Prevalent™

A Checklist for Office of the Superintendent of Financial Institutions (OSFI) of Canada Guideline B-13 Compliance

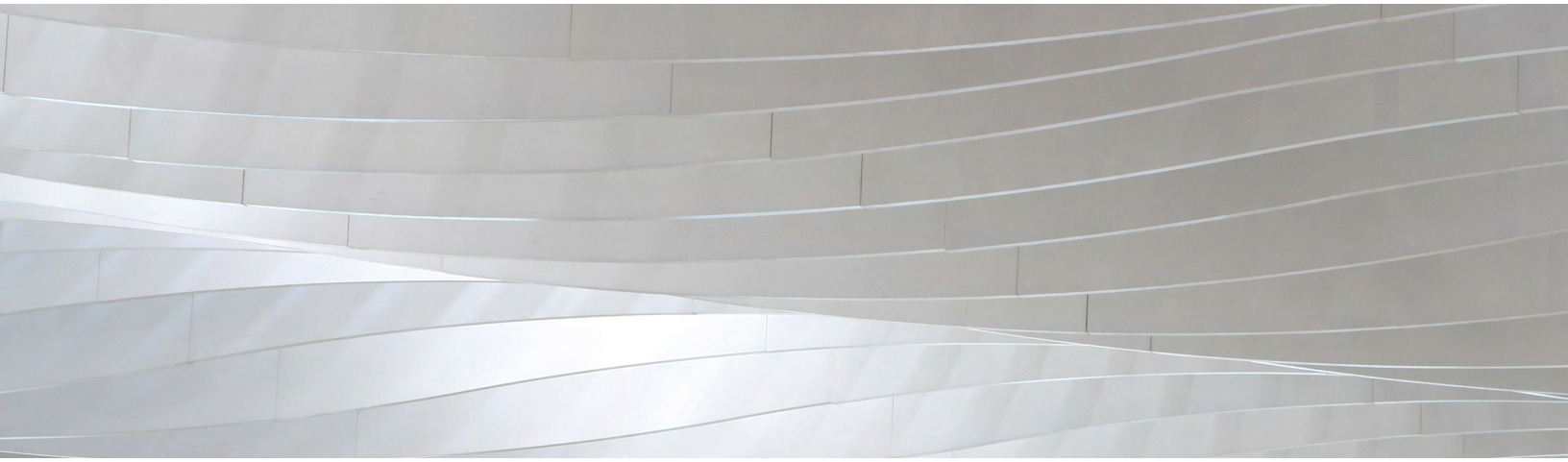
OSFI Guideline B-13 & Third-Party Risk Management

Table of Contents

OSFI Guideline B-13 and Third-Party Risk Management

OSFI B-13 is a guideline issued by the Office of the Superintendent of Financial Institutions (OSFI) in Canada that outlines risk management requirements for developing greater resilience to technology and cyber risks – including those posed by third parties. Similar to Guideline B-10, which addresses third-party outsourcing, Guideline B-13 is applicable to all federally regulated financial institutions (known as FRFIs), including foreign bank branches and foreign insurance company branches operating in Canada.

This document examines the third-party risk management requirements in OSFI Guideline B-13 and identifies best practices for addressing them.



OSFI Principles At-a-Glance

Originally issued in July 2022, Guideline B-13 is organized into three domains, Governance and Risk Management, Technology Operations and Resilience, and Cybersecurity. Each domain has a desired outcome that contributes to resilience against technology and cyber risks. Outcomes are supported by 17 Principles which in turn are supported by individual guidelines.

Domain 1: Governance and Risk Management

Principle 1: 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 FRFI.

Principle 2: FRFIs should define, document, approve and 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 the FRFI's technology and cyber environment.

Principle 3: FRFIs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.

Domain 2: Technology Operations and Resilience

Principle 4: FRFIs should implement a technology architecture framework, with supporting processes to ensure solutions are built in line with business, technology, and security requirements.

Principle 5: FRFIs should maintain an updated inventory of all technology assets supporting business processes or functions. FRFI's asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency.

Principle 6: Effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within the FRFI's risk appetite.

Principle 7: FRFIs should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support of business objectives.

Principle 8: FRFIs should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.

Principle 9: FRFIs should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws.

