SmartSuite

Framework / Cybersecurity / Other

OSFI B-13 — Technology and Cyber Risk Management Guideline

OSFI Guideline B-13 sets 17 principles in three domains for technology and cyber risk management at Canada's federally regulated financial institutions, effective January 1, 2024.



What it is

OSFI Guideline B-13, Technology and Cyber Risk Management, sets the Office of the Superintendent of Financial Institutions' expectations that every federally regulated financial institution (FRFI) govern technology and cyber risk through clear accountability, run stable and recoverable technology operations, and keep a secure technology posture. It was released on July 13, 2022 and has been effective since January 1, 2024.

OSFI, Canada's federal prudential regulator, publishes it for banks, foreign bank branches, foreign insurance branches, life, property and casualty insurers, and trust and loan companies. It is a guideline of supervisory expectations that OSFI applies in a risk-based way, with 17 principles in three domains: Governance and risk management, Technology operations and resilience, and Cyber security.

At a glance

PUBLISHER
Office of the Superintendent of Financial Institutions (OSFI)

TYPE
Framework

VERSION
Guideline B-13 (July 2022), 17 principles in three domains

EFFECTIVE
January 1, 2024

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Canada

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Why it matters

- **Senior accountability** Senior Management is accountable for technology and cyber security operations and assigns named senior officers, such as the CIO, CTO or CISO (principle 1).
- **A defined risk appetite** The technology and cyber risk management framework sets a risk appetite with limits, thresholds and tolerance levels aligned to enterprise risk management (principle 3).
- **Tested recovery** Institutions run an Enterprise Disaster Recovery Program and test it against severe but plausible scenarios (principles 12 and 13).
- **Intelligence-led testing** Institutions set triggers and minimum frequencies for intelligence-led threat assessments, including penetration testing and red teaming (section 3.1.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OSFI B-13

Principles Library and Ownership

Load the 17 principles in three domains as controls, each with a named senior-officer owner and review date (principle 1).

Technology and Cyber Risk Framework

Track risk appetite measures, the risk taxonomy and risk assessments with treatment plans and approvals (principle 3).

Asset Inventory and Technology Currency

Keep records of technology assets with criticality, configuration baseline and end-of-support dates (principle 5).

Disaster Recovery and Scenario Testing

Schedule disaster recovery tests against severe but plausible scenarios, capture results and track remediation to closure (principles 12 and 13).

Incident Response and OSFI Reporting

Record incidents with classification, severity and timeline, including the 24-hour notice under the OSFI advisory and post-incident reviews (principles 10 and 17).

Third-Party and Supervisory Reporting

Show posture by domain, open gaps and third-party dependencies on a dashboard for Senior Management and for supervisory discussions.

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

Who must follow OSFI Guideline B-13?

All federally regulated financial institutions: banks, foreign bank branches, foreign insurance company branches, life, property and casualty insurers, and trust and loan companies. Branch expectations are set out in Guideline E-4 (section A).

Is B-13 a law or a certifiable standard?

No. It is an OSFI guideline that sets supervisory expectations, to be applied in a risk-based way that reflects an institution's size, complexity and risk profile. There is no certification; OSFI assesses institutions against it through supervision.

How is B-13 organized?

It has 17 principles in three domains: Governance and risk management (principles 1 to 3), Technology operations and resilience (principles 4 to 13), and Cyber security (principles 14 to 17). Each domain states a desired outcome.

When must a technology or cyber incident be reported to OSFI?

OSFI's Technology and Cyber Security Incident Reporting Advisory, updated August 13, 2021, asks federally regulated financial institutions to report to OSFI's Technology Risk Division and their Lead Supervisor within 24 hours, or sooner if possible. B-13 refers institutions to this advisory.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

When did B-13 take effect?

OSFI released the final Guideline on July 13, 2022 and set an effective date of January 1, 2024 to give institutions time to self-assess and prepare. OSFI also publishes a self-assessment tool for the Guideline.

License included / downloadable: Yes Guideline B-13 is published free by the Office of the Superintendent of Financial Institutions and is included with the platform for reference.

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