OSFI
BSIF

WHITEPAPER

Navigating OSFI Risk Compliance

A How-To Guide for Canadian Businesses

JULY 2023

TABLE OF CONTENTS

What Is the OSFI?

The Office of the Superintendent of Financial Institutions, (OSFI) or also referred to as OSFI-BSIF, is an independent federal agency in Canada. Established in 1987, the agency emerged when the Department of Insurance (DOI) and the Office of the Inspector General of Banks (OIGB) merged.

Today, the Office of the Superintendent of Financial Institutions plays an essential role in the stability and security of the Canadian financial system. In fact, the agency was designed to help promote public confidence in the Canadian financial system.

The OSFI is the only agency in Canada that supervises and oversees federally regulated financial institutions including, foreign branch banks, insurance companies, cooperative credit associations, life and fraternal benefit societies, deposit-taking institutions, property, and casualty companies, and federally incorporated or registered trust and loan companies.

What Does the OSFI Have to Do with Risk Management in Canada?

One of the essential functions of the OSFI is implementing risk management guidelines for Canada's financial institutions. The agency ensures that the following processes are being met:

- ✓ Current and emerging risks are identified.
- ✓ Risk assessment and measurement systems are developed.
- ✓ Policies, practices, and other control strategies to manage risks are established.

There are several types of risk that the agency plays a role in. These include:

Climate Risk Management

The OSFI works hard to evaluate, detect, and assess new and emerging climate risks that could affect federally regulated institutions. This could mean anything from a public health crisis that affects the economy to new technology threats.

Cyber Risk Management

Cyber security is another area of risk that the OSFI regulates. The agency assesses and evaluates new and emerging cyber threats to help ensure that a financial institution's technology operations meet the industry standard for preventing such risks.

These responsibilities help Canadians stay rest assured that the financial system is safe and secure, giving them the confidence to trust the country's institutions.

Third-Party Risk Management

Federally regulated financial institutions and entities use, and outsource to, third-party businesses or individuals for products, services, and more. Although third parties are essential to making any company or organization function properly, they come with related risks.

The OSFI expects institutions in the Canadian financial sector to manage the potential risks associated with third parties. However, to ensure third-party risk management, OSFI requires federally regulated financial institutions to provide information on their arrangements with third parties, including risk management strategies.

What Are the Risk Management Responsibilities of the OSFI?

The OSFI has several responsibilities that help the agency ensure Canada's financial sector remains safe and secure. Some of the agency's roles and responsibilities include:

Establishing Guidelines

The Office of the Superintendent of Financial Institutions publishes guidelines, or best practices, that it requires federally regulated financial institutions to follow. These guidelines are considered best practice for financial institutions to adhere to, and in some cases, it's required that institutions meet the qualifications.

The agency constantly creates new frameworks, guidelines, and regulations that federally regulated financial institutions must follow. These new guidelines are based on many factors affecting Canada's financial system, including climate-related and cyber risks.

Implementing Risk Management

As mentioned above, the Office of the Superintendent of Financial Institutions works to reduce the risk in the country's financial institutions. The agency sets forth criteria for risk assessment and establishes policies to monitor risks. Numerous types of risks can affect financial institutions.

How Are OSFI Risk Management Frameworks Created?

One of the agency's responsibilities is to advance and administer a regulatory framework to promote risk management. Have you ever wondered how OSFI regulations and requirements are developed?

The Office of the Superintendent of Financial Institutions reviews legislation and analyzes risks to predict the scenarios banks and other entities in Canada may face.

Learning about the risks that other countries are experiencing helps the agency determine its own frameworks. Therefore, when developing new policies and regulations for Canadian financial institutions, the OSFI considers international organizations.

Some international organizations it exchanges information with include the Financial Stability Board, the International Association of Insurance Supervisors, and the Basel Committee on Banking Supervision.

Since the risks in Canada and worldwide are constantly evolving, the OSFI is always creating new regulations and frameworks to help improve risk management.

Federally regulated financial institutions should stay on top of new and updated frameworks to ensure that their business meets regulations and best practices. Adhering to the regulations the OSFI releases also helps ensure the chances of success among these institutions.

How Does the OSFI Regulate Compliance?

To act as a financial stability board, the Office of the Superintendent of Financial Institutions must create guidelines and regulations for federally regulated institutions to adhere to. But how does it do this?

The OSFI process works in several ways to regulate the Canadian banking and financial institution system. It operates by developing rules and guidelines. It also ensures that new accounting, actuarial, and auditing standards are being met to reduce operational risk.

Additionally, the OSFI assesses, analyzes, and evaluates various types of risk that may affect institutions in the country's financial industry. It determines how everything from greenhouse emissions and public health crises to cyber risks and new technologies could impact institutions. It then develops regulations and frameworks to ensure that financial institutions can change their strategies, policies, and methods to prepare for various risks.

OSFI Guideline B-10: How to Best Achieve Compliance

The cyber threat landscape is constantly evolving. To advise federally regulated financial institutions on how to manage cybersecurity, OSFI released Guideline B-10 in May 2023. The new provision sets clear expectations on how to manage cybersecurity pratices and ensure programs comply with current best practices.

