MAY 30, 2022 • 16 MIN READ

OSFI B-10 beyond outsourcing: OSFI begins consultation on a replacement of Guideline B-10

AUTHORS


Adam S. Armstrong


Steven Slavens


Wendes Keung

On April 27, the Office of the Superintendent of Financial Institutions (OSFI) released a draft of its proposed major update to Guideline B-10, Outsourcing of Business Activities, Functions and Processes, and began a consultation process. This is the first major update to B-10 since 2009 and reflects a significant change in approach to regulating third-party risk management for federally regulated financial institutions (FRFIs).

Download a side-by-side comparison of the current and revised B-10 Guidelines, or see below for the same table on this page.

What you need to know

- Currently, B-10 sets out the expectations for FRFIs that outsource, or contemplate outsourcing, one or more of their business activities to a service provider[1]. Its focus was almost solely on material outsourcings and several of its requirements have proved difficult to meet as the outsourcing landscape has evolved and cloud computing and other shared platforms have become more common than traditional bespoke outsourcing arrangements.
- The proposed revisions to B-10, titled Guideline B-10, Third Party Risk Management Guideline (Revised B-10) is intended by OSFI to reflect a more comprehensive risk-based approach within an expanded third-party ecosystem used by FRFIs—notably, even beyond outsourcings. Revised B-10 is also intended to provide a more nuanced approach to different service delivery models.
- The following are the principal changes that OSFI has identified as forming the basis of Revised B-10[2].
  - **Expanded scope:** establishing that all third-party arrangements (including things like the use of brokers, utilities, clearing and settlement systems, software providers, and even independent professionals) and not just outsourcings are captured in the scope of Revised B-10.
  - **Widened risk lens:** beyond the typical risks associated with outsourcing, focusing on a wider range of risks related to third parties, including “technology, cyber, data security, financial, operational, business continuity management, subcontracting/supply chain risks, and concentration risks”.
  - **Enhanced risk focus:** replacing the binary one-time material assessments with a lifecycle-based approach employing a sliding scale to be managed according to individual levels of risk and criticality over time.
  - **Modernized guidance:** replacing legalistic language of the guideline with a more streamlined approach emphasizes clear outcomes and principles.

- In addition to the above principal changes identified by OSFI, we would also suggest that Revised B-10's key changes are the inclusion of the Outcomes and Principles to guide FRFIs' approach, the reframing of contractual requirements—in particular related to standardized contracts proffered by third parties and issues related to audit and oversight.
- At OSFI's May 4 information session, OSFI shared its proposed timeline for consultation and implementation of Revised B-10. Comments are to be submitted to b10@osfi-bsif.gc.ca by July 27, 2022, and OSFI intends to implement Revised B-10 toward the end of 2022 (with allowances for transitioning to the new guidance to be included in Revised B-10 once finalized) and begin a series of training and industry sessions in early 2023.

Outcomes and principles

As noted above, Revised B-10's approach is focused on outcomes and principles.

Revised B-10 presents five expected outcomes for FRFIs, which are meant to contribute to the FRFI's operational and financial resilience and help safeguard its reputation[3]:

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 assessed, and risks 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.

The following are the 11 principles that form the basis of the Revised B-10[4]:

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.
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.
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.
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.
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.
6. The FRFI should enter into written arrangements that set out the rights and responsibilities of each party.
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.

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.

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.

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.

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.

These outcomes and principle do not, in our view, mark a significant change from the approach that most FRFIs take to third-party arrangements, but their inclusion in explicit terms may be helpful for focusing FRFIs on key expectations.

Minimum contractual requirements

Similar to the current form of B-10, Revised B-10 includes a number of expectations for what ought to be included within the agreement with the third party but most of the changes are relatively subtle, new syntax notwithstanding. We've prepared a cheat sheet, available here.

The main thematic difference related to contract requirements is OSFI's recognition that a one-size-fits-all approach is not the expectation.

Consistent with Revised B-10's emphasis on a risk-based approach beyond the binary consideration of whether or not an engagement is a material outsourcing, Revised B-10 acknowledges that not all arrangements with third parties will include a customized contract. Instead, Revised B-10 includes a section regarding "Standardized Contracts/Special Arrangements" to address these circumstances. In lieu of contractual terms that support a typical material outsourcing, OSFI's requirement is that the FRFI have a risk management program covering the relationship that is proportionate to the level of risk and criticality of the arrangement. Mitigating steps other than contractual rights are expressly encouraged.

