OSFI Guidelines B-10 and B-13

Amendments to Guidelines Related to Foreign Branches

Overview of Amendments to Guidelines B-10 and B-13

On February 22, 2024 the Office of the Superintendent of Financial Institutions (OSFI) published changes to **Guideline B-10: Third-Party Risk Management** and **Guideline B-13: Technology and Cyber Risk Management**.

The changes clarify how these guidelines apply to foreign bank branches and foreign insurance company branches. Both guidelines were amended to clarify that they apply to **foreign bank branches** and **foreign insurance company branches** to the extent it is consistent with applicable requirements and legal obligations related to the branch's business in Canada.

Compliance Dates

Branches are to comply with the Guidelines by the following dates:

February 22, 2024	March 31, 2025
Date that OSFI Guidelines B-10 and B-13 were amended	Date for branches to adhere to Guideline B-10.

The clarification to Guideline B-13 does not change its practical application to branches. Branches should already adhere to Guideline B-13.

Foreign Branches In-Scope of Guideline Amendments

The rule applies to **foreign bank branches** (i.e., foreign banks authorized to conduct business in Canada on a branch basis) **and foreign insurance company branches** (i.e., foreign entities that are authorized to insure in Canada risks on a branch basis).

Regulatory Objectives of Guideline B-10

This Guideline presents six expected outcomes for FRFIs to achieve through managing risks associated with third-party arrangements:

1. Governance and accountability structures will be clear with comprehensive risk management strategies and frameworks in place;
2. Risks posed by third parties will be identified and assessed;
3. Risks posed by third parties will be managed and mitigated within the FRFI's risk appetite framework;
4. Third party performance will be monitored and assessed, and risks and incidents will be proactively addressed;
5. The FRFI's third-party risk management program will allow it to identify and manage its third-party relationships on an ongoing basis;
6. Technology and cyber operations carried out by third parties will be transparent, reliable and secure.

Regulatory Objectives of Guideline B-13

This Guideline presents three expected outcomes for FRFIs to achieve through technology and cyber risk management:

1. Technology and cyber risks will be governed through clear accountabilities and structures, and comprehensive strategies and frameworks;
2. Technology environment will be stable, scalable and resilient by keeping the environment current and supported by robust processes;
3. Secure technology environment that maintains the confidentiality, integrity and availability of the FRFI's technology assets.

OSFI Guideline B-10

Third-Party Risk Management Requirements

This Guideline sets out OSFI's principal-based expectations for federally regulated financial institutions (FRFIs) to manage risks associated with their third-party arrangements. OSFI affirms that the FRFI retains accountability for its business activities, functions and services outsourced to a third party. The Guideline is applicable to all FRFIs including foreign bank branches and foreign insurance company branches.

FRFI Requirements on Third-Party Risk Management

Topics	FRFI Requirements
Governance	• Manage the risks arising from all types of third-party arrangements; • Establish a third-party risk management framework that sets out clear accountabilities, policies and procedures for identifying, managing, mitigating, and reporting on risks relating to the use of third parties.
Management of third-party risk: Risk identification & assessment	• Identify and assess the risks of a third-party arrangement before entering the arrangement and periodically thereafter. Risk assessments should be proportionate to the criticality of an arrangement; • Undertake due diligence prior to entering contracts or other forms of arrangement with a third party, and on an ongoing basis proportionate to the level of risk and criticality of the arrangement; • Identify, monitor and manage risks from the subcontracting arrangements undertaken by third parties.
Management of third-party risk: Risk management & mitigation	• Enter into written arrangements that set out the rights and responsibilities of each party; • Both the FRFI and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data; • The third-party arrangements should allow timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks, including right for an independent audit; • The agreement with the third party should include the ability to deliver operations through disruption, including the maintenance, testing, and activation of business continuity and disaster recovery plans.
Management of third-party risk: Risk monitoring & reporting	• Monitor the third-party arrangements to verify they are meeting obligations and effectively managing risks; • Both the FRFI and its third-party should have documented processes in place to effectively identify, investigate, escalate, track, and remediate incidents.
Special arrangements	• Identify and manage a range of third-party relationships on an ongoing basis including relationships bound by standardized contracts with pre-defined terms and conditions, and those with no written contract. FRFI is also to ensure that the external auditor is independent of the third-party;
Technology and cyber risk in third-party arrangements	• Consider additional controls to manage technology and cyber risks such as developing cloud-specific requirements and considering cloud portability when entering an arrangement with a cloud service provider. Also establish clear roles and responsibilities between the FRFI and the third-party.

OSFI Guideline B-13

Technology and Cyber Risk Management Requirements

This Guideline sets out OSFI's principal-based expectations related to technology and cyber risk management of federally regulated financial institutions (FRFIs). OSFI maintains that the Guideline should be implemented from a risk-based perspective as there is no one-size-fits-all approach for managing technology and cyber risks given the unique risks and vulnerabilities that vary with a FRFIs' size, complexity of its operations, and risk profile. It's applicable to all FRFIs including foreign bank branches and foreign insurance company branches.

FRFI Requirements on Technology & Cyber Risk Management

Topics	FRFI Requirements
Governance and risk management	• Senior Management should assign responsibility for managing technology and cyber risks to senior officers. It should also ensure an appropriate organizational structure and adequate resourcing are in place for managing technology and cyber risks across the enterprise; • Implement a strategic technology and cyber plan(s). The plan(s) should align to business strategy and set goals and objectives that are measurable and evolve with changes in technology and the cyber environment; • Establish a technology and cyber risk management framework (RMF) which defines risk appetite and establishes the FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.
Technology operations and resilience	• Implement a technology architecture framework to ensure solutions are built in line with requirements; • Maintain an updated inventory of all technology assets supporting business functions which includes asset classification, and monitoring of technology currency where there is to be safe disposal of assets at the end of their life cycle; • Establish processes to govern and manage technology projects to ensure project outcomes meet business objectives; • Implement a System Development Life Cycle framework for development, acquisition and maintenance of its technology; • Establish a technology change and release management process that minimizes disruption to the production environment; • Implement patch management processes to address vulnerabilities and flaws; • Effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts; • Develop service and capacity standards and processes to monitor operational management of technology; • Establish and maintain an Enterprise Disaster Recovery Program (EDRP) to deliver technology services through disruption; • Perform scenario testing on disaster recovery capabilities to confirm technology operates as expected through disruption.
Cyber security	• Maintain a range of practices, capabilities, processes and tools to identify and assess cyber security weaknesses that could be exploited; • Maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets; • Maintain continuous security detection capabilities to enable monitoring, alerting and forensic investigations; • Respond to, contain, recover and learn from cyber security incidents impacting technology assets or third-party providers.

OSFI Guidelines B-10 and B-13

Botsford Team Contacts

For additional information about this Regulatory brief or Botsford Associates Financial Services Regulatory Practice, and how we can help you, please contact:

Jon Block
Managing Partner
Financial Services
NYC: 917.647.3434 / TOR: 416.915.0438
jblock@botsford.com

Andrew Moreira
Managing Director - Consulting
Financial Services
NYC: 917.722.0939 / TOR: 647.361.4404
amoreira@botsford.com

Gordon Wong
Managing Director - Advisory
Financial Services
NYC: 917.722.1200 ext 319 / TOR: 437.253.4933
gwong@botsford.com