Prepare for change: OSFI's Updated B-10 guideline reinforces third-party risk management requirements

May 05, 2023

On April 25, 2023 the Office of the Superintendent of Financial Institutions (OSFI) released a new revised version of its B-10 guideline on third-party risk management (the Guideline).

OSFI stated that starting from May 1, 2024, third-party arrangements of federally regulated financial institutions (FRFIs), including banks, federally regulated insurers, trusts, and credit unions, must adhere to the Guideline. For arrangements established before this date, they should be assessed and amended at the earliest opportunity in order to align with the May 1, 2024 effective date or as soon as possible thereafter.

Expanded scope from previous guideline B-10 on outsourcing

In contrast to the previous version of B-10, which focused on outsourcing arrangements, the new Guideline significantly expands its scope to encompass business and strategic arrangements with third parties broadly. In effect, this expanded scope now captures arrangements with entities such as, brokers, utility providers, payment, clearing and settlement services, as well as services offered by parent holding companies, affiliates, or subsidiaries.[1]

Furthermore, the Guideline specifies its applicability to third-party relationships that FRFIs engage in, regardless of whether the FFRI is party to an agreement or whether there is a written agreement at all.

Consequently, it no longer focuses exclusively on outsourced risk, rather, it applies generally to all external arrangements that present third-party risk. Third-party risk is defined broadly, as any risk to the FRFI's operational and financial resilience or reputation due to a third-party failing to provide goods, business activities, functions and services, protect data or systems, or otherwise carry out activities in accordance with the arrangement exposing the FRFI to negative outcomes.

Rather than insisting on reliance on contractual provisions to manage risks, the new Guidelines puts an emphasis on governance and risk management programs in the management of third-party arrangements and risk.

It insists on the fact that the FRFI is ultimately accountable for all business activities, functions, and services outsourced to third parties and for managing the risks related to arising from all types of third-party arrangements. For this purposes, it requires that FRFI establish an enterprise-wide 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.

The Guideline explicitly states that OSFI expects FRFIs to conduct due diligence on third parties before entering an arrangement and continuously thereafter, with a focus on high-risk and critical arrangements. In doing so, they should consider key factors such as the third party's experience, financial strength, compliance with laws and regulations, reputation risk, risk management programs, technology and cyber risk management, business continuity plans, concentration risk, geographic location, and insurance coverage.

The enterprise wide-third party risk management framework will have to establish clear accountabilities, policies and processes for identifying, monitoring and managing third party risk.

Interestingly, the Guideline now explicitly states that where a third party is subject to government regulation or supervision, the FRFI may take this into consideration as part of its risk assessment. This may apply, for example, to a FRFI dealing with provincially regulated financial institutions.

Requirements and outcomes

The Guideline identifies fundamental outcomes alongside various general guiding principles. As an overview, these include: governance, management of third-party risk, special arrangements, and technology and cyber risk in third-party arrangements. These obligations, expected outcomes and their underlying principles impose a number of requirements on FRFIs, which include the following.

- Establish a comprehensive and effective third-party risk management framework to manage the risks associated with outsourcing, in which governance and accountability structures are clear.
- Establish process for appropriate and proportionate ongoing due diligence when entering into third party arrangements and engaging third-party service providers.
- Monitor the risk and performance of third-party service providers and manage risks throughout the entire third-party arrangement, including subcontracting risks
- Where possible, enter into clear and comprehensive agreements between FFRIs and third-parties that set out the rights, responsibilities and obligations of each party, risk management frameworks, incident management reporting, and termination or exit provisions, and which has been reviewed by the FRFI’s legal counsel. For third-party arrangements which a customized contracts may not be feasible, or for which a formal contract or agreement may not exist, however, FRFI is still required to take measures to manage the risk of such arrangements.

