MAY 31, 2023 • 23 MIN READ

OSFI B-10 Third-Party Risk Management: updates to Guideline B-10 expand scope beyond outsourcings

AUTHORS

 Joel Ramsey

 Steven Slavens

 Danielle Colliver

 Wendes Keung

 Adam S. Armstrong

On April 24, the Office of the Superintendent of Financial Institutions (OSFI) released a new Guideline B-10 (Revised Guideline B-10), the Third-Party Risk Management Guideline, approximately one year after releasing its initial draft for comment (for more background, read our full analysis of the Draft Guideline B-10).

Consistent with Draft Guideline B-10, Revised Guideline B-10 shifts focus from outsourcing arrangements to setting expectations for federally regulated financial institutions (FRFIs) when managing risks associated with third-party arrangements of all kinds. It also reframes the risk analysis and guides FRFIs in their development and implementation of a risk-based approach to managing third-party risk.

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

What you need to know

- OSFI has provided a transition period ending May 1, 2024 for FRFIs to begin applying Revised Guideline B-10, and OSFI expects that third-party arrangements commencing on or after the end of the transition period adhere to Revised Guideline B-10. Third-party arrangements entered into during the transition period should be reviewed and updated at the earliest renewal or re-opening of the contract so that they adhere to Revised Guideline B-10 by the end of the transition period or as soon as possible thereafter. FRFIs should consider making updates to their policies and procedures, including establishing a third-party risk management framework, to meet that timeline.
- Revised Guideline B-10 reflects a more comprehensive risk-based approach within an expanded third-party ecosystem used by FRFIs—notably, beyond outsourcings.
- Revised Guideline B-10 allows FRFIs to take a more nuanced approach than considering the binary questions of outsourcing vs. not outsourcing and material vs. immaterial. It requires FRFIs to consider risk and the degree of criticality when examining third-party arrangements to determine the intensity with which to apply the expectations set out in Revised Guideline B-10. OSFI has confirmed that it expects all third-party arrangements to be analyzed to determine the criticality and risk of the arrangement so that FRFIs can manage the relationship and mitigate risks accordingly.

- Revised Guideline B-10 recognizes that alternatives to traditional contractual approaches to oversight may be appropriate for certain third-party relationships which are subject to standard contractual terms or where FRFIs otherwise have little room to negotiate terms.
- Since publishing Draft Guideline B-10, OSFI made the following significant updates:
  - transparency, reliability and security of technology has been added as an expected outcome;
  - further detail regarding the risk analysis to be undertaken by FRFIs has been included;
  - the approach to subcontractors of third-party providers has been modified; and
  - the relationship between Revised Guideline B-10 and other OSFI directives (most notably its advisory on technology and cyber security incident reporting) has been clarified.

Aims and approach

In its letter introducing Revised Guideline B-10[1], OSFI set out the following aims for the revisions:

- **Address a comprehensive set of third-party risks** within an expanded third-party ecosystem, placing emphasis on governance and risk management programs and setting outcomes-focused, principles-based expectations for FRFIs on the sound management of third-party risk.
- **Reflect a principles-based approach** with increased emphasis on a risk-based approach to managing third-party arrangements, reflecting the expectation that FRFIs apply Revised Guideline B-10 in a manner that is proportionate to the level of risk and criticality of each arrangement and the size, nature, scope, complexity and risk profile of the FRFI.
- **Adopt a pragmatic approach to managing subcontractor and concentration risks,** with FRFIs managing subcontractor risk according to the level of risk and criticality of the given third-party arrangement, taking reasonable steps to manage concentration risks related to their third-party arrangements, and assessing systemic concentration risk to the greatest extent possible.
- **Does not impede the development of a federal framework for consumer-directed data mobility** within the financial sector. Once the framework is designed, OSFI may provide relevant guidance as appropriate.
- **Provide adequate implementation time to self-assess and build adherence by May 1, 2024**, with the expectation that third-party arrangements commencing on or after the end of the transition period adhere to Revised Guideline B-10 and those entered into during the transition period are reviewed and updated at the earliest opportunity so that they adhere to Revised Guideline B-10 by the end of the transition period or as soon as possible thereafter.

Risk-based approach to applicability

Revised Guideline B-10 addresses concerns raised during the consultation process[2] about the broad scope of the application proposed in Draft Guideline B-10. To address these concerns, Revised Guideline B-10 indicates that FRFIs should consider the risk and criticality of each third-party arrangement to determine the intensity with which to apply the expectations set out in the guideline.

OSFI acknowledges that third-party arrangements may take a variety of forms, ranging from services that are critical to the FRFI to minor support arrangements or strategic arrangements where no services are provided. In light of this, OSFI identifies **two key factors** to be considered in determining the intensity level at which to apply Revised Guideline B-10: (i) the risk and criticality of each third-party arrangement; and (ii) the size, nature, scope, complexity and risk profile of the FRFI[3].

