

Guideline

Third-party Risk Management

Date: October 28, 2025
Distribution: B.C. Incorporated Insurance Companies
Effective: January 1, 2028

TABLE OF CONTENTS

INTRODUCTION	2
BACKGROUND INFORMATION	2
DEFINITIONS	3
OUTCOMES	4
RELATED GUIDANCE	4
SECTION 1 – GOVERNANCE	5
1.1 Accountability	5
1.2 Third-Party Risk Management Framework	5
SECTION 2 – MANAGEMENT OF THIRD-PARTY RISK	6
2.1 Risk-based Approach	6
2.2 Risk Identification and Assessment	7
2.3 Risk Management and Mitigation	9
2.4 Monitoring and Reporting	12
SECTION 3 – SPECIAL ARRANGEMENTS	13
3.1 Standardized Contracts	14
3.2 No Written Contract	14
3.3 Third-party Arrangements with the External Auditor	14
SECTION 4 – TECHNOLOGY AND CYBER RISK IN THIRD-PARTY ARRANGEMENTS	15
4.1 Clear Roles and Responsibilities are Established for Technology and Cyber Controls	15
4.2 Third parties Comply with the Insurance Company’s Technology and Cyber Standards	15
4.3 Cloud-specific Requirements are Established	15
4.4 Cloud Portability is Considered	15
APPENDIX 1: EXAMPLES OF DUE DILIGENCE CONSIDERATION	16
APPENDIX 2: PROVISIONS FOR THIRD-PARTY AGREEMENTS	17

INTRODUCTION

This Guideline provides a BCFSa version of a guideline published by the Office of the Superintendent of Financial Instruments (“OSFI”) titled B-10 Third-party Risk Management. The BCFSa version follows OSFI’s closely, with appropriate adjustments to ensure it is suitable for the B.C. jurisdiction. The Guideline sets out expectations for managing risks associated with third-party arrangements and is applicable to all B.C. incorporated insurance companies (“insurance companies”).

Insurance companies engage in business and strategic arrangements with external parties—entities or individuals—to perform business activities, functions, and services or obtain goods in support of their own operations or their business strategy.

External arrangements, or third-party arrangements, can be beneficial to an insurance company by introducing efficiencies, driving innovation, managing shifting operational needs, and improving services. However, risks can arise from third-party arrangements that can threaten the insurance company’s operational and financial resilience.

BCFSa expects insurance companies to manage the risks related to all third-party arrangements and emphasizes that an insurance company retains accountability for business activities, functions and services outsourced to a third party.

To that end, insurance companies are required to provide BCFSa, upon request, information related to their business and strategic arrangements with third parties, risk management, and control environments, to support supervisory monitoring and review work. BCFSa expects to be promptly notified of substantive issues affecting an insurance company’s ability to deliver critical operations due to a third-party arrangement.

In all cases, BCFSa’s supervisory powers should not be constrained, irrespective of whether an activity is conducted in-house, outsourced, or otherwise obtained from a third party.

BACKGROUND INFORMATION

Third-party arrangements have a variety of forms, which include but are not limited to, critical services for the insurance company, minor support arrangements, and strategic arrangements where no service is actually being provided. BCFSa expects insurance companies to consider risk and criticality when examining third-party arrangements to determine the intensity with which to apply the expectations set out in this Guideline. For example, an exit or contingency plan may not be needed for a low-risk arrangement, nor will subcontracting risk be a significant factor in managing every third-party arrangement. Similarly, a legal review may not be necessary for a low-risk, short-term arrangement.

Fundamental to applying this Guideline in a prudent manner is identifying the type and level of risk arising from each third-party arrangement (including subcontracting arrangements), such that the insurance company can manage each third-party arrangement with the appropriate level of intensity.

Therefore, BCFSa expects the insurance company to understand the risk and criticality of all its third-party arrangements and apply this Guideline in a manner that is proportionate to both:

- the risk and criticality of each third-party arrangement; and
- the size, nature, scope, complexity of operations and risk profile of the insurance company.

BCFSa acknowledges that not all contracts with third parties will be negotiable, and for certain third-party arrangements there may be no contracts. Section 3.1 has been added in recognition of these situations. While the opportunity to manage third-party risk through terms of a contract may be limited in such cases, BCFSa nonetheless expects the insurance company to manage risk, as appropriate, through monitoring, business continuity measures, contingency planning, and other resiliency mechanisms.

DEFINITIONS

‘Cloud portability’ as defined by the US National Institute of Standards and Technology (NIST) is “the ability for data to be moved from one cloud system to another or for applications to be ported and run on different cloud systems at an acceptable cost.”¹

‘Concentration risk’ has two forms. Institution-specific concentration risk is the risk of loss or harm to the insurance company 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 insurance companies.²

‘Contingency plan’ is a series of actions for the insurance company to take to maintain critical operations in the event of an unplanned disruption at a critical third-party.

