

OCTOBER 2021

Outsourcing Guideline

BC Credit Unions, Insurance and Trust
Companies and Pension Plan
Administrators

BCFSA 

Contents

Introduction	1
Scope	1
Approach	2
Governance and Accountability	2
Expectations for FIs	2
Expectations for Pension Plan Administrators	4
Assessing the Materiality of Outsourcing Arrangements	4
Expectations for FIs and Pension Plan Administrators	4
Outsourcing Risk Management Framework	6
Expectations for FIs and Pension Plan Administrators	6
Risk Assessments	7
Expectations for FIs and Pension Plan Administrators	7
Expectations for FIs	8
Due Diligence Processes	8
Expectations for FIs and Pension Plan Administrators	8
Outsourcing Contracts	9
Expectations for FIs	9
Information Security	9
Appendix: Items in Outsourcing Contracts	10
Nature and Scope of the Service Being Provided	10
Performance Measures	10
Reporting Requirements	10
Resolution of Differences	10
Defaults and Termination	10
Ownership and Access	11
Contingency Planning	11
Audit Rights	11
Subcontracting	12
Pricing	12
Insurance	12
Confidentiality, Security and Separation of Property	12



Production of this document included environmentally friendly best practices.
Please reduce, reuse and recycle.

Copyright © 2021 BCFS A O All Rights Reserved O Classification: Choose classification

Introduction

BC Financial Services Authority (“BCFSA”) Guidelines establish principles that regulated entities are expected to implement and follow. This Guideline sets out BCFSA’s principles and expectations for Provincially Regulated Financial Institutions (“PRFIs”) ¹ that outsource, or contemplate outsourcing, one or more of their activities or functions.

PRFIs outsource activities, functions, and processes in order to meet the challenges of technological innovation, increased specialization, and heightened competition as well as to improve efficiency and cost control. However, as a result, outsourcing can also increase a PRFI’s dependence on third parties, which may increase its risk profile. BCFSA, consistent with other financial sector regulators, is responding by introducing guidance related to the management of outsourcing risks.

Whereas PRFIs have the flexibility to configure their operations in the way most suited to achieving their objectives, PRFIs retain accountabilities for all activities, regardless of whether they are outsourced or not. Therefore, BCFSA will regulate and supervise significant activities even if they are outsourced to a third-party provider.

Scope

The principles in this Guideline apply to all outsourcing arrangements of a PRFI. An outsourcing arrangement is an agreement between a PRFI and a service provider whereby the service provider performs an activity, function, or process that is, or could be, undertaken by the PRFI. A PRFI may discuss with BCFSA when they are uncertain whether a particular arrangement falls within this definition.

In applying this Guideline, the PRFI is expected to consider the impact of outsourcing arrangements on the PRFI and its services and, for financial institutions (FIs) ², its consolidated operations. BCFSA’s attention will be placed on outsourcing arrangements that are material or support significant activities of the PRFI.

The expectations apply to all organizations regardless of size; however, BCFSA will use the principle of proportionality in undertaking its reviews by adjusting the supervisory intensity depending on the nature, size, complexity, and risk profile of the PRFI and the potential system impact of the PRFI’s failure.

¹ For the purposes of this Guideline, PRFIs include BC incorporated credit unions, insurance companies, and trust companies, and administrators of BC registered pension plans.

² Financial institutions include BC incorporated credit unions, insurance companies, and trust companies.

Approach

This Guideline sets out both high level principles and specific BCFSAs expectations.

Principles form the foundation for good governance; BCFSAs expects principles to be proportionately implemented across all PRFIs. For each principle, specific BCFSAs expectations are provided which outline the procedures and practices³ that achieve the objective of each principle. As pension plans and FIs differ in their organizational structures and legislation, separate expectations for each sector are identified where appropriate in this Guideline.

Governance and Accountability

The PRFI's governing body is ultimately responsible for all outsourced activities and is expected to support its monitoring, control, and management of outsourcing risks through a sound governance structure.

For the purposes of this Guideline, the governing body for FIs is the Board of Directors. The term "Board of Directors" also includes any group or individual who would hold a comparative position in an FI.

