Letter

Title	Operational Risk Management and Resilience — Letter
Category	Sound Business and Financial Practices
Date	August 22, 2024
Sector	Banks Cooperative Credit Associations Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies

Table of Contents

What does the guideline do?

What should you do?

OSFI's Response to Draft Guideline E-21 on Operational Resilience and Risk Management

- Guideline Structure and Terminology
- Scenario Testing and Analysis
- Change Management
- Phased Implementation

Today, OSFI released final Guideline E-21: Operational Risk Management and Resilience. It concludes an extended consultation on operational risk management and resilience that began in July 2021.

The final guideline is revised with simplified language to make it clearer and better streamlined. The expectations are, in substance, the same as in the consultation draft, other than some changes based on feedback (see below).

What does the guideline do?

- Enhances expectations for operational risk management.
- Sets new expectations for operational resilience, a vital component of our supervisory framework.
- Sets new expectations for business continuity risk management, crisis management, change management, and data risk management, which strengthen operational resilience.

Financial institutions are familiar with our expectations related to operational risk management, which have been in place since 2016 and therefore sections 1 and 2 are effective immediately. Other new expectations deal with concepts many financial institutions generally are experienced in managing.

What should you do?

- By September 1, 2025
    - **Full adherence to section 4**. Although the expectations in this section are new, they cover risk categories already addressed by the 2016 guideline on Operational Risk Management. Therefore, institutions should have remediated any gaps by this date.
- By September 1, 2026
    - **Full adherence to this guideline**. While we recognize that operational resilience programs will mature over time, institutions should have completed identification, mapping and setting tolerances for disruption of their critical operations. Furthermore, institutions should also have developed their scenario testing methodology and begun the testing process so that by September 1, 2027, testing has been completed for all critical operations.

During the transition period, we plan to selectively conduct supervisory work to assess institutions' progress in implementing their operational resilience programs. We will also continue to assess whether institutions have effective operational risk management practices.

OSFI's Response to Draft Guideline E-21 on Operational Resilience and Risk Management

Guideline Structure and Terminology

Feedback: Reorient the guideline with operational risk management preceding operational resilience to make it more intuitive to understand.

> **Response**: The guideline was reoriented this way and revised with simplified language to make it clearer and easier to understand.

Feedback: Clarify meaning of "business and central functions" and "risk management and compliance."

> **Response**: These terms are clarified, and explained in our Supervisory Framework:
>
> - The business and central functions own and manage risks.
> - The risk management and compliance functions oversee and challenge risk decisions and practices.

Scenario Testing and Analysis

Feedback: Clarify that the list of operational risk management tools is not exhaustive, particularly that scenario analysis is still relevant to operational risk management.

> **Response**: Clarified that:
>
> - The list of operational risk management tools is not exhaustive.
> - Scenario analysis is still relevant and focuses on identifying and assessing the impact, controls, and mitigating actions of operational risks at the business unit level and enterprise wide.
> - Scenario testing goes further to test whether critical operations can remain within tolerances for disruption on an end-to-end basis, across multiple business lines, in severe but plausible circumstances.

Feedback: Frequency of scenario-testing should be risk-based rather than annual.

> **Response:** Clarified that scenario-testing should align with risk and criticality but when significant changes in the risk environment arise, it should take place outside the regular cycle.

Feedback: Third-party participation in scenario-testing may not always be available.

Response: Clarified that critical third parties should be involved in scenario-testing on a best-effort basis.

Change Management

Feedback: Provide flexibility to scale change management activities to the type of change initiated.

Response: Change management activities should apply to significant changes.

Feedback: Apply the change management section to the operational risks introduced by change, not to change management practices themselves.

Response: We disagree. Poorly executed change can lead to disruption. We clarified that processes should govern the risks introduced by change and the change management practices themselves.

Phased Implementation

Feedback: The guideline should be subject to phased implementation.

Response: The expectations in the guideline are subject to the phased implementation set out above.