption.
- Provide adequate training to staff on operational risk management and resilience.

1.3 Independent oversight

The independent risk and compliance functions oversee and challenge the risk and resilience activities of the business and central functions, including by:

- Establishing and overseeing adherence to the operational risk management framework and operational resilience approach.
- Reviewing action plans to address identified gaps.
- Ensuring assessment and reporting tools are developed and monitored.

- Ensuring decisions, actions, and assessments are adequately documented.
- Ensuring that appropriate escalation channels are developed and maintained and that significant issues are resolved.

1.4 Independent assurance

Internal audit or a similar function should provide independent assurance to senior management and the board of directors that operational risk management controls, policies and procedures, and systems are designed and operating effectively.

Outcome 2: Operational risks are managed within approved risk appetite and risk limits

2. Operational risk management

Managing operational risks effectively is fundamental to operational resilience.

Principle 2: An effective enterprise-wide operational risk management framework is in place.

2.1 Operational risk management framework

An effective operational risk management framework includes:

- An approved operational risk appetite statement with operational risk limits.
- Policies and procedures that are regularly reviewed and updated.
- A risk taxonomy that includes categories of risks related to people, inadequate internal processes and systems, and external events.
- Assessment and monitoring tools to evaluate risks and controls.

Principle 3: A risk appetite for operational risks is defined and adhered to.

2.2 Operational risk appetite

The operational risk appetite statement should be integrated into the risk appetite framework, as described in the Corporate Governance Guideline.

> Refer to the Corporate Governance Guideline for expectations related to the Risk Appetite Statement.

The operational risk appetite articulates the types and level of operational risks the financial institution is willing to accept to achieve its business goals. The operational risk appetite should:

- Include qualitative and quantitative measures.
- Be forward-looking (i.e., anticipate potential risks in the future).
- Explicitly set out risk limits.

Operational risk limits should typically be less than those established for tolerances for disruption (see section 3.2).

Frameworks, policies, and procedures should cover circumstances when an institution is close to breaching – or breaches – its risk appetite due to evolving risks, events, proposed transactions, changes to the business model, or other reasons. Such circumstances should prompt a decision to accept, avoid, or mitigate the risk, or review the operational risk appetite and limits.

Regular reviews of the operational risk appetite and operational risk limits should consider:

- Changes in the external environment, business volumes, or activities.
- The quality of the control environment.
- The effectiveness of risk mitigation strategies.
- Operational risk event experiences.
- The frequency, volume, or nature of breaches of risk appetite.

Principle 4: Operational risks should be comprehensively identified and assessed using appropriate tools and methods.

2.3 Operational risk management tools

Operational risk should be regularly assessed to ensure it remains within the operational risk appetite and limits and that risks are identified and effectively managed. This should be done using appropriate tools, such as:

- Risk and control assessments.
- Key risk indicators.
- Operational risk event data analysis.
- Scenario analysis.

2.3.1 Risk and control assessments

A self-assessment tool, such as a risk and control assessment, should be used to:

- Identify inherent operational risks.
- Identify and assess associated controls to determine residual operational risks.

A risk and control self-assessment or similar tool helps determine whether residual risks are within operational risk limits. Where residual risk exceeds operational risk limits, the financial institution should develop and implement action plans that include:

- Reviewing the appropriateness of operational risk limits.
- Further mitigating the operational risk to the extent possible.
- Explicitly accepting the level of operational risk exceeding operational risk limits.

Residual operational risks should be reassessed periodically, for example, when undertaking a significant change (see section 4.4) or when there has been a significant operational risk event.

2.3.2 Key risk indicators

Key risk indicators are tools used to assess and monitor the main drivers of operational risk and assess whether the financial institution continues to operate within its operational risk limits. They may be developed using input from risk and control assessments (see section 2.3.1), operational risk events (see section 2.3.3), and other sources. Key risk indicators should be in place at various levels within the organization, including at the business unit and enterprise-wide levels.