For pension plans, the governing body would be the administrator established under the plan documents.

EXPECTATIONS FOR FIS

BCFSAs expects the roles and responsibilities for managing outsourcing risks to be defined, documented, and incorporated in the FI's overall governance structure.

Board of Directors

The Board of Directors should:

- Approve the policies that apply to outsourcing arrangements (e.g., outsourcing risk philosophy, materiality criteria and costs);
- Review a list of all material outsourcing arrangements and other relevant reports at least once per year; and
- Ensure that an outsourcing risk management program is applied.

The Board of Directors retains responsibility for the oversight of material outsourcing arrangements.

³ Procedures operationalize policies. Practices are detailed instructions.

Senior Management

Senior management should:

- Develop and implement the policies that apply to outsourcing arrangements (and any associated procedures) for approval by the Board of Directors as well as periodically review their effectiveness;
- Periodically review outsourcing contracts⁴ for compliance and materiality;
- Notify the Board of Directors of any significant issues with a service provider's compliance with the contract and develop action plans as needed;
- Oversee maintenance of the centralized list of outsourcing arrangements;
- Notify BCFSa within a reasonable time of any events that are likely to have a significant negative impact on compliance, operations, or the delivery of the service provided by a material outsourcing arrangement;
- Manage outsourcing costs; and
- Ensure business continuity should the service provider(s) be unable to fulfill expectations.

Senior management will always retain overall accountability for an outsourcing arrangement.

Policies and Procedures

Policies and procedures should include:

1. An outsourcing risk philosophy reflected in the FI's Enterprise Risk Management framework (ERM)⁵.
2. The FI's outsourcing risk philosophy should comprise its principles related to outsourcing, the basis for its decision making on outsourcing, and the parameters for managing outsourcing risks. Outsourcing risk philosophies will vary across FIs, but should address the following:
 - i. Integration of outsourcing arrangements, both individually and in aggregate, with overall business and strategic objectives. This could include an identification of any functions that, for strategic or internal control reasons, the FI would not contemplate outsourcing.
 - ii. Importance and adequacy of internal expertise and management frameworks to oversee and manage the outsourced activity and the relationship with the service provider.
 - iii. Short-and long-term cost implications, contingency plans and any relevant prudential and/or market conduct matters.
3. A materiality assessment for outsourcing arrangements. This assessment is expected to identify both the processes for determining the materiality of individual outsourcing arrangements and the underlying materiality factors such as those set out in the section titled 'Assessing the Materiality of Outsourcing Arrangements'.
4. The expectations included in the section titled 'Outsourcing Risk Management Framework' integrated into the ERM and applied consistently throughout the FI. BCFSa expects management to pay particular attention to business continuity planning on an enterprise-wide basis (see the section on Business Continuity under 'Assessing the Materiality of Outsourcing Arrangements').

⁴ An outsourcing contract is the document by which an outsourcing arrangement is codified in writing.

⁵ For the purposes of this guideline, "ERM" includes equivalents.

5. Limits regarding the level or authority that enables the FI's officers to approve outsourcing arrangements of varying magnitudes, either individually or in aggregate. This system should be consistent with the outsourcing risk philosophy and materiality criteria.

EXPECTATIONS FOR PENSION PLAN ADMINISTRATORS

Pension plan administrators should:

- Perform and document a materiality assessment for outsourcing arrangements;
- Ensure that policies and procedures for the oversight of outsourcing arrangements are well documented;
- Establish contracts for all material functions done by third parties;
- Monitor performance; and
- Review these documents in a timely manner.

Assessing the Materiality of Outsourcing Arrangements

A PRFI is expected to develop and implement a process for determining the materiality of outsourcing arrangements.

EXPECTATIONS FOR FIS AND PENSION PLAN ADMINISTRATORS

BCFSA recognizes that outsourcing arrangements may not be readily classified as either material or immaterial. In general, BCFSA expects that a PRFI will ensure that, where appropriate, its ERM⁶ applies to all its material outsourcing arrangements and that the risk mitigants employed under this framework are appropriate to the particular outsourcing arrangement. As such, application of the ERM should be scaled to apply different requirements depending on the type of outsourcing arrangement. Arrangements deemed material should be subject to the full expectations set out in the section titled 'Outsourcing Risk Management Framework'. BCFSA may review a PRFI's materiality assessment on a case-by-case basis as part of the supervisory review process.