‘Criticality’ denotes importance to the insurance company’s operations, strategy, financial condition or reputation. It emphasizes the impact of a risk event, irrespective of the likelihood of such risk event occurring. The criticality of an arrangement is an important input in the assessment of an arrangement’s risk. Critical third-party arrangements provide goods, business activities, functions and services to insurance companies which, if disrupted, could put at risk the continued operation of the insurance company, its safety and soundness or its role in the financial system, and thereby jeopardize its operational resilience.

‘Critical operations’ are the services, products or functions of a insurance company which if disrupted, could put at risk the continued operation of the insurance company, its safety and soundness, or its role in the financial system.

‘Exit plan’ is a series of actions for the insurance company to take in the event of a planned (i.e. non-stressed) or unplanned (i.e. stressed) exit from a third-party arrangement, along with triggers for invoking the plan in either event. Please see Section 2.3.5 for further details.

‘Risk acceptance’ refers to a decision to accept an identified risk and not take any, or further, mitigating actions.

‘Subcontractor’ is an entity within the third party’s contracting, external arrangements or supply chain.

‘Subcontracting risk’ stems from the third-party’s own business or strategic arrangements with entity(ies) or individuals, by contract or otherwise.

‘Third-party arrangement’ refers to any type of business or strategic arrangement between the insurance company(ies) and an entity(ies) or individuals, by contract or otherwise, save for arrangements with insurance company customers (e.g., depositors and policyholders) and employment contracts, which are excluded from this definition.

Third-party arrangements include, among other things:

- outsourced activities, functions, and services that would otherwise be undertaken by the insurance company itself;
- use of independent professional consultants;
- brokers (e.g., mortgage, insurance, deposit brokers);
- utilities (e.g., power sources, telecommunications);

¹ NIST 500-291, version 2: NIST Cloud Computing Standards Roadmap

² In the case of systemic concentration risk, insurers should seek to understand this risk to the greatest extent possible.

- financial market infrastructures (e.g., payments systems, clearing and settlement systems, other insurance companies in cases where the insurance company does not have direct access to financial market infrastructures);
- services provided by parent holding companies, affiliates, and subsidiaries, or through joint ventures and partnerships; and
- other relationships involving the provision of goods and services or the storage, use or exchange of data (such as cloud service providers, managed service providers, technology companies that deliver financial services).

‘Third-party risk’ is the risk to the insurance company due to a third party failing to provide goods, business activities, functions and services, protect data or systems, or otherwise exposing the insurance company to negative outcomes. Third-party risk scenarios could include, but would not be limited to:

- insolvency of the third party;
- operational disruption at the third party due to people, inadequate or failed processes and systems, or from external events (e.g., cyber incidents);
- political, geographic, legal, environmental, or other risks impeding the third party from providing services according to its arrangement with the insurance company;
- insolvency or operational disruption at a subcontractor;
- risks arising from interconnections between multiple third parties and multiple insurance companies;
- corruption of insurance company data or insurance company data breaches; and
- loss of data by the third party.

OUTCOMES

This Guideline presents six expected outcomes for insurance companies to achieve through effective third-party risk management. These outcomes contribute to the insurance company’s operational and financial resilience and help safeguard its reputation.

The outcomes are:

Governance and accountability structures are clear with comprehensive risk management strategies and frameworks in place.

Risks posed by third parties are identified and assessed.

Risks posed by third parties are managed and mitigated within the insurance company’s risk appetite framework.

Third party performance is monitored and assessed, and risks and incidents are proactively addressed.

The insurance company’s third-party risk management program allows the insurance company to identify and manage a range of third-party relationships on an ongoing basis.

Technology and cyber operations carried out by third parties are transparent, reliable and secure.

RELATED GUIDANCE

This Guideline should be read in conjunction with applicable legislation and relevant guidance, including but not limited to BCFSA’s [Information Security Guideline](#) and Operational Risk Management and Resilience Guideline, as well as OSFI’s Corporate Governance Guideline.

SECTION 1 – GOVERNANCE

Outcome 1: Governance and accountability structures are clear with comprehensive risk strategies and frameworks in place.

1.1 Accountability

Principle 1: The insurance company is ultimately accountable for managing the risks arising from all types of third-party arrangements.

1.1.1 The insurance company retains accountability for services outsourced to a third party and manages risk arising from all third-party arrangements

The insurance company has the flexibility to arrange its operations in a way that achieves its business and strategic objectives. However, the insurance company retains accountability for business activities, functions, and services outsourced to third parties, for data exchanged with third parties or data to which third-parties have access, and for managing risk arising from third-party arrangements.