Key risk indicators may be either leading or lagging. Leading indicators are used to identify risk exposures and emerging risks. Lagging indicators provide insight into control weaknesses. Both should have escalation protocols to warn when risk levels approach or exceed limits. These warnings should prompt management actions to mitigate the risks.

2.3.3 Operational risk event data

Operational risk event data exceeding established limits should be captured to assess:

- What the root cause of the operational risk event is.
- Whether the operational risk event was actual, potential, or a near-miss.
- What the underlying operational risk category exposures contributing to the event were.
- What corrective measures ought to be taken to address deficiencies or control failures.

2.3.4 Scenario analysis

Scenario analysis identifies potential operational risk events, their impacts, control gaps, and helps develop mitigating actions. It focuses on the sources of operational risk and exposure. Scenario analysis should be conducted using appropriate techniques at both the business unit and enterprise-wide levels and incorporate a range of severe but plausible scenarios.

Scenario analysis should be an iterative process that becomes increasingly sophisticated over time. The results of previous analyses, past events (internal and external), and near misses should be considered in the design of future scenario analysis.

Scenario analysis results may be used to inform operational resilience scenario testing (see section 3.3).

Principle 5: Operational risks should be continuously monitored and reported to identify control weaknesses and potential breaches of risk appetite and limits.

2.4. Monitoring and reporting

2.4.1 Monitoring

Ongoing monitoring should be conducted to help prepare for, and respond to, changes in operational risks. It should assess adherence to the operational risk appetite statement and operational risk limits, as well as tolerances for disruption (see section 3.2). Monitoring should be risk-based, with high-risk activities subject to greater scrutiny.

Monitoring should be supported by comprehensive metrics. Operational risk management tools may be used to support risk monitoring and identify any corrective measures.

2.4.2 Reporting and escalation

Reporting and escalation mechanisms should ensure senior management and the board of directors are provided with timely reports and kept informed of significant concerns identified through the operational risk management tools (see section 2.3). This includes where:

- Significant issues and deficiencies are discovered.
- Risk limits are approached or breached.
- Residual risks are explicitly accepted.

Reports should include an aggregated assessment of risk profile that is current and forward-looking, along with corrective measures.

Senior management and the board of directors should also receive the results of scenario analysis (see section 2.3.4) and scenario testing (see section 3.3). This should include:

- Analysis of deficiencies.
- An assessment of operational resilience, and whether critical operations can be maintained within established tolerances for disruption (see section 3.2).
- Plans to address shortcomings.

Outcome 3: Critical operations continue to be delivered through disruptions.

3. Operational resilience

Operational resilience entails a sound understanding of critical operations end to end and their delivery through severe but plausible circumstances within tolerances for disruption.

While critical operations ought to be prioritized, over time, a mature approach to operational resilience should include other operations that could have a significant impact on the financial institution.

Principle 6: Critical operations are identified and assessed, and internal and external dependencies are mapped.

3.1 Identification and mapping

Critical operations should be identified and assessed for their ability to withstand disruptions. Assessments should be reviewed and updated regularly, including estimates of direct and indirect financial losses due to disruptions.

Once identified, critical operations should be mapped for internal and external dependencies.

Mapping should:

- View critical operations end to end.
- Consider people, technology, processes, information, facilities, third parties, and connections or dependencies among them.
- Focus on the activities that are needed to deliver the critical operations.

- Identify vulnerabilities, which can inform scenario testing for operational resilience (see section 3.3).

Where a third party is identified as critical, sufficient information should be obtained to assess its resilience.

Principle 7: Tolerances for disruption of critical operations are established.

3.2 Establishing tolerances for disruption

Tolerances for disruption should set out the maximum level of disruption a financial institution can withstand across a range of severe but plausible scenarios.

Tolerances for disruption are different and would typically be greater than risk appetite. Risk appetite relates to the level of risk an institution would willingly accept to achieve its business goals; whereas tolerance for disruption relates to the maximum disruption an institution can withstand in a crisis.