The materiality of an outsourcing arrangement will depend on the extent to which it impacts the governance and risk oversight of a significant business line. Significant lines of business encompass not just those that are significant in size, but also those that are significant in decision making.

Significant changes in the volume or the nature of business conducted will require the PRFI to reassess an outsourcing arrangement's materiality. In cases where an arrangement is reassessed as material, it should comply with this Guideline.

⁶ For a pension plan, the equivalent to an ERM may be the governance policy.

Intra-group Outsourcing Arrangements

At a minimum, BCFSa expects the following to be addressed when an affiliated company or pension plan administrator enters a material outsourcing arrangement with an entity that is a member of the same PRFI group⁷ or its parent entity⁸:

- An outsourcing contract that details, among other things, the scope of the arrangement, the services to be supplied, the nature of the relationship between the PRFI and the service provider, and procedures governing the subcontracting of services;
- An appropriate business continuity plan;
- A process for monitoring and oversight; and
- Legislative requirements relating to location of records (refer to the section on Location of Records under 'Outsourcing Risk Management Framework').

As appropriate, a parent entity may address these expectations within enterprise-wide processes or plans if any specific risks to each individual subsidiary or pension plan are addressed. A parent PRFI may also establish the program, approve the policies, and develop and maintain the reporting on behalf of its PRFI subsidiaries.

Consistent with the risk-based supervisory approach, BCFSa may have additional expectations for PRFI group arrangements, depending on the risks related to the outsourcing arrangement and the conclusions of BCFSa's supervisory review.

Outsourcing Arrangements with the Auditor

A PRFI may obtain non-audit services from outsourced or "co-sourced" external auditors. In such cases, a PRFI is expected to assure itself that the auditor follows the relevant auditor independence standards of the Canadian accounting profession, as well as any other applicable auditor independence requirements, for the services to be performed.

In addition, a PRFI should not outsource the following activities to its external auditor:

- 1) Any actuarial service unless it is reasonable to conclude that the results of the service will not be subject to audit procedures during an audit of the PRFI's financial statements. For this purpose, actuarial services refer to the determination of an amount to be recorded in the financial statements of the PRFI or work normally undertaken by its appointed actuary. Actuarial services do not include services that involve assisting the PRFI in understanding the methods, models, assumptions, and inputs used or advising management on the appropriate actuarial methods and assumptions that will be used. The PRFI may use an actuary working in the company's external auditor firm for the external review of the appointed actuary's work and reports.
- 2) Any internal audit service related to the internal accounting controls, financial systems, or financial statements of the PRFI unless it is reasonable to conclude that the results of the service will not be subject to audit procedures during an audit of the PRFI's financial statements. This does not prohibit the external auditor from providing a non-recurring service to evaluate a discrete item or program, if the service is not, in substance, the outsourcing of an internal audit function.

⁷ A PRFI group is a group that includes a PRFI as well as any of the following: a) the entity that controls the PRFI if that entity is also a PRFI; b) a subsidiary of the PRFI; and c) a subsidiary of the entity referred to in a).

⁸ A parent entity is an entity of which the PRFI is a subsidiary or, for pension plan administrators of multi-employer plans, one of the companies sponsoring the pension plan.

Outsourcing Risk Management Framework

A PRFI is expected to ensure its ERM appropriately manages and monitors risks commensurate with the materiality of the arrangements, paying particular attention to business continuity.

EXPECTATIONS FOR FIS AND PENSION PLAN ADMINISTRATORS

Risk Management Framework

In general, BCFSA expects that a PRFI's ERM program applies to all material outsourcing arrangements and that the risk mitigants employed will be commensurate with the PRFI's assessment of the risks associated with the outsourcing arrangement.