Principle 10: FRFIs should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts.

Principle 11: FRFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.

Principle 12: FRFIs should establish and maintain an Enterprise Disaster Recovery Program (EDRP) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

Principle 13: FRFIs should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected through disruption.

Domain 3: Cybersecurity

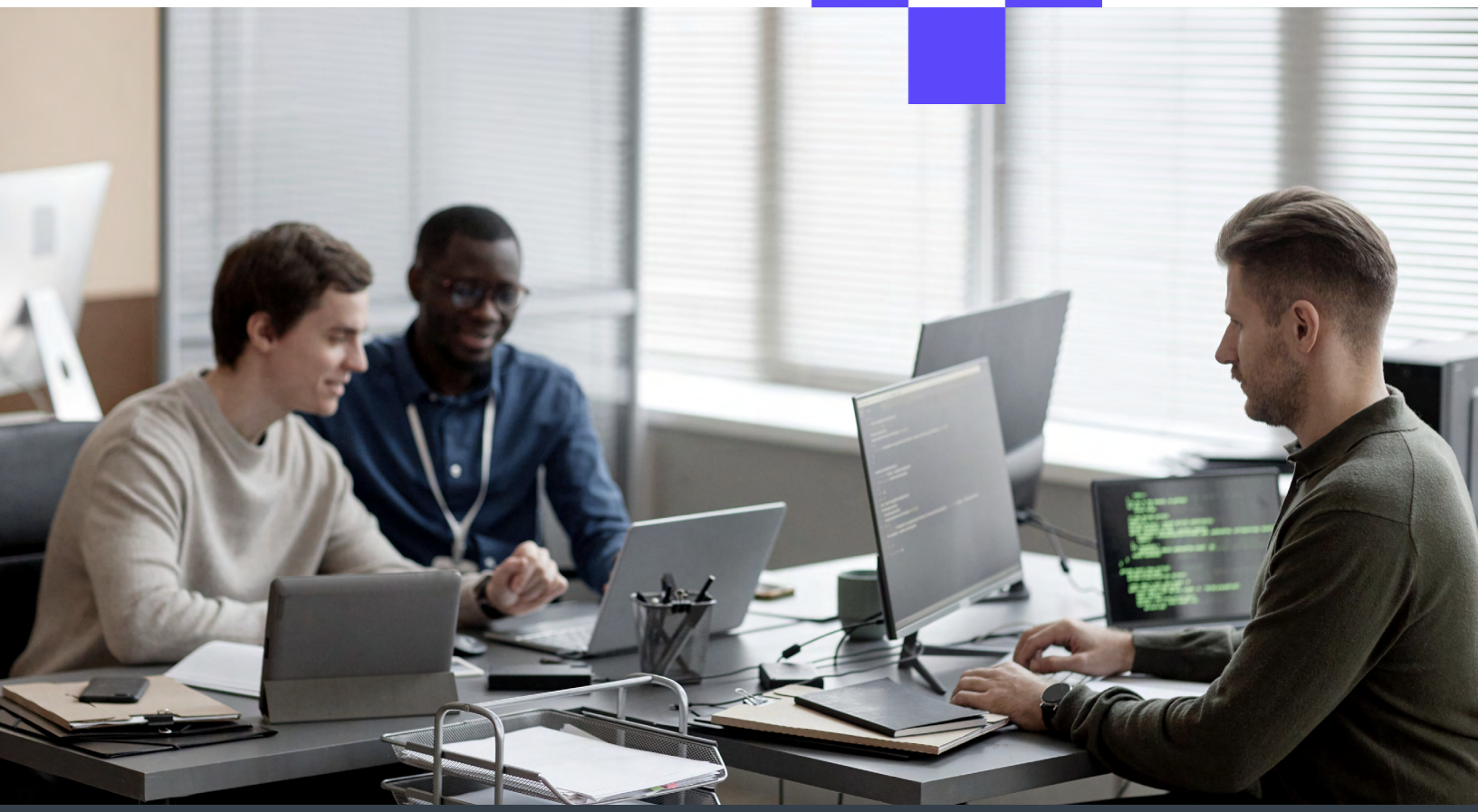
Principle 14: FRFIs should maintain a range of practices, capabilities, processes and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors.