Revised Guideline B-10 also includes a more comprehensive list of factors that FRFIs can consider in determining the criticality and risk of each third-party arrangement, as compared to Draft Guideline B-10. These factors are:

Criticality factors

- the severity of loss or harm to the FRFI if the third party or subcontractor fails to meet expectations due to insolvency or operational disruption;
- substitutability of the third party, including the portability and timeliness of a transfer of services;
- the degree to which the third party or subcontractor supports a critical operation of an FRFI; and
- the impact on business operations if the FRFI needed to exit the third-party arrangement and transition to another service provider or bring the business activity in-house.

Risk factors

- the probability of the third party or subcontractor failing to meet expectations due to insolvency or operational disruption;
- the ability of the FRFI to assess controls of the third party and continue to meet regulatory and legal requirements in respect of activities performed by the third party, particularly in the case of disruptions;
- the financial health of the third party and the "step-in" risk, whereby the FRFI is required to provide financial support to the third party;
- the third party's use of subcontractors and the complexity of the supply chain;
- the degree of the FRFI's reliance on third parties with elevated concentration risk;
- the information management, data, cyber security, and privacy practices of the third party and its subcontractors; and
- any other relevant financial and non-financial risks associated with the use of the third party.

Finally, OSFI has clarified in Revised Guideline B-10 that the due diligence factors in Annex 1 should apply in respect of high and critical arrangements (at minimum), whereas Draft Guideline B-10 was not prescriptive as to the types of arrangements these factors would apply to.

Outcomes and principles

Revised Guideline B-10's approach is focused on outcomes and principles. FRFIs should keep these principles and outcomes in mind both when designing their third-party risk management programs and when entering into any third-party arrangements.

Revised Guideline B-10 presents **six expected outcomes** for FRFIs through third-party risk management, which are meant to contribute to the FRFIs' operational and financial resilience and help safeguard their reputation[4]. The first five were included in Draft Guideline B-10, with only minor wording differences in Revised Guideline B-10, whereas the sixth was added to Revised Guideline B-10.

1. Governance and accountability structures are clear with comprehensive risk management strategies and frameworks in place.
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 monitored and assessed, and risks and incidents are proactively addressed.
5. The FRFI's third-party risk management program allows the FRFI to identify and manage a range of third-party relationships on an ongoing basis.
6. Technology and cyber operations carried out by third parties are transparent, reliable and secure.

The following are the **11 principles** that form the basis of Revised Guideline B-10[5]. These have not changed significantly between Draft Guideline B-10 and Revised Guideline B-10:

1. The FRFI is ultimately accountable for managing the risks arising from all types of 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 risks relating to the use of third parties.
3. The FRFI should identify and assess the risks of a third-party arrangement before entering into the arrangement and periodically thereafter. Risk assessments should be proportionate to the criticality of an 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 before 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 is responsible for identifying, monitoring and managing risk arising from subcontracting arrangements undertaken by its third parties.
6. The FRFI should enter into written arrangements that set out the rights and responsibilities of each party.
7. Throughout 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 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 maintain risk levels within the FRFI's risk appetite.

These outcomes and principles do not, in our view, mark a significant change from the approach that many FRFIs take to third-party arrangements, but their inclusion in explicit terms may help focus FRFIs on key expectations.

Third-Party Risk Management Framework (TPRMF)

Most FRFIs likely have policies and procedures designed to address certain arrangements with third parties—outsourcings, auditors, etc. Many FRFIs, however, do not have those policies integrated into a comprehensive third-party risk management framework which is designed to evaluate, risk-rate, classify and manage all third-party relationships across the enterprise. This is what Revised Guideline B-10 requires.

The TPRMF should be developed to manage the entire lifecycle of third-party arrangements, from sourcing all the way to exit and transition-out. It is through the TPRMF that the FRFI will identify and assess; manage and mitigate; and monitor and report on third-party risk.

Among other things, this enterprise-wide approach will help FRFIs manage various forms of risk, including concentration risk, which can sometimes be difficult to assess and manage on a single-engagement-by-single-engagement basis.

Clarifications regarding subcontractors

OSFI has indicated that Revised Guideline B-10 addresses concerns raised during the consultation process[6] about the difficulties in imposing B-10 requirements on fourth-party subcontractors by clarifying the responsibilities of FRFIs for managing the risks posed by subcontracting. Whereas Draft Guideline B-10 required FRFIs to assess whether the existence of **material** subcontracting might negatively impact their operational and financial resilience during disruption and whether this risk could outweigh the benefits of the arrangement, Revised Guideline B-10 is broader and requires the FRFI to assess risks arising from subcontractors that could impact the FRFI. Revised Guideline B-10 indicates that FRFIs should receive ongoing updates and reporting on a third party's use of subcontractors and that the contractual provisions used to achieve this should be tailored to the level of risk and the criticality of services provided by the third party.