Business Continuity

A PRFI's business continuity plan⁹ should address situations—either temporary or permanent—where the service provider fails to continue providing service. The business continuity plan and backup systems should be commensurate with the risk of a service disruption. In particular, the PRFI's business continuity plan should ensure that the PRFI has in its possession, or can readily access, all records necessary to allow it to sustain business operations, meet its statutory obligations, and provide all information as may be required by BCFSA in the event the service provider is unable to provide the service. The PRFI should also have, as part of its continuity plan, a strategy for finding a substitute when it is necessary to exit a material outsourcing arrangement.

Monitoring and Reporting

Every PRFI engaged in material outsourcing is expected to develop, implement, and oversee procedures to monitor and control outsourcing risks in accordance with its outsourcing risk-management policies. The sophistication of the procedures should be commensurate with the size and complexity of the outsourcing arrangement(s) and with the expectations of this Guideline.

A PRFI is expected to maintain a centralized list of all its material outsourcing arrangements. A parent entity may maintain the list on behalf of the PRFI group. The list should contain information pertaining to the name of the service provider, the business function of the activity being outsourced, the date of the last review of the outsourcing arrangement and whether any sensitive information is involved. The list should be updated on an ongoing basis. BCFSA may request access to the list at any time, at which point the PRFI is required to produce the records.

A PRFI is expected to monitor all material outsourcing arrangements to ensure that the service is being delivered in the manner expected and in accordance with the terms of the contract. Monitoring should include periodic

⁹ For the purposes of this Guideline, "business continuity plan" includes equivalents.

reviews of the service provider, which would be commensurate with the level of risk involved and could include an assessment of the service provider's circumstances (e.g., financial strength and technical competence as well as use and performance of significant subcontractors). Monitoring may also include regular formal meetings with the service provider.

A PRFI is expected to notify its BCFSAs Relationship Manager or Analyst within a reasonable time of any events that are likely to have a significant negative impact on the delivery of the service.

For FIs, BCFSAs expects management to prepare regular reports based on the FI's monitoring and oversight activities. These reports may outline the success of the outsourcing arrangement and the effectiveness of the ERM and may be reflected in the documentation delivered to the FI's senior management and the Board of Directors.

Location of Records

BCFSAs expects PRFIs to provide the Superintendent access to their records upon request.¹⁰ PRFIs should also ensure compliance with applicable Canadian laws and regulatory requirements, including the *Personal Information Protection Act* and the federal *Personal Information Protection and Electronic Documents Act*. These requirements include records held by outsourcing service providers.

Risk Assessments

A PRFI is expected to identify external and internal threats as well as potential failures in people, processes, and systems on an ongoing basis. In addition, a PRFI is expected to promptly assess the vulnerabilities in material outsourcing arrangements and manage the resulting outsourcing risks in accordance with its risk tolerance.

EXPECTATIONS FOR FIS AND PENSION PLAN ADMINISTRATORS

A PRFI is expected to assess its material outsourcing arrangements to ensure compliance with its risk tolerance, its outsourcing policies and procedures, and the expectations of this Guideline. Assessments of material outsourcing arrangements should be periodically undertaken by the PRFI's internal audit department or another independent review function, either internal or external to the PRFI, provided it has the appropriate knowledge and skills and is commensurate with the resources of the PRFI.

PRFIs are expected to ensure that all relevant outsourcing risks are identified and assessed.

Assessments should test the PRFI's risk management activities for outsourcing to:

- Ensure risk management policies and procedures for outsourcing are being followed;
- Ensure effective management controls over outsourcing activities;
- Verify the adequacy and accuracy of management information reports; and

¹⁰ See section 133 of the *Financial Institutions Act* for FIs and sections 34 and 111 of the *Pension Benefits Standards Act* for pension plan administrators.

- Ensure that personnel involved in risk management for outsourcing are aware of the PRFI's risk management policies and have the expertise required to make effective decisions consistent with those policies.

Management should adjust the scope of the assessment depending on the nature of the outsourcing arrangement as well as the size and nature of the PRFI.