The insurance company's senior management should be satisfied that business activities, functions, and services performed by third parties are done in a safe and sound manner, and in compliance with applicable legislative and regulatory requirements and the insurance company's own internal policies, standards, and processes. The insurance company's senior management should also be satisfied that third-party arrangements are in alignment with the insurance company's risk appetite and managed proportionate to the level of criticality and risk.

Please refer to OSFI's Corporate Governance Guideline for expectations of Boards of Directors in regard to business strategy, risk appetite and operational, business, risk and crisis management policies. Please also refer to the [B.C. Insurer Code of Market Conduct](#) for the Fair Treatment of Customers ("FTC") Principles.

1.2 Third-Party Risk Management Framework

Principle 2: The insurance company should establish a Third-Party Risk Management Framework ("TPR 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.

1.2.1 The TPR Framework is enterprise-wide and governs the lifecycle of third-party arrangements

The insurance company should establish a TPR Framework that provides an enterprise-wide view of its exposures to third parties. The TPR Framework should reflect the insurance company's risk appetite and be consistent with its risk management frameworks.

The TPR Framework should be developed to span the lifecycle of a third-party arrangement, from sourcing and due diligence of a third-party provider to potential exit from the third-party arrangement. The TPR Framework should set out how the insurance company will identify and assess; manage and mitigate; and monitor and report on third-party risk.

BCFSA expects the insurance company to review and update its TPR Framework on a regular basis to ensure it is relevant and appropriate and to make continuous improvements based on implementation, effectiveness and other lessons learned (e.g., past incidents).

1.2.2 The TPR Framework establishes accountabilities, policies and processes for identifying, monitoring and managing third party risk

These should include:

- accountability for third-party risk management, including for oversight functions;

- clear roles and responsibilities for overseeing and managing third-party arrangements and associated risk management processes;
- third-party risk appetite and measurement (e.g., limits, thresholds and key risk indicators);
- methodology for assessing the level of risk and criticality of third-party arrangements;
- policies to govern third-party risk, which are approved, regularly reviewed and consistently implemented enterprise-wide;
- processes and systems for identifying, assessing, managing, monitoring, measuring, and reporting on:
 - an inventory of third parties delineated by level of risk and criticality;
 - third-party compliance with contractual provisions and/or service level agreements, including processes for managing exceptions and incidents;
 - third-party risks introduced by individual arrangements (including, among others, technology, cyber, information security, concentration, business continuity, strategic and financial risks); and
 - aggregation of third-party risk exposures and trends to inform the insurance company's current and emerging risk profile.

SECTION 2 – MANAGEMENT OF THIRD-PARTY RISK

BCFSA expects the insurance company to manage third-party risks in a manner that is proportionate to the level of risk and complexity of the insurance company's third-party ecosystem. BCFSA expects the insurance company to assess its third-party arrangements regularly, with higher-risk and more critical arrangements subjected to more frequent and rigorous assessment and more robust risk management.

For critical third-party arrangements and those that pose a high risk to the insurance company, BCFSA expects that all expectations set out in Section 2 be considered minimum expectations.

2.1 Risk-based Approach

2.1.1 Risk assessment criteria are comprehensive and scalable

The insurance company's criteria to assess the risks of third-party arrangements should be comprehensive to accurately determine the risk of each arrangement. Assessment criteria should also be reviewed periodically to ensure that they remain current for the risk landscape.

Criticality is an important input to the assessment of risk and can be used to scale risk assessments.

In determining the level of criticality, the insurance company should consider as deemed appropriate:

- the severity of loss or harm to the insurance company 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 insurance company; and
- the impact on business operations if the insurance company needed to exit the third-party arrangement and transition to another service provider or bring the business activity in-house.

2.1.2 Level of risk of third-party arrangements are assessed

In determining the level of risk, the insurance company should consider, as deemed appropriate:

- the probability of the third party or subcontractor failing to meet expectations, due to insolvency or operational disruption;
- the ability of the insurance company to assess controls at 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 insurance company 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 insurance company’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.

2.1.3 Rigor of risk management activities matches the level of risk and criticality

The robustness and frequency of the insurance company’s third-party risk management activities (e.g., risk assessment, mitigation, monitoring, measuring, and reporting) should be proportionate to the level of risk and criticality associated with the third-party arrangement.

2.2 Risk Identification and Assessment

Outcome 2: Risks posed by third parties are identified and assessed.

Principle 3: The insurance company should identify and assess the risks of a third-party arrangement before entering the arrangement and periodically thereafter. Risk assessments should be proportionate to the criticality of an arrangement. Specifically, the insurance company 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.