Principle 15: FRFIs should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets.

Principle 16: FRFIs design, implement and maintain continuous security detection capabilities to enable monitoring, alerting and forensic investigations.

Principle 17: FRFIs should respond to, contain, recover and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.

Although all Principles are essential for FRFIs to adhere to, not every Principle carries a strong third-party association with it. The next section of this paper examines those Principles with strong third-party risk management requirements.



OSFI B-13 and Third-Party Risk Management Compliance

When it comes to third-party risk management, Guideline B-13 emphasizes the need for financial institutions to implement comprehensive strategies to manage risks associated with outsourcing and third-party relationships. The table below summarizes the third-party risk management-specific guidelines in B-13 and provides best practice recommendations to address the requirements.

NOTE: *This table summarizes only third-party risk-specific requirements. For a full list of all requirements and all Principles, please consult the complete OSFI guideline.*

OSFI B-13 Principles	TPRM Best Practices
Domain 1: Governance and risk management This domain sets OSFI's expectations for the formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. **Outcome:** Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.	
Principle 1: 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 FRFI. **Principle 2:** FRFIs should define, document, approve and 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 the FRFI's technology and cyber environment.	Seek out experts to collaborate with your team on defining and implementing TPRM processes in the context of your overall risk management approach; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence to termination and offboarding. As part of this process, define: • Clear roles and responsibilities (e.g., RACI). • Third-party inventories. • Risk scoring and thresholds based on your organization's risk tolerance. • Assessment and monitoring methodologies based on third-party criticality. • Fourth-party mapping to understand risk in your extended vendor ecosystem. • Sources of continuous monitoring data (cyber, business, reputational, financial). • Key performance indicators (KPIs) and key risk indicators (KRIs). • Governing policies, standards, systems and processes to protect data. • Compliance and contractual reporting requirements against service levels. • Incident response requirements. • Risk and internal stakeholder reporting. • Risk mitigation and remediation strategies.

OSFI B-13 Principles	TPRM Best Practices
Principle 3: FRFIs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.	See out a risk management solution that features a large library of framework-specific risk assessments – such as ISO, NIST, or others. Leverage pre-built, framework-specific risk assessments to simplify controls mapping and reporting. A chosen framework should align with enterprise-level risk management requirements.
Domain 2: Technology operations and resilience This domain sets OSFI's expectations for "management and oversight of risks related to the design, implementation, management and recovery of technology assets and services. **Outcome:** A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable technology operating and recovery processes.	
Principle 7: FRFIs should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition, and maintenance of technology systems that perform as expected in support of business objectives.	As part of the due diligence process, require vendors to provide updated software bills of materials (SBOMs) for their software products. This will help you identify any potential vulnerabilities or licensing issues that may impact your organization's security and compliance posture.

OSFI B-13 Principles	TPRM Best Practices
Principle 10: FRFIs should effectively detect, log, manage, resolve, monitor, and report on technology incidents and minimize impacts.	Continuously track and analyze external threats to third parties. As part of this, monitor the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. Monitoring sources should include: • Criminal forums; onion pages; dark web special access forums; threat feeds; and paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. • Databases containing several years of data breach history for thousands of companies around the world. All monitoring data should be correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, remediation, and any response initiatives. Once all assessment and monitoring data is correlated into a central risk register, apply risk scoring and prioritization according to a likelihood and impact model. This model should frame risks into a matrix, so you can easily see the highest impact risks and can prioritize remediation efforts on those. Assign owners and track risks and remediations to a level acceptable to the business.
Principle 11: FRFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.	Continually evaluate the effectiveness of your TPRM program according to changing business needs and priorities, measuring third-party vendor key performance indicators (KPIs) and key risk indicators (KRIs) through the third-party relationship lifecycle.