Tolerances for disruption should consider the impact of a disruption on:

- Other critical operations of the financial institution that rely on the same resources.
- Systems, facilities, and third-party suppliers on which critical operations depend.
- Other financial institutions, the financial system, and the broader economy.

When setting a tolerance for disruption, financial institutions should also be mindful that the use of critical operations may vary at different times of day and throughout the year.

Refer to Guideline B-10 on Third-Party Risk Management for expectations related to third-party risk.

Principle 8: Scenario testing should regularly assess the ability of critical operations to persist through severe-but-plausible disruptions within established tolerances for disruption.

3.3 Scenario testing

Regular scenario testing improves understanding of when tolerances for disruption would be breached (see section 3.2). This goes beyond operational risk scenario analysis, which identifies potential operational risk events, their impacts, controls, and mitigating actions (see section 2.3.4).

Scenario testing should include a range of severe but plausible scenarios, including concurrent scenarios and those of longer duration. Examples include:

- Power outages.
- Large-scale technology failures.
- Critical third-party service disruptions.
- Cyber incidents.
- Natural disasters.
- Health pandemics.

Scenario testing typically applies an end-to-end approach to determine the total impact across multiple business units. It includes internal and external dependencies. Based on criticality, a variety of testing methodologies should be used, including table-top exercises, simulations, and live-systems testing.

The business and central functions, risk and compliance functions, and internal audit or a similar function may provide input and collaborate in the design and testing of scenarios.

The financial institution should also coordinate with critical third parties, where possible, to conduct broader exercises.

The frequency and intensity of testing should be proportional to the criticality of and risk to operations. Where there are significant changes in the risk environment, testing should take place more frequently and outside the regular cycle.

Scenario testing is iterative. It should become more sophisticated over time. The results of previous tests should inform the design of future tests.

4. Key areas of operational risk management that strengthen operational resilience

Key areas of operational risk management that strengthen resilience include:

- Business continuity risk management.
- Disaster recovery risk management.
- Crisis management.
- Change management.
- Technology and cyber risk management.
- Third-party risk management.
- Data risk management.

This list is not exhaustive. As the risk landscape evolves, other emerging risk areas may play a greater role in achieving operational resilience.

Adhering to the expectations below contributes to outcomes one through three above.

4.1 Business continuity risk management

Business continuity risk management is the process of planning for, and recovering from, disruptions to operations. It should be integrated with and strengthen operational resilience. Over time, its focus should evolve from business processes to critical operations end to end.

It should include:

- Conducting business impact analyses.
- Developing and testing business continuity plans.

4.1.1 Business impact analysis

A business impact analysis assesses the risks and potential impacts of a range of disruptive events on operations. It should identify and measure:

- The impact of disruptions.
- The maximum limits on recovery objectives before severe consequences or losses occur.

It should be regularly reviewed and updated, as appropriate.

4.1.2 Business continuity plans

Business continuity plans set out the response and recovery actions for a range of potential threats. They are designed to address disruptions related to people and physical assets, making sure they can function quickly when disaster strikes.

This should include:

- Establishing protocols for invoking the plan and making decisions.
- Defining roles and responsibilities for managing disruptions.
- Designating backup personnel to cover unexpected absences.
- Implementing precautions to ensure safety of staff.
- Setting targets for recovery levels and times.
- Conducting business impact analysis, workarounds, and recovery strategies.
- Developing internal and external communication plans.

Staff should be provided with training on business continuity plans, including their activation and how operations will be managed during disruption.

4.1.3 Business continuity plan testing

Business continuity plan tests should provide reasonable assurance that plans are effective. They should promote understanding among senior management and staff about their roles and responsibilities in the business continuity

plan and how operations will be managed during disruption.

Tests should consider a range of severe but plausible circumstances, including scenarios with disruptions that:

- Are long in duration.
- Are simultaneous in nature.
- Involve critical third parties.

The frequency and type of testing should be tailored to the results of business impact analyses and align with the operational risk appetite. Critical third parties should also demonstrate robustness in their own business continuity plans and testing. There should be processes to address gaps identified during testing, as well as contingency plans for critical third parties.