2.2.1 Risk assessment

2.2.1.1 Risk and criticality of the arrangement are assessed throughout its lifecycle

The insurance company should conduct assessments of each third-party arrangement to determine the risk and criticality of the arrangement, considering both risks created and reduced by the arrangement (for example, using suppliers in various jurisdictions would reduce geographic concentration risk but also increase geopolitical and legal risks), as well as risk mitigants. Where a third party is subject to government regulation or supervision, the insurance company may take this into consideration as part of its risk assessment.

The insurance company should conduct risk assessments:

- prior to entering into the third-party arrangement (see Section 2.2.2);
- regularly throughout the lifecycle of the arrangement, including renewal, at a frequency and scope proportionate to the level of criticality; and
- whenever there is material change in the arrangement or third party (including disruption at the third party or in the service provided).

Such risk assessments should, at minimum:

- determine whether the arrangement aligns with the insurance company’s risk appetite for third-party risk and other relevant risks;

- document the criticality of the arrangement;
- establish the level of risk; and
- develop a plan, with appropriate intensity of monitoring and mitigating actions, to manage the arrangement within the insurance company's risk appetite.

2.2.2 Due diligence

Principle 4: The insurance company 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.

2.2.2.1 A due diligence process is established

The insurance company should establish due diligence processes for third-party arrangements to apply initially and on an ongoing basis, including documented risk escalation, approval and acceptance processes.

2.2.2.2 Due diligence is performed proportionate to level of risk and criticality

The insurance company should conduct due diligence proportionate to the level of risk and criticality of each third-party arrangement:

- prior to entering into the arrangement;
- as part of the contract renewal process; and
- periodically on an ongoing basis proportionate to the level of risk and criticality or whenever there are material changes to the third-party arrangement, such as the nature of the arrangement or its criticality.

Due diligence should consider all relevant qualitative (i.e., operational) and quantitative (i.e., financial) factors related to the third-party arrangement. A non-exhaustive list of factors to consider in respect of high-risk and critical arrangements is set out in Appendix 1 of this Guideline.

2.2.2.3 Out-of-Canada arrangements are considered

When considering third-party arrangements with a geographic presence outside of Canada (or subcontractors with a geographic presence outside of Canada) the insurance company should review the legal requirements of relevant jurisdictions, as well as the political, legal, security, economic, environmental, social, and other risks that may impede the ability of the third party to provide services.

2.2.3 Concentration risk

2.2.3.1 Concentration risk is assessed

To determine the appropriate level of mitigation, the insurance company should assess concentration risk both prior to entering a contract or agreement and on an ongoing basis. Processes established should take reasonable steps to assess concentration risk over multiple dimensions including geography, supplier, and subcontractor. Throughout the process, concentration should be considered within the insurance company's business functions/units and legal entities, and across the insurance company's entire organization. To the greatest extent possible, the insurance company should also assess systemic concentration risk.

2.2.4 Subcontracting risk

Principle 5: The insurance company is responsible for identifying, monitoring and managing risk arising from subcontracting arrangements undertaken by its third parties.

2.2.4.1 Risks introduced by subcontracting practices are identified and understood

The insurance company should assess risks arising from third-party subcontractors that could impact it.

Prior to entering a third-party arrangement the insurance company should identify and understand the third party's subcontracting practices, including:

- number and criticality of subcontractors;
- the adequacy and performance of the third party's own third-party risk management program, including assurance that significant performance, legal and regulatory requirements are aligned with the contract entered into with the insurance company; and
- impact of subcontracting arrangements on the insurance company's own concentration risk (refer to Section 2.2.3 above).

2.2.4.2 Monitor and manage subcontracting risks

The insurance company should ensure that they will receive appropriate ongoing updates and reporting on the third party's use of subcontractors so the insurance company can appropriately manage subcontracting risk. Depending on the level of risk and the criticality of services provided by the third party, the insurance company can achieve this by contractual provisions:

- prohibiting the use of subcontractors for certain functions;
- requiring that the insurance company be informed, in writing and on a timely basis, when a subcontractor is retained, or substituted, to carry out some of the functions contracted for the third party to perform;
- reserving a right of the insurance company to refuse a subcontractor; and
- allowing the insurance company to commission or conduct an audit of subcontractors.

2.3 Risk Management and Mitigation

Outcome 3: Risks posed by third parties are managed and mitigated within the insurance company's Risk Appetite Framework.

2.3.1. Written agreements/contracting

Principle 6: The insurance company should enter into written arrangements that set out the rights and responsibilities of each party.

