cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Agenda Item 4(a)(i)(1)
July 26/22 EOC Meeting

Fasken Financial Services Bulletin

JULY 18, 2022

On April 27, 2022, the Office of the Superintendent of Financial Institutions (OSFI) released a draft update to its Guideline B-10, **Draft Guideline B-10: Third-Party Risk Management** (Draft Guideline), which sets out enhanced expectations for federally regulated financial institutions (FRFIs) in managing an expanded scope of third-party risks. The Draft Guideline is a substantial revision to **the current Guideline B-10** and places a greater emphasis on governance and risk management plans and specific outcomes and principles. The Draft Guideline is near the end of its three-month public consultation period. Interested stakeholders may still submit their comments to **b10@osfi-bsif.gc.ca** until **September 30, 2022**. The final Guideline B-10 is expected to be issued in fall 2022.
The Draft Guideline offers a new perspective on risk-management expectations through four main changes relative to the existing Guideline B-10.

First, the scope of the Draft Guideline is expanded to include a wider variety of third-party arrangements. The current Guideline B-10 applies to "outsourcing arrangements", which are arrangements "whereby the service provider performs a business activity, function or process that is, or could be, undertaken by the [FRFI] itself". In developing the Draft Guideline, OSFI recognizes FRFIs are increasingly relying on a broad range of third parties in delivering critical activities that go beyond outsourcing arrangements. As a result, the Draft Guideline applies to "third-party arrangements" more broadly, which include any business or strategic arrangement with external entities. Examples of arrangements that would be subject to the Guideline include the use of independent professionals, brokers, and utilities (such as telecommunications); use of financial market infrastructure; other relationships involving the provision of services for the storage, use or exchange of data; and, generally any outsourced activities, functions, and services.

Second, the Draft Guideline widens the scope of risk governance beyond outsourcing activities to encompass third party risks generally. The Draft Guideline introduces "third-party risks" as an expanded concept that captures "risk to the FRFI's operational and financial resilience or reputation due to a third party failing to provide goods and services, protect data or systems, or otherwise carry out activities in accordance with the arrangement".

Third, the Draft Guideline replaces the materiality threshold in the current guideline and introduces a new "risk-based approach", which requires a more comprehensive risk management framework that accounts for the level of risk and the criticality associated with individual third-party arrangements. The level of risk and FRFI's operational and financial resilience are not measured against the "materiality" of the agreement, but through "criticality", which is defined "as the degree of impact of the third-party arrangement on the FRFI's risk profile, operations, strategy and/or financial condition."

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

OSFI provides that the exercise of determining risk should be a multi-pronged assessment that takes into consideration:

- the risks intrinsic in a particular third party (such as insolvency risks and the possibility of operational disruptions),
- the "criticality" of the nature of engagement with that third party, and
- the "concentration risks" associated with reliance on a small number of and/or geographically concentrated third-party providers or subcontractors.

Ultimately, the FRFIs are expected to manage the third-party risks in a manner that is proportionate to the level of risk and complexity of the FRFI's third-party ecosystem.

OSFI's Key Expectations as Set Out in the Draft Guideline

The fourth major change in the Draft Guideline is that it introduces a modernized guidance structure that is designed around five overarching outcomes based on 11 principles to enhance the operational and financial resilience of FRFIs. The intended outcomes start with foundational issues to ensure that FRFIs have put into place appropriate governance and accountability structures that deal with third-party engagements. This risk management framework is then expected to be used to identify and assess the risks posed by third parties, to manage and mitigate those risks within the FRFI's risk appetite, as well as to continually monitor the performance of third parties. Finally, OSFI expects the FRFI's risk management program to be dynamic and actively capture a range of third-party arrangements and interactions, including those with standardized contracts or those involving technology and cyber risks. Below is a summary of OSFI's desired outcomes and the principles and other expectations devised by OSFI to help FRFIs achieve these outcomes.

