OSFI RELEASES FINAL GUIDELINE B-10 IMPACTING FRFIS ENGAGING IN BUSINESS WITH THIRD PARTIES

Posted on April 26, 2023

Categories: Insights, Publications

On April 24, 2023, the Office of the Superintendent of Financial Institutions ("**OSFI**") published its final Third-Party Risk Management Guideline (the "**Guideline**") coming into effect May 1, 2024. The Guideline has been introduced to manage risks arising from third-party arrangements and applies to all federally regulated financial institutions ("**FRFIs**") with the exception of foreign bank and insurance branches (who are subject to certain outsourcing requirements as set out in Guideline E-4). Of the many outcomes and principles detailed in the Guideline, OSFI expects FRFIs to assess risk and criticality when examining third-party arrangements to determine how and to what extent to apply each principle. In April 2022, OSFI released a draft of the "new" Guideline B-10 that was subject to a consultation period. Since the draft, OSFI has clarified the scope and extent of risk assessments to be completed by FRFIs. They have also increased emphasis on using a risk-based approach to arrangements and clarified the expectations of FRFIs where it was not clear in the draft.

Governance

FRFIs are accountable for managing risks stemming from third-party arrangements even if they outsource to third parties. It is incumbent upon an FRFI's Senior Management to ensure that the business activities, functions and services performed by third parties comply with applicable laws, policies and procedures. The Guideline also calls for FRFIs to introduce a Third-Party Risk Management Framework (the "**Framework**") that can be used to identify, manage, mitigate, monitor and report on third-party related risks. The Framework should be customized to align with each third-party arrangement and should be reflective of the FRFI's risk appetite.

Management of Third-Party Risk

OSFI notes that each third party arrangement should be assessed to determine its related risks and criticality with risk assessments taking place before and during the life of the arrangement. FRFIs are expected to assess each third-party arrangement regularly, reviewing high risk and critical arrangements more frequently and conducting more stringent risk management. This obligation to identify, monitor and manage risks remain true even when third parties enter subcontracting agreements. The Guideline also details the criteria for

criticality assessments and sets out factors that impact the assessment of third party risk. As it pertains to foreign third-party arrangements, FRFIs should assess these arrangements by reviewing the legal, political, economic, social, amongst other landscape when assessing the risk.

FRFIs are also expected to conduct appropriate due diligence proportionate to the level of risk and criticality of the third-party arrangement. This due diligence process should take place before entering a third-party arrangement and should be done on an ongoing basis. OSFI also expects FRFIs to enter into written agreements with respect to third-party arrangements. These agreements should set out the rights and responsibilities of each party. For those arrangements that are high risk and critical, OSFI also provides specific provisions to be included in these written contracts.

FRFIs are expected to establish and maintain appropriate measures to uphold confidentiality, integrity and manage access to records and data. FRFIs should ensure that its agreements with third parties do not impinge on its reporting obligations under OSFI's Technology and Cyber Security Incident Reporting Advisory.

There are also certain record keeping requirements as per the *Bank Act*, *Insurance Companies Act*, and the *Trust and Loan Companies Act* (collectively "**FRFI Statutes**") that FRFIs must keep in mind. These detailed records should be updated and accurate as at the end of each business day. OSFI maintains that electronic records must be capable of being reproduced in written form within a reasonable period of time. However, certain categories of information, such as reinsurance arrangements or files related to complex activities, an "executed copy" may need to be available to OSFI upon request. FRFIs must maintain copies of the records at its head office, or at such other place in Canada as the directors of the FRFI think fit. If the records are in electronic form, complete copies must be kept on a computer server physically located at the places stipulated in the FRFI Statutes.

FRFIs should also ensure that they have access to accurate and comprehensive information as part of its third-party arrangements. This is important in risk assessment and facilitates audits of third parties to ensure that these third parties are meeting performance goals and effectively managing risks. Where incidents arise, FRFIs should ensure that there is an effective reporting system in place to ensure that third parties have adequate procedures to identify, investigate and notify the FRFI of such incidents.

It is important that third-party arrangements stipulate that third parties should report events that materially affect risks in a timely manner and should provide the FRFI and OSFI the right to assess current risk management practices or appoint auditors to do so. Third-party agreements should contemplate providing support during moments of disruption to ensure continuity of service. In the event that FRFIs need to end their third-party arrangements, FRFIs should establish contingency and exit plans for doing so efficiently without disrupting the FRFI's operations.

Special Arrangements

The Guideline also contemplates procedures to be followed when FRFIs enter into standardized contracts with third parties. Whether an arrangement is set out in a written agreement or otherwise, FRFIs are expected to use their third-party risk management programs to address the relationship and assess risks. Where FRFIs employ external auditors, the auditors must be independent and not be relied upon to conduct actuarial or internal audits.

Technology and Cyber Risk in Third-Party Arrangements

FRFIs should consider controls to manage technology and cyber risks that might stem from its third-party arrangements. FRFIs should ensure that third parties with increased technology and cyber risks comply with the FRFI standards to effectively mitigate risk. Cloud-specific requirements should be established to optimize operations while managing risks and be accompanied by effective cloud governance to ensure oversight and compliance monitoring to safeguard its use.

by Darcy Ammerman and Shaniel Lewis (Articling Student)

A Cautionary Note