SmartSuite

Framework / Cybersecurity / Other

OSFI B-13 — Technology and Cyber Risk Management Guideline

OSFI B-13 guides Canadian federally regulated financial institutions on managing technology and cyber risks to maintain operational resilience.

What it is

Canada OSFI B-13 — Technology and Cyber Risk Management Guideline is a regulatory guideline that assists federally regulated financial institutions in managing technology risks and strengthening cybersecurity and operational resilience. The framework establishes expectations for governance, risk management, and security controls to safeguard critical systems and sensitive data.

Issued by the Office of the Superintendent of Financial Institutions (OSFI), B-13 applies to banks, insurance companies, and other federally regulated entities in Canada. The guideline addresses areas such as cybersecurity controls, technology risk assessment, incident response planning, and third-party management. It serves as a cornerstone for regulatory compliance and aligns with global risk management practices.

At a glance

PUBLISHER Office of the Superintendent of Financial Institutions (OSFI)	TYPE Framework	VERSION Guideline B-13
EFFECTIVE July 2017	DOMAIN Cybersecurity	FAMILY Other
REGION Canada	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13-jul-let.aspx

Why it matters

- **Strengthen cybersecurity governance** Enhance oversight by clearly defining responsibilities for technology risk management and ensuring board-level attention to cybersecurity priorities.
- **Enhance regulatory alignment** Support compliance by aligning organizational practices with OSFI requirements and other globally recognized standards tailored to Canada's financial sector.
- **Promote operational resilience** Reduce the risk of business disruptions by requiring robust controls for critical systems, incident response, and ongoing technology risk assessments.
- **Improve third-party risk oversight** Enable organizations to better assess and manage technology risks associated with third-party vendors and service providers.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OSFI B-13

B-13 Requirement Library and Ownership

Organize governance, resilience, and cybersecurity expectations with ownership.

Technology and Cyber Risk Assessments

Run periodic assessments and track treatment plans and approvals.

Operational Resilience Testing Program

Schedule testing, capture results, and manage remediation through closure.

Third-Party and Outsourcing Oversight

Track due diligence, contract controls, and ongoing monitoring evidence.

Incident Response and Recovery Workflows

Run incidents and recovery tasks with documented timelines and outcomes.

Supervisory Reporting Dashboards

Provide leadership-ready reporting on posture, gaps, and remediation status.

Common framework mappings

EU DORA | ISO 27001:2022 | ISO 27002:2022 | ISO 27017 | ISO 27018 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

Canada OSFI B-13 Technology and Cyber Risk Management Guideline

Describes the risk management expectations for technology and cybersecurity in financial institutions.

osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13-jul-let.aspx

Frequently asked questions

What is OSFI B-13 used for?

OSFI B-13 is designed to help federally regulated financial institutions in Canada manage technology and cyber risks. It sets regulatory expectations for governance, risk management, and security controls to protect critical systems and sensitive information.

Is OSFI B-13 mandatory or certifiable?

OSFI B-13 is a mandatory guideline for banks, insurers, and other entities regulated by the Office of the Superintendent of Financial Institutions (OSFI). While it is not a certifiable standard, compliance is subject to regulatory review and audits.

Who does the OSFI B-13 guideline apply to?

B-13 applies to all federally regulated financial institutions in Canada, including banks, insurance companies, and trust companies. Its requirements are relevant to organizations handling critical financial systems and customer data.

What are the key requirements and controls in OSFI B-13?

The guideline emphasizes governance, operational resilience, risk assessment, incident response, third-party management, change management, and ongoing monitoring. It requires institutions to establish internal controls, inventories, and processes for risk identification and mitigation.

How does implementation of OSFI B-13 typically work?

Implementation involves aligning existing information technology and cybersecurity practices with B-13's expectations. This includes conducting regular risk assessments, mapping policies to controls, maintaining compliance evidence, and integrating governance into IT operations.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does OSFI B-13 relate to other cybersecurity frameworks?

OSFI B-13 complements international standards such as NIST and ISO 27001 by providing sector-specific guidance tailored to Canadian financial entities. Organizations often map B-13 requirements to existing controls from these global frameworks to ensure comprehensive coverage.

What are the ongoing compliance requirements for OSFI B-13?

Organizations must maintain a governance structure for continuous monitoring, perform regular technology risk assessments, test incident response plans, and provide evidence of compliance for regulatory audits. Ongoing reporting to senior management and the board is essential for sustained compliance.

How would SmartSuite support OSFI B-13?

SmartSuite enables organizations to manage OSFI B-13 compliance by centralizing risk registers, developing control libraries, and linking policies to controls. It supports evidence collection, facilitates audit readiness with workflow automation, and provides dashboards and reporting tools to streamline governance and demonstrate compliance to regulators and boards.

License included / downloadable: Yes OSFI Guideline B-13 is publicly available through the Office of the Superintendent of Financial Institutions and can be accessed without a commercial license.

Full framework page and mappings: smartsuite.com/frameworks/canada-osfi-b-13-technology-and-cyber-risk-management-guideline