2.3.1.1 Clear responsibilities are set out in the agreement

BCFSA expects third-party arrangements to be supported by a written contract or other agreement (e.g., service level agreement) that sets out the rights and responsibilities of each party and which has been reviewed by the insurance company's legal counsel. BCFSA recognizes that there are certain third-party arrangements for which a customized contract may not be feasible, or for which a formal contract or agreement may not exist. Please see Section 3 of this Guideline for expectations related to such third-party arrangements.

2.3.1.2 The third party is expected to comply with the insurance company's provisions

To manage the risks associated with each third-party arrangement, the insurance company should structure its written agreement with the third party in a manner that allows it to meet the expectations set out in this Guideline. BCFSA expects the insurance company to include in written agreements for high-risk and critical arrangements the provisions that are set out in Appendix 2 of this Guideline.³

2.3.2 Data security and controls (including data location)

³ Except for those contracts where Section 3 applies.

Principle 7: Throughout the duration of the third-party arrangement, the insurance company and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data.

2.3.2.1 Responsibilities for security of records and data are established

Third-party agreements are expected to set out each party's responsibilities for the confidentiality, availability and integrity of records and data. Agreements should establish, among other things:

- the scope of the records and data to be protected;
- availability of the records and timely access to data by the insurance company and BCFSA, upon request;
- controls and monitoring over the third party's use of the insurance company's systems and information;
- clear responsibilities of each party in managing data security;
- which party is liable for any losses that might result from a security breach; and
- notification requirements if there is a breach of security.

As appropriate, these agreements should also specify that the insurance company's data and records be isolated from those of other clients at all times, including during the transfer process and under adverse conditions (e.g., disruption of services). Based on the level of risk, data and records should be subject to the equivalent standard of protection at the third party that they would be at the insurance company.

2.3.2.2 Record keeping requirements

The *Financial Institutions Act* ("FIA") contains requirements with respect to certain records that insurance companies must prepare and maintain (the "records").⁴ BCFSA expects the records to be updated and accurate as at the end of each business day (records that change less frequently than daily remain accurate until they change), and that the records will be sufficiently detailed to enable:

- BCFSA to conduct an examination and inquiry into the business and affairs of the insurance company;
- A provisional liquidator to manage the insurance company's assets, prior to the appointment of a court-appointed liquidator, where applicable; and
- A liquidator, receiver or receiver manager to conduct an effective liquidation of the insurance company's assets.

Electronic records must be capable of being reproduced in intelligible written form within a reasonable period of time. BCFSA expects electronic records to be accessible and intelligible without incurring additional costs and by using readily available commercial applications. For certain types of information, such as reinsurance arrangements or files on more complex activities, reproduced electronic records may not be sufficient for BCFSA's review and the executed copy may need to be available, upon BCFSA's request.

The FIA requires insurance companies to maintain facilities that the Superintendent considers satisfactory by which the Superintendent may obtain access to records.

2.3.3 Information rights and audit

Principle 8: The insurance company's third-party arrangements should allow the insurance company timely access to accurate and comprehensive information to assist it in overseeing third-party performance and

⁴ FIA s. 127-130, 133.

risks. The insurance company should also have the right to conduct or commission an independent audit of a third party.

2.3.3.1 The third party provides the insurance company with information and reporting

The third-party agreement should specify the type and frequency of information to be reported to the insurance company by the third party. This should include reports that allow the insurance company to assess whether performance measures are being met and any other information required for the insurance company's monitoring program, including risk measures (see Section 2.4).

2.3.3.2 The third-party reports events that could materially impact the insurance company

The agreement should include requirements and procedures for the third party to report events in a timely manner to the insurance company that may materially affect the risks and delivery of the service.

2.3.3.3 Service performance and controls are evaluated, and audit rights established, as appropriate

The agreement should give the insurance company and BCFSA the right to evaluate the risk management practices related to the service provided. Specifically, the insurance company and BCFSA should be able to evaluate the risks arising from the arrangement or appoint independent auditors to evaluate the risk management practices related to service provided and the risks arising from the relationship on the insurance company's or on BCFSA's behalf. The insurance company and BCFSA should also be able to access audit reports in respect of the service being performed for the insurance company.

The insurance company should employ a range of audit and information gathering methods (e.g., independent reports provided by third parties, individually performed or pooled audits).

2.3.4 Business continuity planning and testing

Principle 9: The insurance company'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 insurance company should have contingency plans for its critical third-party arrangements.

2.3.4.1 Business continuity and recovery capabilities are established and tested

Third-party agreements should require the third party, at minimum, to:

- outline the third party's measures for ensuring continuity of services in the event of disruption;
- test regularly the third party's business continuity and disaster recovery programs as they pertain to services provided to the insurance company;
- notify the insurance company of test results; and
- address any material deficiencies.