OSFI B-13 Principles	TPRM Best Practices
Domain 3: Cybersecurity This domain sets OSFI's expectations for "management and oversight of cyber risk. **Outcome:** A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets.	
Principle 14: FRFIs should maintain a range of practices, capabilities, processes and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors.	Look for solutions that feature a large library of pre-built templates for third-party risk assessments. Assessments should be conducted at the time of supplier onboarding, contract renewal, or at any required frequency (e.g., quarterly or annually) depending on material changes in the relationship. Assessments should be managed centrally and be backed by workflow, task management and automated evidence review capabilities to ensure that your team has visibility into third-party risks throughout the relationship lifecycle. Importantly, a TPRM solution should include built-in remediation recommendations based on risk assessment results to ensure that your third parties address risks in a timely and satisfactory manner and can provide the appropriate evidence to auditors. As part of this process, continuously track and analyze external threats to third parties. All monitoring data should be correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, remediation and response initiatives.

OSFI B-13 Principles	TPRM Best Practices
Principle 17: FRFIs should respond to, contain, recover and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.	As part of your broader incident management strategy ensure that your third-party incident response program enables your team to rapidly identify, respond to, report on, and mitigate the impact of third-party vendor security incidents. Key capabilities in a third-party incident response service should include: • Continuously updated and customizable event and incident management questionnaires. • Real-time questionnaire completion progress tracking. • Defined risk owners with automated chasing reminders to keep surveys on schedule. • Proactive vendor reporting. • Consolidated views of risk ratings, counts, scores and flagged responses for each vendor. • Workflow rules to trigger automated playbooks to act on risks according to their potential impact on the business. • Built-in reporting templates for internal and external stakeholders. • Guidance from built-in remediation recommendations to reduce risk. • Data and relationship mapping to identify relationships between your organization and third, fourth or Nth parties to visualize information paths and reveal at-risk data. Also, consider leveraging databases that contain several years of data breach history for thousands of companies around the world – including types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications. Armed with these insights, your team can better understand the scope and impact of the incident; what data was involved; whether the third party's operations were impacted; and when remediations have been completed – all by leveraging experts.

Best Practices for Addressing Guideline OSFI B-13 Requirements

Guideline B-13 requirements are part of a broader framework aimed at ensuring that financial institutions manage technology and cyber risk effectively, especially in a landscape where third-party services are increasingly used. Start your journey to compliance with these practices:

Due Diligence

Conduct thorough pre-contract due diligence before entering into relationships with third parties. This includes assessing the third party's financial stability, reputation, and the adequacy of their cybersecurity measures.

Third-Party Contracts

Include specific terms in third-party contracts that address technology and cyber risk. This includes clauses related to data protection, the right to audit, adherence to key performance indicators and key risk thresholds, and incident response requirements.

Risk Assessments

Conduct regular risk assessments to understand the potential risks that third parties may pose, particularly related to technology and cybersecurity. This should include an assessment of how third parties handle data and the potential impact of disruptions or data breaches.

Monitoring and Reporting

Continuously monitor for cyber risks, third-party performance and adherence to contractual agreements. They should have processes in place to report and address any issues or data breaches promptly.

Incident Management and Response

Ensure that third parties have adequate incident management and response plans. This includes clear communication channels and protocols for responding to cyber incidents.

Business Continuity and Contingency Planning

Confirm that third parties have robust business continuity plans in place that align with the institution's own contingency plans. This helps to maintain the continuity of critical services in the event of disruptions.

Termination and Exit Strategies

Establish clear strategies and procedures for terminating third-party relationships and ensuring a smooth transition without compromising security or service continuity.

How Prevalent Helps OSFI B-13 Compliance

OSFI Guideline B-13 provides a comprehensive framework for ensuring resilience against technology and cyber risks – including those posed by third parties. Prevalent can help organizations automate the assessment and continuous monitoring of third-party business resilience to support compliance and conformity with OSFI Guideline B-13.

The Prevalent Third-Party Risk Management Platform:

- Delivers comprehensive pre-contract due diligence assessments of business resilience practices.
- Simplifies contracting processes to ensure all business resilience key performance indicators (KPIs) are in place and tracked.
- Automates incident response process, speeding time to resolution.
- Includes compliance and risk reporting by framework or regulation.
- Delivers a prescriptive offboarding process to ensure secure contract termination.
- Adds workflow to automate the risk assessment,risk scoring, and risk remediation process.
- Continuously monitors third parties for cyber, business, reputational, and financial risk monitoring to correlate risks against assessment results and validate finding.

For more on how Prevalent can help your team address the requirements set forth in OSFI Guideline B-13, request a demo today.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers across every step of the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.