MARCH 1, 2024 • 7 MIN READ

Understanding B-13: OSFI's guidance on technology and cyber risk management

AUTHORS


Rosalie Jetté


Angela Jiao


Adam S. Armstrong


Molly Reynolds

On January 1, 2024, Canada's Office of the Superintendent of Financial Institutions' (OSFI) new *Guideline B-13 – Technology and Cyber Risk Management* (B-13) came into effect. B-13 establishes OSFI's expectations for how federally regulated financial institutions (FRFIs) should manage technology and cyber risk.

In B-13, OSFI defines technology and cyber risk as the risk arising from any inadequacy, disruption, failure or damage from unauthorized access or use of technology assets, which encompasses any IT failure, data incident or cyber incident. It also includes the risk arising from the people or processes that enable and support business needs as they relate to technology assets. In articulating technology and cyber risk in this way, we believe OSFI perceives technology risk management as a comprehensive, enterprise-wide exercise at both technical and governance levels.

B-13 covers three broad categories of requirements:

- **Governance and risk management** requirements set out the expectations for formal accountability, leadership and organizational structure used to support risk management and oversight of technology.
- **Technology operations and resilience** requirements set out expectations for management and oversight of risks related to the design, implementation, management, and recovery of technology.
- **Cyber security** requirements set out expectations for management and oversight of cyber risk.

B-13 as it relates to additional OSFI measures

As technology and cyber risks intersect with other risk areas, OSFI notes that B-13 should be read and applied in conjunction with other OSFI guidance, tools and supervisory communications, in particular, OSFI *Guideline B-10 (Third-Party Risk Management)* (B-10) and *Guideline E-21 (Operational Risk Management)* (E-21). The following high-level intersections are relevant when reading B-13 alongside other OSFI Guidelines:

- The updated version of B-10, coming into effect May 1, 2024, will apply when the technology asset comes from, or the technology and cyber risk is being managed by, a third-party vendor for the FRFI.
- E-21 aims at mitigating operational risks, which can provide useful insight into the management of operational risks stemming from technology assets, whether proprietary to the FRFI or procured from a third-party vendor.

- The Integrity and Security Guideline (I&S) provides insight for the management of security risks stemming from technology assets, whether proprietary to the FRFI or procured from a third-party vendor.

To assist with the compliance efforts that are required by OSFI, we take a look at the new requirements of B-13 and highlight their interactions with the requirements of other guidelines published by OSFI, while offering some practical insights, in our side-by-side comparison chart.

Download our full side-by-side comparison of B-13 and other overlapping OSFI guidelines.

What does it mean for clients?

FRFIs should review their information technology and cyber security policies, practices and procedures to ensure that they mitigate the technology or cyber risks of their technology in accordance with their risk tolerance, as established in considering B-13. In doing so, they should consider how these policies and procedures can intersect with other risk areas (such as third-party and operational risk management) and how existing processes (e.g., due diligence, risk rating, risk assessments) may be leveraged as part of the compliance efforts for B-13 as well.

Organizations not directly subject to OSFI's Guidelines should also familiarize themselves with B-13 and consider their governance, security, and resilience posture in the face of these guidelines to a) consider how their organization could utilize OSFI's guidelines to improve their policies and contracting practices, and b) where applicable, prepare for contractual negotiations with FRFIs that are required to comply.

Assessing and mitigating risks

The chart, "Key risk management expectations across OSFI guidelines" (available for download below) aims to highlight and align key expectations of OSFI across various guidelines (though not exhaustively). OSFI guidance makes clear that by considering technological, operational and third-party risks together, organizations will ensure that they have the best practices in place to mitigate their technology or cyber risk in a manner that adheres to their overall risk tolerance. This in turn will enable FRFIs to comply with the regulator's expectations.

Practical insights for FRFIs

Governance

Collectively, B-13, B-10 and E-21 all set the expectation that FRFIs will create and implement risk-based frameworks. In recognizing that there is no "one-size-fits-all approach" for managing risks created by technologies, OSFI recognizes that compliance with its guidance will require FRFIs to make numerous risk-based decisions that reflect "the unique risks and vulnerabilities that vary with an FRFI's size, the nature, scope, and complexity of its operations, and risk profile".

Since all four guidelines are intended to help FRFIs consider risk mitigation based on their acceptable, considered risk profile, it makes sense for FRFIs to align all of their policies to a consistent, cohesive risk profile. In applying the guidelines, FRFIs should note that taking an action to mitigate a risk in one area (e.g., B-10) may lessen the overall risk assessment under B-13. FRFIs should determine their risk tolerance as a whole before drafting policies and negotiating third-party agreements.

Assessing risk

In conducting a risk assessment of the relevant technology, FRFIs will need to consider multiple overlapping factors, such as accountability for the management of the technology asset (including, for example, the management of changes, patches and releases), integration of systems, subcontracting, concentration risk of the third party and

technology, cyber security risk, etc.

FRFIs should consider using OSFI's *Cyber Security Self-Assessment* to analyze a technology's cyber risk.

In all cases, the assessment should also be informed by legal and regulatory requirements, as well as industry standards. For example, an artificial intelligence system designated as "high risk" under legislation such as the proposed federal *Artificial Intelligence and Data Act* (AIDA) will likely be considered high risk during a B-13 or B-10 assessment.

Managing risks

All four guidelines mentioned above require that FRFIs mitigate risks created by technology and, if applicable, third-party vendors, by ensuring that there is an operational framework to respond to such risks. In this operational framework, an incident management plan or business continuity plan, for example, should be: 1) adequately and regularly tested to ensure that it is practically workable; 2) preventative and reactive; 3) set out in writing; and 4) responsive to material changes in the arrangement.

All four guidelines mentioned above require that FRFIs manage how material changes are handled. There are a variety of ways to manage changes in practice, such as setting out a detailed change management process, triggering termination grounds or triggering transition service obligations following material changes.

When setting up appropriate processes within the organization, cyber security vulnerabilities are a key consideration. Organizational (e.g., training and awareness, participating in information-sharing amongst industry actors, etc.), technical (extended detection and response tool, 24/7 monitoring, threat hunting, etc.) and legal measures (template contracts, negotiation playbooks, and internal policies) should be included in this respect.

Performance and incident management

FRFIs should ensure that their internal processes and procedures, as well as their vendor arrangements, allow them timely access to accurate and comprehensive information about the performance of their assets and security, such as through technical (e.g., access to systems or logs) or legal measures (e.g., ongoing due diligence, audit rights).

In addition, FRFIs should review their vendors' and their own incident response processes and practices and ensure alignment. They should also ensure that their agreements with third parties include provisions relating to 1) notification, including triggers and deadlines; 2) prompt cooperation, including clear expectations relating to information sharing; 3) oversight over the investigation and mitigation measures, including appropriate escalations; and 4) if applicable, responsibility for notification of individuals whose information may be impacted by the incident, including reporting to relevant authorities, such as to OSFI under the *Technology and Cyber Security Incident Reporting Advisory*.

Download our full side-by-side comparison of B-13 and other overlapping OSFI guidelines.

To discuss these issues, please contact the author(s).