Among other things, the insurance company's business continuity and disaster recovery plans should:

- address severe but plausible situations (either temporary or permanent), including prolonged disruptions and multiple simultaneous disruptions, where the third party could fail to continue providing service;
- document backup systems and redundancy capabilities that are commensurate with the criticality of the service provided; and

- ensure the insurance company has in its possession, or can readily access, all necessary records to allow the insurance company to sustain business operations, meet statutory obligations, and provide all information as may be required by BCFSa, in the event of disruption to third-party services.⁵

As applicable, joint design and testing of business continuity plans and disaster recovery plans should be considered between the third party and the insurance company, commensurate with the criticality of the service.

2.3.5 Contingency and exit strategy / planning

2.3.5.1 Contingency and exit strategies are developed to ensure continuity of critical services

The insurance company should establish contingency and exit plans proportionate to the level of risk and criticality of individual third-party arrangements to ensure continuity of the insurance company's operations through normal and stressed times.

Insurance companies should include the following elements in their documented plans for arrangements deemed high-risk or critical, and consider including them in their plans for arrangements deemed to have lower risk or criticality:

- triggers for invoking exit/contingency plans;
- activities to perform to maintain critical operations during disruptions or when exiting because of unplanned circumstances, such as failure or insolvency of the service provider (a "playbook" for stressed exit);
- activities to perform when exiting through a planned and managed exit due to commercial, performance, or strategic reasons (a "playbook" for non-stressed exit);
- reference to contractual provisions that could impact exit, such as notification requirements and provisions obliging the third party to provide services over a prescribed period of time following notification of termination;
- sufficient detail (e.g., alternative options or providers, supported by timelines, costs, resourcing, revenue impacts, and interim workarounds) so as to allow rapid execution; and
- documented plans for responding to severe but plausible scenarios, including prolonged and multiple disruptions.

Contingency plans and exit strategies should be reviewed regularly, and more frequently in the event of material changes to the third-party arrangements.

2.4 Monitoring and Reporting

Outcome 4: Third-party performance is monitored and assessed, and risks and incidents are proactively addressed.

Principle 10: The insurance company should monitor its third-party arrangements to verify the third party's ability to continue to meet its obligations and effectively manage risks.

2.4.1 Oversight of third-party provider

2.4.1.1 The insurance company monitors its third-party arrangement(s)

The insurance company should monitor its third-party arrangement(s) to ensure that the service is being delivered in accordance with the terms of the agreement, and that the third party remains financially sound.

⁵ Please see Sections 2.3.2.1 and 2.3.2.2 of this Guideline.

Monitoring should also cover regular oversight of current and emerging risks and risk acceptances and compliance of the third-party arrangement with the insurance company's risk policies and procedures and BCFSA's expectations. Monitoring should be conducted at the individual arrangement level, as well as at an aggregate business unit, segment, platform, and enterprise level. The extent and frequency of monitoring should be proportionate to the level of risk and criticality of the third-party arrangement.

2.4.1.2 Metrics confirm residual risk remains within risk appetite

The insurance company should establish processes to confirm regularly that the residual risk of their third-party arrangements, individually and in aggregate, remains within the insurance company's risk appetite. To facilitate this outcome, the insurance company should establish and report metrics and associated thresholds to alert senior management when a threshold is being approached as well as triggers for invoking the insurance company's escalation process.

2.4.2 Incident management and reporting

Principle 11: Both the insurance company 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 insurance company's risk appetite.

2.4.2.1 The third party has clearly defined incident management processes

As part of an effective third-party risk management program, the insurance company should ensure that its third parties have clearly defined and documented processes for identifying, investigating, escalating, remediating and notifying the insurance company in a timely manner of incidents — including subcontractor incidents — that could directly or indirectly impact the third party's ability to deliver the contracted goods, business activities, functions and services.

2.4.2.2 Incident reporting and notification requirements of the third party support insurance company compliance with BCFSA's incident reporting requirements

The insurance company should ensure that its written agreements with third parties contain adequate provisions to enable the insurance company to comply with its reporting expectations under BCFSA's Information Security Guideline. Such provisions could include, among other things, requirements to promptly notify the insurance company of technology and cybersecurity incidents (at the third party or the subcontractor) including providing information on each incident.

2.4.2.3 Internal incident management process is established

The insurance company should also have clearly defined internal processes for effectively managing and escalating third-party incidents and for subsequently tracking remediation. The processes established should clearly define accountabilities at all levels of the insurance company and triggers for escalation within the insurance company.