What Are the New Guideline Recommendations?

In May 2023, the Office of the Superintendent of Financial Institutions (OSFI) released its updated B-10 guidelines, reinforcing the requirements for third-party risk management in the financial sector. There are several key aspects that the organization needs to consider aligning with the new requirements. These include:

Enhanced Due Diligence
Federally regulated financial institutions must strengthen their due diligence processes when selecting and assessing third-party service providers. This includes evaluating provider's financial health, security controls, and business continuity plans.

How RiskRecon by Mastercard can help:
RiskRecon enables users to effectively evaluate the security controls of all potential vendors, facilitates a thorough scan upon selection then continues to monitor vendors in alignment to risk programs of each OSFI organization. Additionally, using RiskRecon in conjunction with a comprehensive questionnaire helps to better identify business continuity plans and the assets that support them. For example, if an organization claims they have a geographically diverse redundant system, with disparate hosts and providers, this would be easily verified in RiskRecon using our IT Profile resources.

Ongoing Monitoring
Regular monitoring and reassessment of third-party providers are critical to ensure continued compliance and risk mitigation. It is suggested to implement robust monitoring mechanisms and establish clear escalation procedures to promptly address and identify risk.

How RiskRecon by Mastercard can help:
RiskRecon is unique in the fact that it not only categorizes vendors, but it also highlights the priority of assessment requirements based on relationship criticality - unique to each vendor. This categorization and prioritization ensures vendors are relevantly assessed. Plus, there are alert systems and mechanisms to interact with vendors to ensure compliance - further reducing the likelihood of an event. RiskRecon also alerts vendors who have fallen out of compliance enabling the immediate escalation of an incident response plan.

Governance and Oversight
Federally regulated financial institutions must establish effective government frameworks that ensure oversight of third parties' relationships. This includes assigning clear roles and responsibilities within the organization.

How RiskRecon by Mastercard can help:
RiskRecon has built in labeling systems to help third-party risk management (TPRM) analysts manage the vendor relationship. And in conjunction with a comprehensive Risk Management Plan, RiskRecon can improved risk incident reporting times.

Risk Assessment

There is emphasis on comprehensive risk assessment process that considers both the criticality of the services provided by the third parties and the potential impact on the institution's operations.

How RiskRecon by Mastercard can help:
RiskRecon's intuitive interface enables analysts to quickly understand the overall state of the third-party portfolio and understand low performers in relation to the criticality of the service or risk relationship to the vendor. This improves the effectiveness of the risk assessment, increases the capacity to manage more vendors, and improves the ability to understand the cyber risk of each vendor in a meaningful way.

RiskRecon determines value at risk for each system by discovering authentication, transaction capabilities, and data types collected, such as form fields collecting email addresses, credit card numbers, and names.

Business Continuity and Incident Response

Federally regulated financial institutions must collaborate with their third-party providers to develop robust business continuity and incident response plans. These plans should address potential disruptions and security incidents to minimize the impact on institutions and their customers.

How RiskRecon by Mastercard can help:
While RiskRecon doesn't play a role in the building or construction of incident/BC plans, RiskRecon can help ensure that the technical architecture meets the agreed upon security standards. Plus, it can monitor the posture of those assets to improve the likelihood of successful DR and RTO/RPO objectives.

Risk Appetite Framework
Federally regulated financial institutions must establish a risk appetite framework that aligns with their business objectives and risk tolerance. This framework helps in assessing and managing third party risks effectively.

How RiskRecon by Mastercard can help:
Although RiskRecon does not aid in the actual establishment of a risk appetite framework, it can map vendors to an established risk relationship structure outlined in a risk registry. This helps in understanding the schedule and necessity of an assessment and can help escalate the depth and breadth of the overall assessment.

Documentation and Reporting
Federally regulated financial institutions must maintain comprehensive documentation of their third-party relationships, including contracts, due diligence reports, and audit findings. Robust reporting mechanisms should be implemented to keep senior management and OSFI informed about the institution's third-party risk management.

How RiskRecon by Mastercard can help:
RiskRecon provides robust reporting that details and identifies current state, recent changes and potential risks that may affect the risk posture of a OSFI regulated institution. Additionally, the new Self-Serve Reporting module now allows organizations to build comprehensive reports to not only provide insights and information on the state of the third-party domain, but also on individual third-party companies as well.

Free Offer: Know Your Third-Party Security Risks

As a busy third-party risk professional taking swift action with limited information is no easy feat. Fortunately, Riskrecon is offering complimentary enterprise access to assess and monitor the cybersecurity of your supply chain for 30 days.

For 30 days you can enjoy a detailed view of the risk up to 50 vendors pose to your organization. Plus, you'll learn how to use these scores to influence corrective action with risk prioritized data based on issue severity.

What's Included in the Offer?

- Detailed assessment of your own IT assets
- Security ratings and summary assessment of up to 50 vendors
- Full access to Riskrecon technical support
- A risk-prioritized view into your vendor ecosystem with our vulnerability matrix
- Superior data accuracy (over 99% - which drastically reduces false positives)

Register to get insights into your supply chain at https://www.riskrecon.com/know-your-portfolio.