EXPECTATIONS FOR FIS

For FIs, the risks include systemic risk arising from concentration in the provision of some outsourced and third-party services provided to FIs. Potential systemic risk could arise if, for instance, a sufficiently large number of FIs became dependent on one or a small number of service providers for the provision of critical services that are impossible or very difficult to substitute effectively and within an appropriate timeframe. Where there is no appropriate mitigant in place, a major disruption, outage, or failure at one of these service providers could create not only a single point of failure with potential adverse consequences for the overall sector but could also have significant effects on the FI.

While there may be instances where there are no reasonable alternatives or effective methods of mitigating such a risk, an FI should ensure it is aware of the risk and, where possible, take reasonable efforts to manage it. This expectation is not meant to discourage FIs from engaging service providers that provide services to many other FIs or from obtaining multiple services from one service provider. It is instead intended to ensure that FIs remain aware of the potential risks and take reasonable steps, where appropriate, to mitigate those risk.

Due Diligence Processes

A PRFI is expected to conduct ongoing due diligence, including evaluating the service provider's reputation and ability to provide quality service.

EXPECTATIONS FOR FIS AND PENSION PLAN ADMINISTRATORS

BCFSA expects a PRFI to conduct internal due diligence to determine the nature and scope of the business activity to be outsourced (including any subcontracted outsourcing arrangements), its relationship to the rest of the PRFI's activities, and how the activity is managed.

In selecting a service provider or substantially amending or renewing an outsourcing arrangement, PRFIs are expected to undertake a due diligence process that fully assesses the risks associated with the outsourcing arrangement and addresses all relevant aspects of the service provider, including qualitative (i.e., operational) and quantitative (i.e., financial) factors. PRFIs should also ensure they perform due diligence for any subcontracted outsourcing arrangements and should perform ongoing due diligence for third-party provision of services.

Due diligence processes will vary depending on the PRFI and on the nature of the outsourcing arrangement being contemplated. For example, in the case of renewals where no material change has occurred that would affect the viability of the outsourcing relationship, it may be appropriate to conduct more streamlined due diligence provided there are no other concerns, such as conflicts of interest.

Outsourcing Contracts

A PRFI is expected to document outsourcing arrangements with written contracts that address all relevant conditions, including performance measures for the service provider to ensure it fulfills the contract conditions.

EXPECTATIONS FOR FIS

BCFSA expects material outsourcing arrangements to be documented by a written contract that addresses all elements of the arrangement and has been reviewed by the PRFI's legal counsel. These contracts should explicitly lay out expectations between the PRFI and the service provider, including compensation arrangements (covering applicable fees and expenses) and reporting relationships. Additionally, the PRFI should have a formal process for hiring third party service providers, including the identification of requirements and any other criteria influencing hiring decisions. Finally, a process for the termination of services from a third-party service provider should be established.

For a list of suggested items to include in an outsourcing contract, please see the Appendix. Some of the items identified may not be applicable in all circumstances; however, PRFIs 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 PRFI and their stakeholders.

INFORMATION SECURITY

A PRFI should assure itself that its outsourcing service providers comply with all applicable legislation, Rules, and BCFSA's Information Security Guideline in their treatment of information.

A PRFI should assure itself that its outsourcing service providers comply with applicable legislation, particularly the *Personal Information Protection Act* and the federal *Personal Information Protection and Electronic Document Act*. The service provider is also expected to be able to logically isolate the PRFI's data, records, and items in process from those of other clients at all times, including under adverse conditions.

Appendix:

Items in Outsourcing Contracts

The following expectations apply to contracts for material outsourcing arrangements. Some of the items identified may not be applicable in all circumstances; however, PRFIs 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 PRFI.

NATURE AND SCOPE OF THE SERVICE BEING PROVIDED

The contract 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 contract is expected to detail the physical location where the service provider will provide the service.

PERFORMANCE MEASURES

Performance measures should be established to allow each party to determine whether the commitments contained in the contract are being fulfilled.

REPORTING REQUIREMENTS

The contract is expected to specify the type and frequency of information the PRFI receives from the service provider. This would include reports that allow the PRFI to assess whether the performance measures are being met and any other information required for the PRFI's monitoring framework (see the section titled 'Outsourcing Risk Management Framework'). In addition, the contract is expected to include procedures and requirements for the service provider to report events to the PRFI that may have the potential to materially affect the delivery of the service.

