Prevalent™

A Checklist for Office of the Superintendent of Financial Institutions (OSFI) of Canada Guideline B-10 Compliance

OSFI Guideline B-10 & Third-Party Risk Management

Table of Contents

OSFI & Third-Party Risk Management

In April 2022, the Canadian Government Office of the Superintendent of Financial Institutions (OSFI) issued a draft of Third-Party Risk Management Guideline B-10, which addresses the operational and financial risks associated with vendor and supplier relationships.

Guideline B-10 sets expectations for federally regulated financial institutions (FRFIs) to manage risks associated with third-party arrangements. It is applicable to all FRFIs, except for foreign bank branches and foreign insurance company branches. The Guideline states:

> *"The Office of the Superintendent of Financial Institutions (OSFI) expects that FRFIs practice effective risk management and retain ultimate accountability for all their business activities, functions, and services, whether they are performed in-house or through a third-party arrangement.*
>
> *"To that end, FRFIs are required to provide to OSFI, upon request, information related to their business and strategic arrangements with third parties, risk management, and control environments, to support supervisory monitoring and review work. OSFI expects to be promptly notified of substantive issues affecting the soundness of the FRFI due to a third-party arrangement."*

The guideline also expands the definition of a third party to include more entities like independent professionals, brokers, and utilities, and recommends including all types of third parties in risk assessments.

Driving these new requirements is the shift from materiality to criticality – where a third party performs a function that is integral to the FRFI's provision of a significant operation, function or service, requiring a dual-pronged approach where risk and criticality inform the nature and extent of due diligence activities.

This document examines the third-party risk management requirements in OSFI Guideline B10 and identifies capabilities in the Prevalent Third-Party Risk Management Platform that can address the requirements.

Five Expected Outcomes

Guideline B-10 presents five expected outcomes for FRFIs to achieve through managing third-party risk. These outcomes are meant to contribute to the FRFI's operational and financial resilience and help safeguard its reputation. Integrating contract lifecycle management systems with existing risk and procurement solutions will support contracting requirements such as rights and responsibilities of each party throughout its lifecycle, as expected by OSFI.

1	**Governance and accountability structures are clear with comprehensive risk management strategies and frameworks in place to contribute to ongoing operational and financial resilience.**
2	**Risks posed by third parties are identified and assessed.**
3	**Risks posed by third parties are managed and mitigated within the FRFI's risk appetite framework.**
4	**Third party performance is continually monitored and assess, and risk and incidents are proactively addressed.**
5	**The FRFI's risk management program is dynamic and actively captures and appropriately manages a range of third-party relationships and interactions.**

Five expected outcomes for FRFIs to achieve through managing third-party risk. Graphic adapted from OSFI Guideline B-10.

Mapping Prevalent Capabilities to OSFI Guideline B-10 Principles

Supporting the five expected outcomes are 11 principles that OSFI describes as best practices for third-party risk management. The summary table below maps Prevalent Third-Party Risk Management Platform capabilities to these 11 principles.

NOTE: This table should not be considered comprehensive, definitive guidance. Consult your auditor for a complete list of requirements.