A similar approach informs Revised B-10's approach to audit rights, employing methods other than an onsite audit by FRFI or OSFI (such as independent reports provided by third parties) to achieve oversight. In our experience, this has at times been the process adopted by FRFIs with certain vendors, but the explicit recognition of the validity of these sorts of audit reports—and the decision not to include audit provisions within the annex of Minimum Provisions for Third-Party Agreements—does mark a notable change in approach from OSFI.

As OSFI receives comments on Revised B-10, it may be that additional changes to the contractual requirements will be incorporated, but in the present draft many of the changes are quite subtle.

To manage the risks associated with each third-party arrangement, OSFI expects that FRFIs structure their written agreement with third parties in a manner that allows them to meet the expectations set out in the Revised Guideline B-10. The following table compares the new non-exhaustive minimum contractual requirements with the current Guideline B-10.

Download a PDF version of this side-by-side comparison of the current and revised B-10 Guidelines.

Current and proposed B-10 minimum contractual requirements

Guideline B-10[5]	Revised Guideline B-10[6]
Nature and scope of the arrangement	

The agreement is expected to specify the scope of the relationship, which may include provisions that address the frequency, content, and format of the service being provided. The agreement is expected to detail the physical location where the service provider will provide the service.	The agreement should specify the nature and scope of the arrangement, including provisions that address the frequency, content and format of services, duration of the agreement, and physical location of the services being provided.
Roles and responsibilities	
Not included as a separate contractual requirement.	The agreement should clearly establish the roles and responsibilities of the FRFI and the third party and any material subcontractors of the third party, including the management of technology and cyber risks and controls.
Use of subcontractors	
The agreement is expected to set out any rules or limitations to subcontracting by the service provider. Security and confidentiality standards should apply to subcontracting or outsourcing arrangements by the primary service provider. The audit and inspection rights of the FRFI and OSFI should continue to apply to all significant subcontracting arrangements.	The agreement should establish parameters on the use of subcontractors and require the third party to notify the FRFI of any subcontracting of services so that the FRFI may conduct due diligence, as well as assess and manage the risk of the subcontractors and any potential impacts from a change in service.
Pricing	
The agreement should fully describe the basis for calculating fees and compensation relating to the service being provided.	The agreement should set out the basis for calculating fees relating to the services being provided.
Performance measures	
Performance measures should be established that allow each party to determine whether the commitments contained in the contract are being fulfilled.	The agreement should establish performance measures that allow each party to determine whether the commitments set out in the agreement are being fulfilled.
Ownership and access	
Identification and ownership of all assets (intellectual and physical) related to the outsourcing arrangement should be clearly established, including assets generated or purchased pursuant to the outsourcing arrangement. The agreement should state whether and how the service provider has the right to use the FRFI's assets (e.g., data, hardware and software, system documentation, or intellectual property) and the FRFI's right of access to those assets.	The agreement should identify and establish ownership of all assets (intellectual and physical) related to third-party arrangements, including assets generated or purchased pursuant to the arrangement. The agreement should also specify whether and how the third party has the right to use the FRFI's assets (e.g., data, hardware and software, system documentation, or intellectual property), including authorized users, and the FRFI's right of access to those assets.
Security of records and data	

At a minimum, the agreement is expected to set out the FRFI's requirements for confidentiality and security. Ideally, the security and confidentiality policies adopted by the service provider would be commensurate with those of the FRFI and should meet a reasonable standard in the circumstances. The agreement should address which party has responsibility for protection mechanisms, the scope of the information to be protected, the powers of each party to change security procedures and requirements, which party may be liable for any losses that might result from a security breach, and notification requirements if there is a breach of security. OSFI expects appropriate security and data confidentiality protections to be in place. The service provider is expected to be able to logically isolate the FRFI's data, records, and items in process from those of other clients at all times, including under adverse conditions.	The agreements should govern the confidentiality, integrity, security, and availability of records and data.
Guideline B-10	**Revised Guideline B-10**
Notifications to the FRFI	
Not included as a separate contractual requirement.	The agreement should require the third party to notify the FRFI of: • incidents/events (at the third party or a subcontractor) that impact or could potentially impact services provided, the FRFI's customers/data, or the FRFI's reputation; • technology and cyber security incidents (at the third party or a subcontractor) to enable the FRFI to comply with its reporting requirements under OSFI's Technology and Cyber Security Incident Reporting Advisory[7]; • significant organizational/operational changes.
Dispute resolution	
OSFI expects the agreement to incorporate a protocol for resolving disputes. The agreement should specify whether the service provider must continue providing the service during a dispute and the resolution period, as well as the jurisdiction and rules under which the dispute will be settled.	The agreement should incorporate a protocol for resolving disputes. The agreement should also specify whether the third party must continue providing the service during a dispute and the resolution period, as well as the jurisdiction, governing law(s), and rules under which the dispute will be settled.
Regulatory compliance	
Not included as a separate contractual requirement.	The agreement should enable the FRFI to comply with all applicable legislative and regulatory requirements, including, but not limited to, location of records and privacy of client information.
Business continuity and recovery	