Business continuity plan testing should also inform scenario testing and contribute to an end-to-end view of critical operations across the enterprise (see section 3.3).

> Refer to Guideline B-10 on Third-Party Risk Management for expectations related to third-party risk.

4.2 Disaster recovery risk management

Disaster recovery risk management helps prepare for severe but plausible risk events related to loss of technology infrastructure (for example, networks and data servers). The disaster recovery plan should include roles and responsibilities and protocols for its invocation.

For technology assets that support critical operations, failover and backup plans should be developed and tested.

> Refer to Guideline B-13 on Technology and Cyber Risk Management for expectations related to disaster recovery.

4.3 Crisis management

Effective crisis management helps keep employees safe, minimizes disruption, provides a timely and coordinated response, and maintains public confidence in the financial institution. A crisis management team can help ensure effective communication, expedited recovery, and an effective response to the crisis.

A crisis management plan should be established that ensures effective, coordinated, and timely responses to potential crises from internal or external sources. It should include:

- Protocols for escalation to senior management and the board.
- Criteria for invoking the plan.
- Internal and external communications protocols for the timely sharing of information with stakeholders.

Lessons-learned exercises should be undertaken following a crisis and incorporated into the plan. The crisis management plan should be regularly tested and shared with the relevant business units in the financial institution and any impacted external parties, as appropriate.

4.4 Change management

Change can create operational risk. Significant changes can include but are not limited to:

- Offering new products or services.
- Engaging in acquisitions and divestitures.
- Entering new markets.
- Implementing new technological systems.
- Significantly modifying business processes.

Comprehensive change management processes should be applied to significant changes, with operational risks assessed and monitored. Processes should govern both the operational risks introduced by the change, as well as the effective management of the change itself.

Effective change management processes should align with the general expectations for operational risk management set out in section 2.

In addition, the financial institution should:

- Adopt robust project management throughout the initiative's lifecycle.
- Review and make any adjustments to operational risk appetite required because of the change.
- Deploy tested contingency plans in the event a change fails.
- Test the change on systems and processes before introducing it.
- Develop metrics to assess the post-implementation effectiveness of the change.

4.5 Technology and cyber risk management

A critical technology failure, infiltration, or loss of data can result in wide-scale disruption impacting operations. Sound technology and cyber risk management is fundamental to bolstering operational resilience.

> Refer to Guideline B-13: Technology and Cyber Risk Management for expectations related to technology and cyber risks.

4.6 Third-party risk management

Threats to operational resilience can arise from critical third-party arrangements, including disruption at the third party or the loss or corruption of critical data. Accordingly, effective third-party risk management is an important contributor to operational resilience.

> Refer to Guideline B-10: Third-Party Risk Management for expectations related to third-party risk.

4.7 Data risk management

In an inter-connected and data-driven world, effective data risk management is an important component of operational risk management and essential to operational resilience. Unavailable, poor quality, or leaked data can hamper decision-making, disrupt critical operations, damage reputation, and impact other financial institutions, the financial system, and the broader economy.

This is particularly so for data that is:

- Related to critical operations.
- Needed for decision-making.
- Personally identifiable.
- Proprietary.

Effective data risk management ensures that data is accurate, complete, timely, secure, and protected. Data risk management should align with the general expectations for operational risk management set out in section 2. It should also comprise a specific data risk management framework that includes a data risk management strategy and program.

The data risk management program should include:

- Appropriate data governance, with clear roles and responsibilities.
- A data architecture and information technology infrastructure that support the collection, aggregation, tracing of lineage, and reporting of critical data across the enterprise.
- Processes for classifying, aggregating, and protecting data.
- Methodologies for ensuring the integrity, adaptability, confidentiality, and availability of data throughout its lifecycle.
- Processes for escalating and responding to data breaches and other data-related incidents.
- Training programs for the people responsible for managing and overseeing data.

Refer to Guideline B-13: Technology and Cyber Risk Management for expectations related to information classification and data protection.