2.4.2.4 Incidents are investigated, analysed and results are shared

To ensure that remediation actions are sufficient, the insurance company should request that the third party perform root cause analysis and share the results for any incidents, commensurate with the severity/potential impact of the incident on the insurance company. The insurance company should also perform its own root cause analysis, as appropriate. Remediation actions should be monitored by the insurance company.

SECTION 3 – SPECIAL ARRANGEMENTS

Outcome 5: The insurance company's third-party risk management program allows it to identify and manage a range of third-party relationships on an ongoing basis.

3.1 Standardized Contracts

Standardized contracts are those mandated by third parties with pre-defined terms and conditions, with a limited ability for the insurance company to negotiate and tailor its own contract terms and conditions. Examples include contracts with utilities, internet providers, financial market infrastructures and others.

3.1.1 Risks of third parties with standardized contracts are managed

Where standardized contracts must be used, BCFSa expects the insurance company's third-party risk management program to address the relationship. The insurance company's risk assessment should consider inherent risks, mitigating controls and other factors to arrive at the final risk rating for these arrangements and, where applicable, formally accept risks presented by standardized contracts.

Among the mitigating actions and controls that the insurance company may consider are the development of redundancies, workarounds, business continuity measures, and other resiliency mechanisms.

3.2 No Written Contract

3.2.1 Third parties with no written contracts still carry risks

The absence of a written arrangement, formal contract or agreement⁶ does not imply the absence of a third-party arrangement and third-party risk. While the insurance company may not have direct relationships with all third parties they interact with, BCFSa expects the insurance company's third-party risk management program to address these relationships.

3.3 Third-party Arrangements with the External Auditor

Arrangements with the external auditor can give rise to conflicts of interest.

3.3.1 External auditors comply with auditor independence standards when providing third-party services

Prior to obtaining management consulting services from its external auditor, the insurance company should assure itself that its external auditor complies with the relevant auditor independence standards of the Canadian accounting profession, as well as any other applicable auditor independence requirements, in respect of such services to be performed by the external auditor.

3.3.2 The insurance company does not obtain actuarial or internal audit services from its external auditor unless certain conditions apply

Unless it is reasonable to conclude that the results of the service will not be subject to audit procedures during an audit of the insurance company's financial statements, the insurance company should not obtain the following services from its external auditor:

- Any actuarial service; and⁷
- Any internal audit service related to the internal accounting controls, financial systems, or financial statements of the insurance company. 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.

⁶ The preference is always to have the arrangement documented in a contract; however, BCFSa recognizes that there may be situations where obtaining a contract is challenging.

⁷ For this purpose, actuarial services relate to the determination of an amount to be recorded in the financial statements of the insurance company or work normally undertaken by its appointed actuary. They do not include services that involve assisting the insurance company in understanding the methods, models, assumptions and inputs used, and advising management on the appropriate actuarial methods and assumptions that will be used. Consistent with OSFI's Guideline E-15 (Appointed Actuary: Legal Requirements, Qualifications and Peer Review), the insurance company may use an actuary working in the company's external auditor firm for the external review of the appointed actuary's work and reports.

SECTION 4 – TECHNOLOGY AND CYBER RISK IN THIRD-PARTY ARRANGEMENTS

Outcome 6: Technology and cyber operations carried out by third parties are transparent, reliable and secure.

BCFSA recognizes that technology and cyber risks in third-party arrangements present elevated vulnerabilities to the insurance company. In addition to the expectations articulated earlier in this Guideline, the insurance company should consider additional controls to manage technology and cyber risks stemming from its third-party arrangements.

4.1 Clear Roles and Responsibilities are Established for Technology and Cyber Controls

As set out earlier in this Guideline, and emphasized in Appendix 2, establishing clear roles and responsibilities between the insurance company and the third party is essential to managing risk, ensuring accountability, and limiting ambiguity between the parties. When setting responsibilities for technology and cyber controls, the insurance company should consider the risk and criticality of its arrangement. Where necessary, the insurance company should establish more granular descriptions of the roles, responsibilities, and procedures that apply to each party when managing the configuration of technology assets.

4.2 Third parties Comply with the Insurance Company’s Technology and Cyber Standards

Where necessitated by risk and/or criticality, the insurance company should establish processes to ensure that third parties with elevated levels of technology and cyber risk comply with its standards—or recognized industry standards—for mitigating risk, notably in the areas of access management, and data security and protection.⁸

Refer to the [Information Security Guideline](#) for expectations on technology and cyber risk management.

4.3 Cloud-specific Requirements are Established

The insurance company should develop cloud-specific requirements to ensure that cloud adoption occurs in a planned and strategic manner. These specific requirements should optimize interoperability while remaining consistent with the insurance company’s stated risk appetite. They should also augment existing insurance company controls and standards, notably in the areas of data protection, key management, and container management.