The agreement should outline the service provider's measures for ensuring the continuation of the outsourced business activity in the event of problems and events that may affect the service provider's operation, including systems breakdown and natural disasters, and other reasonably foreseeable events. The FRFI should ensure that the service provider regularly tests its business recovery system as it pertains to the outsourced activity, notifies the FRFI of the test results, and addresses any material deficiencies. The FRFI is expected to provide a summary of the test results to OSFI upon reasonable notice. In addition, the FRFI should be notified in the event that the service provider makes significant changes to its business resumption and contingency plans, or encounters other circumstances that might have a serious impact on the service.	The agreement should require the third party to outline measures for ensuring continuity of services in the event of disruption, including testing and reporting expectations and mitigation requirements, as well as requirements of the third party to monitor and manage technology and cyber security risk.
Default and termination	
The agreement is expected to specify what constitutes a default, identify remedies, and allow for opportunities to cure defaults or terminate the agreement. The FRFI is expected to ensure that it can reasonably continue to process information and sustain operations in the event that the outsourcing arrangement is terminated or the service provider is unable to supply the service. Appropriate notice should be required for termination of service and the FRFI's assets should be returned in a timely fashion. In particular, data and records relating to data processing outsourcing arrangements should be returned to the FRFI in a format that would allow the FRFI to sustain business operations without prohibitive expense. The agreement should not contain wording that precludes the service from being continued in situations where the Superintendent takes control of the FRFI, or where the FRFI is in liquidation.	The agreement should specify what constitutes a default, or right to terminate, identify remedies, and allow for opportunities to cure defaults or terminate the agreement. Appropriate notice should be required for termination of the service and, where applicable, the FRFI's assets should be returned in a timely fashion. Any data and records should be returned to the FRFI in a format that allows the FRFI to sustain business operations without unreasonable expense. The agreement should not contain any terms that inhibit OSFI, or any other resolution authority or financial compensation scheme, from carrying out their mandate in times of stress or resolution. For example, the agreement should, among other things, remain valid and enforceable in resolution provided there is no default in payment obligations.
Insurance	
The service provider should be required to notify the FRFI about significant changes in insurance coverage and disclose the general terms and conditions of the insurance coverage.	The agreement should require the third party to obtain and maintain appropriate insurance and disclose the general terms and conditions of the insurance coverage. The agreement should also require the third party to notify the FRFI in the event of significant changes in insurance coverage.
Prudent risk management	
Not included as a separate contractual requirement.	The agreement should include any additional provisions necessary for the FRFI to prudently manage its risks in compliance with the Revised Guideline B-10.

Conclusion

Revised B-10 is a true re-framing of the B-10 guideline and while it introduces significant changes to OSFI's guidance on managing third-party arrangements, many FRFIs have already been employing the sort of broad risk-based approach proposed by OSFI in outsourcing and similar arrangements.

Nevertheless, as Revised B-10 continues to develop, FRFIs will want to carefully consider the policies and procedures they employ for managing third-party relationships:

- Conducting intake and proper due diligence for potential third-party arrangements.
- Performing a detailed and broad risk assessment.
- Considering and including appropriate risk mitigation strategies and dealing with circumstances where the FRFI is not able to successfully negotiate all of the protections it desires within the written agreement with the third party.
- Adhering to OSFI's contracting requirements through negotiation, and adequate management and oversight relationships over time.

As part of this process, contract templates, intake processes, and contract governance and relationship management procedures for areas of operation beyond the FRFI's IT infrastructure and other areas that have been the focus of past outsourcings will likely need to be adapted to take OSFI's requirements into account.

As noted above, Revised B-10 is currently in the consultation stage. OSFI seeks feedback and comment (especially on the clarity and granularity of detail of OSFI's risk management expectations) by July 27, 2022 to b10@osfi-bsif.gc.ca.

FOOTNOTES

To discuss these issues, please contact the author(s).