1. **Governance**	
Governance Generally	**Outcome:** Governance and accountability structures are clear with comprehensive risk strategies and frameworks in place to contribute to ongoing operational and financial resilience.
Accountability	**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.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Third-Party Risk Management Framework (TPRMF)	**Principle 2**: The FRFI should establish a third-party risk management framework 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. Additional Expectations: • Establish an enterprise-wide third-party risk management framework (TPRMF) to govern the lifecycle of third-party arrangements. • Regularly review, update, and improve the TPRMF.
1. **Third-Party Risk Management Program**	
Risk Identification and Assessment	**Outcome**: Risks posed by third parties are identified and assessed. **Principle 3**: The FRFI should identify and assess the risks of a third-party arrangement before entering the arrangement and periodically thereafter, proportionate to the level of risk and criticality of the arrangement. **Principle 4**: The FRFI should undertake due diligence prior to entering any form of arrangement with a third party, and on an ongoing basis proportionate to the level of risk and criticality of the arrangement. **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. Additional Expectations: • Conduct risk assessment throughout the lifecycle of a third-party arrangement—including prior to entering into the arrangement, regularly throughout the lifecycle of the arrangement, and whenever there is material change in the arrangement or third party. • Conduct due diligence prior to entering into a third-party arrangement, periodically on an ongoing basis, and whenever there is material change in the arrangement or third party.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

	• Assess concentration risk both prior to entering an arrangement and on an ongoing basis. • Assess subcontracting risks and whether the existence of material subcontracting might negatively impact operational and financial resilience of a third party. • Determine whether the arrangement aligns with the FRFI's risk appetite for the relevant risks.
Risk Management and Mitigation	**Outcome**: 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. **Principle 7:** The FRFI and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data throughout the duration of the third-party arrangement. **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. **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. Additional Expectations: • Define clear rights and responsibilities of between the FRFI and third party in a written agreement, and at a minimum include the provisions that are set out in **Annex 2** of the Draft Guideline, whenever it is feasible to customize the contract.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

	• Through the written agreements, establish and maintain appropriate measures to protect the confidentiality, integrity, and availability of data. • Through the written agreements, specify the reporting obligations of the third party to the FRFI to allow for appropriate monitoring of the performance measures, and to require reporting of events that could materially impact the FRFI, while also reserving audit rights. • Through the written agreements, outline measures for ensuring continuity of services in the event of disruption, and require the third party to regularly test the relevant disaster recovery programs. • Establish exit plans, encompassing both planned and unplanned exits, proportionate to the level of risk and criticality of the third-party arrangement.
Monitoring and Reporting	**Outcome**: 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. **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. Additional Expectations: • Monitor third-party agreements to ensure that the terms of the agreement are being followed, and that the third party remains financially sound. • Verify whether third-party arrangements, individually and in aggregate, remains within the FRFI's risk appetite.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

	• Ensure that third parties have documented processes for identifying, investigating, escalating, remediating, and notifying the FRFI of incidents that could impact the third party's ability to deliver the goods and/or services.
1. **Special Arrangements**	
	Outcome: The FRFI's risk management program is dynamic and actively captures and appropriately manages a range of third-party arrangements and interactions. Additional Expectations: • Where products and services are received under pre-defined terms and conditions in standard contracts—or where written arrangements do not exist—the FRFI should still have a third-party risk management program that covers the relationship, developing redundancies and other resiliency methods. • Where the third party is an external auditor, assure that the auditor would be in compliance with the applicable auditor independence requirements.
1. **Technology and Cyber Risk in Third-Party Arrangements**	
	Additional Expectations: • Where there are technology and cyber risks in a third-party arrangement, establish clear responsibilities between the parties in the written agreement in harmony with the risks and criticality of the arrangement. • Ensure that third parties comply with **FRFI standards for mitigating technology and cyber risks**. • Develop cloud-specific requirements for strategic adoption of cloud services and to enhance controls in data protection, key management, and container management. • Consider portability when entering an arrangement with a cloud service provider as part of the exit strategy planning.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Takeaways for FRFIs and Third-Party Service Providers

With its wider scope and more extensive assessment of risks, the upcoming revision of Guideline B-10 will require FRFIs to re-evaluate their current practices and processes, conduct additional diligence on third-party service providers, and where needed enhance their third-party risk management frameworks. Aside from updates to internal policies and review mechanisms, federally regulated financial institutions will be required to review, enhance, and update their current agreements and contract templates with third parties for critical offerings. The new Draft Guideline B-10 is intended to complete OSFI's **near-term plans** to modernize its risk management guidance (which also includes the introduction of Guideline B-13: Technology and Cyber Risk Management, **the final version of which OSFI expects to release in the coming weeks**), and the FRFIs now have the opportunity to revisit their risk management practices with a more comprehensive view.

Authors

Christopher Ferguson, PARTNER Toronto, ON

Julie He, ASSOCIATE Toronto, ON

Amirali Alavi, SUMMER STUDENT Toronto, ON