- Establish incident management and reporting procedures, as well as contingency planning and exit strategies, in particular, cloud portability (or lack thereof) in the case of exiting cloud services.
- Institute special arrangements for critical operations subject to third-party arrangements and implement a specific risk management framework to address standardized contracts mandated by third parties and their inherent risks.
- Establish technology and cyber controls to manage risks, while monitoring cyber operations carried out by third parties to ensure operations are transparent, reliable and secure.
- Develop cloud-specific requirements to ensure planned and strategic cloud adoption.

Third party arrangements subject to the guideline

The Guideline defines a third-party arrangement as any type of business or strategic arrangement between a FRFI and another entity or individual, by contract or otherwise (except for arrangements with FRFI customers and employment contracts).[2]

This includes outsourcing arrangements, cloud computing services and other types of business arrangements where a third-party is providing services or maintaining functions to the FRFI. Fundamental to applying the Guideline is identifying the type and level of risk arising from each third-party arrangement, including subcontracting arrangements, in a way that the FRFI can manage each third-party arrangement proportionately in accordance with the Guideline's requirements.

OSFI's response to consultation feedback

In response to the feedback received during the consultation process for the Guideline, OSFI has made several changes to the final Guideline. Some key takeaways from the feedback follow.

- **Scope**: Respondents expressed concerns about the broad scope of the Guideline, which could capture certain arrangements not intended to be covered. The final version of the draft maintains a broad definition of third-party arrangement, but now clearly specifies that employment contracts are excluded, in addition to customers contract (e.g., depositors or policyholders).
- **Subcontractors:** [3]
- **Concentration Risk:** [4] Participants mentioned that applying Guideline requirements to subcontractors is challenging. However, OSFI emphasized that FRFIs are responsible for managing risks related to subcontracting, and they expect to conduct supervisory activities even when an FRFI uses subcontractors.
- **Transition Period** : Respondents requested a transition period for implementing the new requirements and OSFI responded by providing a two-year transition period (May 1, 2024). In this regard, OSFI has indicated that it expects third-party arrangements beginning on or after the Guideline's effective date will comply with the Guideline, while those established prior should be assessed and amended at the earliest opportunity in order to align with the Guideline by May 1, 2024 or as soon as possible thereafter.

In the final version of the Guideline, OSFI also provided additional guidance on its expectations relating to provisions that FRFIDs should include in high-risk and critical third-party agreements, in particular by including provisions that cover essential aspects of the relationship between the parties, such as roles, pricing, performance measures, assets ownership, security, notifications of specific events to the FRFI, dispute resolution mechanisms, requirement to adhere to all applicable regulatory requirement, business continuity, termination, insurance and risk management.[5]

If you would like to know more about the Guideline or have any questions regarding its impact on your business activities, please reach out to any of the authors or key contacts listed below.

[1] Arrangements with FRFI customers and employment contracts are excluded.

[2] Guideline excludes foreign bank branches and foreign insurance company branches. OSFI's expectations for foreign bank branches and foreign insurance company branches are set out in Guideline E-4: Foreign Entities Operating in Canada on a Branch Basis.

[3] The Guideline defines "subcontractor" as "an entity within the third-party's contracting, external arrangements or supply chain".

[4] According to the Guideline, "Concentration risk has two forms. **Institution-specific concentration risk** is the risk of loss or harm to the FRFI resulting from overreliance on a single third-party, subcontractor or geography for multiple activities. **Systemic concentration risk** is the risk arising from concentration in the provision of services by one third-party or geography to multiple FRFIs."

[5] See Guideline, Annex 2, for provisions for third-party agreements, a non-exhaustive list including: Nature and scope of the Arrangement, Roles and responsibilities, Use of Subcontractors, Pricing, Performance measures, Ownership and access, Security of records and Data, Notifications to the FFRI, Dispute resolution, Regulatory compliance, Business continuity and recovery, Default and termination, Insurance, Prudent risk management.

By

Guillaume Talbot-Lachance, Cindy Y. Zhang, Jake Palace

Expertise

Banking & Financial Services, Financial Services, Financial Services Regulatory

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749