Table 1. Prevalent Mappings to OSFI Guideline B-10 Principles

OSFI B-10 Principles	How Prevalent Helps
Outcome 1: Governance and accountability structures are clear with comprehensive risk strategies and frameworks in place to contribute to ongoing operational and financial resilience.	
Principle 1: "The FRFI is ultimately accountable for all business activities, functions, and services outsourced to third parties and for managing the risks related to third-party arrangements." **Principle 2:** "The FRFI should establish a third-party risk management framework (TPRMF) that sets out clear accountabilities, responsibilities, policies, and processes for identifying, managing, mitigating, monitoring, and reporting on risks relating to the use of third parties."	Prevalent partners with you to build a comprehensive third-party risk management (TPRM) program based on proven best practices and extensive real-world experience. Our experts collaborate with your team on defining and implementing TPRM processes and solutions; 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, Prevalent can help you 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 • 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-10 Principles	How Prevalent Helps
Outcome 2: Risks posed by third parties are identified and assessed.	
Principle 3: "Before entering a third-party arrangement—and, periodically thereafter, proportionate to the level of risk and criticality of the arrangement—the FRFI should identify and assess the risks of the arrangement. Specifically, the FRFI should conduct risk assessments to decide on third-party selection; (re)assess the risk and criticality of the arrangement; and plan for adequate risk mitigation and oversight."	Prevalent centralizes and automates the distribution, comparison, and management of requests for proposals (RFPs) and requests for information (RFIs). Our solutions also deliver business, reputational, financial, and data breach risk insights to inform and add context to vendor selection decisions. Prevalent moves each selected vendor into contracting and/or onboarding due diligence phases, automatically progressing them through the third-party lifecycle. Prevalent features a library of more than 100 pre-built templates for ongoing third-party risk assessments. These are integrated with native cyber, business, reputational, and financial risk monitoring capabilities, which continuously validate assessment findings and fill gaps between assessments. Built-in remediation recommendations ensure that third parties address risks in a timely and satisfactory manner.
Principle 4: "The FRFI should 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."	Prevalent offers a pre-contract due diligence assessment with clear scoring based on eight criteria to capture, track and quantify inherent risks for all third parties. Criteria includes: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation Using the inherent risk assessment, you can automatically tier suppliers; set appropriate levels of further diligence; and scope of ongoing assessments. Rule-based tiering logic enables vendor categorization using a range of data interaction, financial, regulatory and reputational considerations. Prevalent features a library of more than 100 pre-built templates for third-party risk assessments. Assessments can be conducted at the time of contract renewal or at any required frequency (e.g., quarterly or annually). Assessment questionnaires can be globally focused or regional to address unique legal or operational requirements. Prevalent delivers remediation recommendations based on assessment results. These are backed by workflow and task management capabilities to ensure that third parties address risks in a timely and satisfactory manner. Integrated, native cyber, business, reputational, and financial risk monitoring capabilities flag material changes between periodic assessments and can trigger notifications, follow-up assessments, or other actions.

OSFI B-10 Principles	How Prevalent Helps
Principle 5: "The FRFI should assess, manage, and monitor the risks of subcontracting arrangements entered by third parties, including the impact of these arrangements on concentration risk."	Prevalent can identify fourth-party and Nth-party subcontracting relationships by conducting a questionnaire-based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk. Suppliers discovered through this process are continuously monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening. This approach provides insights to address potential technology or geographic concentration risk.
Outcome 3: Risks posed by third parties are managed and mitigated within the FRFI's Risk Appetite Framework.	
Principle 6: "The FRFI should enter into written arrangements that set out the rights and responsibilities of each party."	Prevalent centralizes the distribution, discussion, retention, and review of vendor contracts. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. Key capabilities include: • Centralized tracking of all contracts and contract attributes such as type, key dates, value, reminders, and status – with customized, role-based views • Workflow capabilities (based on user or contract type) to automate the contract management lifecycle • Automated reminders and overdue notices to streamline contract review • Centralized contract discussion and comment tracking • Contract and document storage with role-based permissions and audit trails of all access • Version control tracking that supports offline contract and document edits • Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access

OSFI B-10 Principles	How Prevalent Helps
Principle 7: "Throughout the duration of the third-party arrangement, the FRFI and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data."	Prevalent delivers a centralized, collaborative platform for conducting privacy assessments and mitigating both third-party and internal privacy risks. Key data security and privacy assessment capabilities include: • Scheduled assessments and relationship mapping to reveal where personal data exists, where it is shared, and who has access – all summarized in a risk register that highlights critical exposures • Privacy Impact Assessments to uncover at-risk business data and personally identifiable information (PII) • Vendor assessments against GDPR and other privacy regulations via the Prevalent Compliance Framework (PCF) – reveals potential hot spots by mapping identified risks to specific controls • GDPR risk and response mapping to controls, includes percent-compliance ratings and stakeholder-specific reports • A database containing 10+ years of data breach history for thousands of companies – includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications • Centralized onboarding, distribution, discussion, retention, and review of vendor contracts – ensures that data protection provisions are enforced from the beginning of the relationship
Principle 8: "The FRFI's third-party arrangements should allow the FRFI timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks. The FRFI should also have the right to conduct or commission an independent audit of a third party."	With Prevalent, auditors can establish a program to efficiently achieve and demonstrate compliance. The solution automates third-party risk management compliance auditing by collecting vendor risk information, quantifying risks, recommending remediations, and generating reports for dozens of government regulations and industry frameworks. Prevalent automatically maps information gathered from control-based assessments to ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, SOX, NYDFS, and other regulatory frameworks, enabling you to quickly visualize and address important compliance requirements.