These requirements should be accompanied by robust cloud governance to provide proper oversight and monitoring of compliance with the insurance company’s risk management practices and alignment to the broader technology strategy.

4.4 Cloud Portability is Considered

In addition to planning appropriate exit strategies (see Section 2.3.5), the insurance company should also consider portability when entering an arrangement with a cloud service provider and as part of the design and implementation process in cloud adoption. As part of the consideration, the insurance company should assess benefits and risks of portability and mitigants in the absence of portability.

The insurance company should consider strategies (e.g., multi-cloud design) to build resilience and mitigate cloud service provider concentration risk (see Section 2.2.3).

⁸ Refer to BCFSA’s Information Security Guideline for BCFSA’s expectations on technology and cyber risk management.

APPENDIX 1: EXAMPLES OF DUE DILIGENCE CONSIDERATION

Before entering an arrangement with a third party—whether written or not—and on an ongoing basis thereafter, the insurance company should perform due diligence proportionate to the risk and criticality of the third-party arrangement.

In respect of its high-risk and critical arrangements at minimum, the insurance company should perform due diligence that consists of the following non-exhaustive factors:

- experience, technical competence, and capacity of the third party to implement and support the activities it is being engaged to provide, including, where applicable, the experience, technical competence, and capacity of subcontractors;
- financial strength of the third party to deliver successfully on the third-party arrangement;
- compliance with applicable laws, rules, regulations and regulatory guidance within Canada and other relevant jurisdictions;
- reputation risk associated with the third-party relationship or its services, including existence of any recent or pending litigation, investigation or complaints against the third party;
- strength of the third party's risk management programs, processes, and internal controls as well as the reporting environment (the insurance company should determine if there is alignment with the insurance company's risk management processes and controls);
- the third party's capacity to:
 - manage technology and cyber risks in accordance with the expectations outlined in BCFSa's Information Security Guideline; and
 - provide the insurance company with sufficient and timely information to comply with its reporting expectations under BCFSa's Information Security Guideline;
- strength of the third party's information security programs including their alignment with the insurance company's programs;
- the third party's capacity to provide critical services through disruption by examining its business continuity and disaster recovery plans, including the quality of such plans and the frequency and results of testing;
- the third party's reliance on, and capacity to, manage subcontractors;
- impact of the third-party arrangement, including its subcontractors, on concentration risk;
- geographic location of the third party's operations and that of its subcontractors;
- ability and ease of substituting the third party with another third party and impact of such substitution on the insurance company's operations;
- portability of applications/services provided by a third party to another third party or the insurance company;
- third party's insurance coverage;
- third party's values and business objectives, code of conduct and related policies, culture, and their alignment with those of the insurance company; and
- political or legal risks related to the jurisdiction of the third party, or the jurisdictions of subcontractors.

APPENDIX 2: PROVISIONS FOR THIRD-PARTY AGREEMENTS

This annex provides a non-exhaustive list of provisions that insurance companies 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 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: The agreement should clearly establish the roles and responsibilities of the insurance company and the third-party and subcontractors, including for managing technology and cyber risks and controls.

Use of subcontractors: The agreement should establish parameters on the use of subcontractors and require the third-party to notify the insurance company of any subcontracting of services. The insurance company should have the ability to conduct due diligence, in order to evaluate the impacts from the change in service.

Pricing: The agreement should set out the basis for calculating fees relating to the services being provided.

Performance measures: 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: 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 insurance company's assets (e.g., data, hardware and software, system documentation or intellectual property), including authorized users, and the insurance company's right of access to those assets.

Security of records and data: The agreements should govern the confidentiality, integrity, security, and availability of records and data.

Notifications to the insurance company: The agreement should require the third party to notify the insurance company of:

- incidents/events (at the third party or a subcontractor) that impact or could impact services provided, the insurance company's customers/data or the insurance company's reputation;
- technology and cyber security incidents (at the third party or a subcontractor) to enable the insurance company to comply with its reporting expectations under BCFSa's Information Security Guideline;
- changes in ownership of the third party;
- significant organizational/operational changes;
- material non-compliance with regulatory requirements (i.e. regulatory enforcement) or litigation.

Dispute resolution: 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: The agreement should enable the insurance company 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 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 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 insurance company's assets should be returned in a timely fashion. Any data and records should be returned to the insurance company in a format that allows the insurance company to sustain business operations without unreasonable expense.

The agreement should not contain any terms that inhibit BCFSa, 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 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 insurance company in the event of significant changes in insurance coverage.

Prudent risk management: The agreement should include any additional provisions necessary for the insurance company to prudently manage its risks in compliance with this Guideline.