Clarifications regarding other guidelines

As part of the consultation process leading up to the publication of Revised Guideline B-10, OSFI has been more explicit in how FRFIs are meant to comply with Revised Guideline B-10 and other guidelines (such as the Technology and Cyber Security Incident Reporting Advisory, Guidelines B-13: Technology and Cyber Risk Management and E-21: Operational Risk Management). Perhaps not surprisingly, Revised Guideline B-10 is meant to be applied in a manner consistent with the other directives and in a manner that is meant to ensure that arrangements with third parties do not impede the FRFI's ability to comply with other OSFI guidance.

Minimum contractual requirements

Revised Guideline B-10 includes expectations for what ought to be included within the agreement with the third party for high-risk and high-criticality arrangements, not necessarily all arrangements. Before the publication of Revised Guideline B-10, similar requirements would have been expected to be included in material outsourcing agreements, but now any type of third-party arrangement (for example, hardware supply, loan purchase and servicing agreements, co-branding arrangements) that is high-risk or high-criticality is expected to address the subject matter of the minimum contractual requirements.

When reviewing Revised Guideline B-10, we think it's important to look beyond Annex 2, which sets out the minimum contractual requirements suggested by OSFI. Expectations for the content of agreements with third parties can be found in other areas of the guideline as well. We've prepared a **comparison cheat sheet**, which compares the existing Guideline B-10 contractual requirements to Revised Guideline B-10 requirements.

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

Consistent with Revised Guideline B-10's emphasis on a risk-based approach beyond the binary consideration of whether or not an engagement is a material outsourcing, Revised Guideline B-10 acknowledges that not all arrangements with third parties will include a customized contract or a written contract at all. Instead, Revised Guideline B-10 includes a section regarding "Special Arrangements" to address these circumstances. In lieu of contractual terms that support a typical material outsourcing, OSFI requires 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 Guideline 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 Annex 2—does mark a notable change in approach from OSFI.

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 Revised Guideline B-10. The following table compares the new non-exhaustive minimum contractual requirements with the existing Guideline B-10.

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

Existing and revised B-10 minimum contractual requirements

Guideline B-10[7]	Revised Guideline B-10[8]
Applicability of Minimum Contractual Requirements	
OSFI expects **material outsourcing arrangements** to be documented by a written contract that addresses all elements of the arrangement. Some of the items identified below may not be applicable in all circumstances, however, FRFIs are expected to address all issues relevant to managing the risks associated with each outsourcing arrangement to the extent feasible and reasonable given the circumstances and having regard to the interests of the FRFI.	Annex 2 provides a non-exhaustive list of provisions that FRFIs should include in **high-risk and critical third-party agreements**. Consideration should be given to adding these provisions to agreements with other third parties as appropriate, proportionate to the risk and criticality posed by the third party.
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, the third-party service provider, and subcontractors, 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 for the use of subcontractors and require the third party to notify the FRFI of any subcontracting of services. The FRFI should have the ability to conduct due diligence to evaluate the impacts of the 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 (experienced by the third party or a subcontractor) that impact or could impact services provided, the FRFI's customers/data, or the FRFI's reputation; • technology and cyber security incidents (experienced by 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[9]; • changes in ownership of the third party; • significant organizational/operational changes; and • material non-compliance with regulatory requirements (i.e., regulatory enforcement) or litigation.
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 a 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 if 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 in 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 OSFI 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 during a dispute 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 its insurance coverage(s).
Audit	
The contract or outsourcing agreement is expected to clearly stipulate the audit requirements and rights of both the service provider and the FRFI. At a minimum, it should give the FRFI the right to evaluate the service provided or, alternatively, to commission an independent auditor to evaluate, on its behalf, the service provided. This includes a review of the service provider's internal control environment as it relates to the service being provided. In addition, in all situations, irrespective of whether an activity is conducted in-house, outsourced, or otherwise obtained from a third party, OSFI retains its supervisory powers.	Audit is not included in the minimum contractual requirements, but section 2.3.3 and Principle 8 indicate that 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. Depending on the arrangement and its criticality and risk level, audit rights may be required to satisfy Principle 8. We suggest that as a default in high-criticality or high-risk arrangements, audit provisions or similar measures should still be included to achieve adequate oversight.
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 Revised Guideline B-10.

Conclusion

Revised Guideline B-10 is a true re-framing of Guideline B-10, 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. The single biggest shift for most

organizations will be broadening the analysis to other third-party arrangements that were not typically dealt with through the sourcing or procurement functions through the implementation of a comprehensive third-party risk management framework that manages the entire lifecycle of third-party arrangements.

FRFIs will want to carefully consider the policies and procedures they employ for managing third-party relationships by:

- Conducting intake and proper due diligence for all 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.
- Ensuring adequate management and oversight over third-party relationships throughout the duration of the third-party arrangements.

As part of this process, contract templates, intake processes, 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 revised requirements into account.

FOOTNOTES

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