OSFI B-10 Principles	How Prevalent Helps
Principle 9: "The FRFI's agreement with the third party should encompass the ability to deliver operations through a disruption, including the maintenance, testing, and activation of business continuity and disaster recovery plans. The FRFI should have contingency plans for its critical third-party arrangements."	Prevalent automates the assessment, continuous monitoring, analysis, and remediation of third-party business resilience and continuity – while automatically mapping results to NIST, ISO, and other control frameworks. To complement business resilience assessments and validate results, Prevalent: • Automates continuous cyber monitoring that may predict possible third-party business impacts. • Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability. • Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns. This proactive approach enables your organization to minimize the impact of third-party disruptions and stay on top of compliance requirements. The Prevalent Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: • Categorize suppliers according to their risk profile and criticality to the business. • Outline recovery point objectives (RPOs) and recovery time objectives (RTOs). • Centralize system inventory, risk assessments, RACI charts, and third parties. • Ensure consistent communications with suppliers during business disruptions. When a termination or exit is required for critical services, Prevalent leverages customizable surveys and workflows to report on system access, data destruction, access management, compliance with relevant laws, final payments, and more. The solution also suggests actions based on answers to offboarding assessments and routes tasks to reviewers as necessary.

OSFI B-10 Principles	How Prevalent Helps
Outcome 4: Third-party performance is continually monitored and assessed, and risks and incidents are proactively addressed.	
Principle 10: "The FRFI should monitor its third-party arrangements to verify the third party's ability to continue to meet its obligations and effectively manage risks."	Prevalent continuously tracks and analyzes external threats to third parties. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. All monitoring data is correlated to assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting and response initiatives. Monitoring sources include: • 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases covering 550,000 companies • A database containing 10+ years of data breach history for thousands of companies around the world • 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, operational updates, and more • A global network of 2 million businesses with 5 years of organizational changes and financial performance, including turnover, profit and loss, shareholder funds, etc. • 30,000 global news sources • A database containing over 1.8 million politically exposed person profiles • Global sanctions lists and over 1,000 global enforcement lists and court filings
Principle 11: "Both the FRFI and its third-party should have documented processes in place to effectively identify, investigate, escalate, track, and remediate incidents to ensure ongoing operational and financial resilience and maintain risk levels within the FRFI's risk appetite."	Prevalent enables your team to rapidly identify and mitigate the impact of third-party vendor incidents by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.

OSFI B-10 Principles	How Prevalent Helps
Outcome 4: The FRFI's risk management program is dynamic and actively captures and appropriately manages a range of third-party arrangements and interactions.	
Results from the Prevalent inherent risk assessment enables you to tier suppliers, set appropriate levels of further diligence, and determine the frequency and scope of subsequent assessments. Rule-based tiering logic enables vendor categorization based on a range of data interaction, financial, regulatory and reputational considerations. Rules apply to all third parties, regardless of contract status. You can also continuously monitor non-contract vendors against cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information to catch potential problems before they escalate.	

The Prevalent Difference

Prevalent can help organizations automate the assessment and continuous monitoring of third-party business and financial resilience to support compliance and conformity with OSFI Guideline B-10. The Prevalent Third-Party Risk Management Platform:

- Automates and adds business resilience risk intelligence to vendor selection decisions.
- Delivers comprehensive pre-contract due diligence assessments to calculate inherent risk.
- Simplifies contracting processes to ensure all business resilience key performance indicators (KPIs) are in place and tracked.
- Profiles and tiers all third parties, right-sizing ongoing due diligence according to criticality.
- Maps fourth parties to understand risk among subcontractors.
- Adds workflow to automate the assessment, risk scoring and remediation process.
- Continuously monitors third parties for cyber, business, reputational and financial risk monitoring to correlate risks against assessment results and validate findings.
- Automates incident response process, speeding time to resolution.
- Includes compliance and risk reporting by framework or regulation.
- Delivers a foundation for an agile third-party risk management program.

For more on how Prevalent can help address the requirements set forth in OSFI Guideline B-10, 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 throughout 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.

© Prevalent, Inc. All rights reserved. The Prevalent name and logo are trademarks or registered trademarks of Prevalent, Inc. All other trademarks are the property of their respective owners.