RESOLUTION OF DIFFERENCES

The contract is expected to incorporate a protocol for resolving disputes. The contract 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.

DEFAULTS AND TERMINATION

The contract is expected to specify what constitutes a default, identify remedies, and allow for opportunities to cure defaults or terminate the arrangement. The PRFI 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 PRFI's

assets should be returned in a timely fashion. Data and records relating to data processing outsourcing arrangements should be returned to the PRFI in a format that would allow the PRFI to sustain business operations without prohibitive expense.

The contract should not contain wording that precludes the service from being continued in situations where the Superintendent takes control of the PRFI or where the PRFI is in liquidation.

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 contract should state whether and how the service provider has the right to use the PRFI's assets (e.g., data, hardware and software, system documentation, or intellectual property) and the PRFI's right to access those assets.

CONTINGENCY PLANNING

The contract 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, natural disaster, and other reasonably foreseeable events. The PRFI should ensure that the service provider regularly tests its business recovery system as it pertains to the outsourced activity, notifies the PRFI of the test results and addresses any material deficiencies. In addition, the PRFI should be notified if 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. PRFIs should also ensure that the service provider has the capacity to provide timely service even in the event of multiple demands on its services (e.g., for reinsurance, if there are multiple natural disasters affecting the reinsurer's clients). BCFSFA may request the service provider's contingency planning test results at any time.

AUDIT RIGHTS

The contract is expected to clearly stipulate the audit requirements and rights of both the service provider and the PRFI. At a minimum, it should give the PRFI the right to evaluate the service provided, or alternatively to have an independent auditor evaluate it on its behalf. 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—BCFSFA retains its supervisory powers. Accordingly, an undertaking from the service provider or a provision in the outsourcing contract should give the BCFSFA or the Superintendent's representative the right to:

- Exercise the contractual rights of the PRFI relating to the audit;
- Accompany the PRFI (or its independent auditor) when it exercises its contractual audit rights;
- Access and make copies of any internal audit reports (as well as associated working papers and recommendations) prepared by or for the service provider in respect of the service being performed for the PRFI, subject to BCFSFA agreeing to sign appropriate confidentiality documentation in form and content satisfactory to the service provider; and

- Access findings in the external audit of the service provider (as well as associated working papers and recommendations) that address the service being performed for the PRFI, subject to the consent of the service provider's external auditor and BCFSa agreeing to sign appropriate confidentiality documentation in form and content satisfactory to the service provider and the external auditor.

BCFSa will provide the PRFI with reasonable notice of its intent to exercise its audit rights and share its findings with the PRFI where appropriate. In the normal course, BCFSa would seek to obtain information it requires through the PRFI itself.

SUBCONTRACTING

The contract is expected to set out any rules or limitations to subcontracting of the outsourced service or component of the service by the service provider. Security and confidentiality standards should apply to subcontracting or outsourcing arrangements by the primary service provider.

Consistent with the principles of this Guideline, the audit and inspection rights of the PRFI and BCFSa should continue to apply to all significant subcontracting arrangements.

PRICING

The contract should fully describe the basis for calculating fees and compensation relating to the service being provided.

INSURANCE

The service provider should be required to notify the PRFI of significant changes in insurance coverage and disclose general terms and conditions of the insurance coverage. The PRFI may also wish to require a minimum level of insurance coverage and outline the liability of the service provider and the PRFI.

CONFIDENTIALITY, SECURITY AND SEPARATION OF PROPERTY

At a minimum, the contract is expected to set out the PRFI's requirements for confidentiality and security. The PRFI should ensure that it remains in compliance with applicable privacy laws (for example, the *Freedom of Information and Protection of Privacy Act* and the federal *Privacy Act*) and laws governing the location of records.



BC Financial
Services Authority

600-750 West Pender Street
Vancouver, BC V6C 2T8

604 660 3555
Toll free 866 206 3030
info@bcfsa.ca