REGULATORY GUIDELINE AND PRUDENTIAL STANDARD

Third-Party Risk Management

SYSTEM COMMUNICATION NUMBER 2025-01

APPLICABLE TO Credit Unions and SaskCentral

ISSUE DATE
JULY 2025

TABLE OF CONTENTS

I. INTRODUCTION

For SaskCentral, pursuant to Part XIII of *The Credit Union Central of Saskatchewan Act*, *2016* (the Act), Credit Union Deposit Guarantee Corporation (the Corporation) may make Prudential Standards that apply to SaskCentral. The Prudential Standard (Standard) contained herein must be adhered to by SaskCentral.

For Saskatchewan Credit Unions, this is a Regulatory Guidance Document (Guideline) as contemplated by the Standards of Sound Business Practice. It supplements and expands upon section 1, Corporate Governance and section 2.4, Risk Management and must be adhered to by Saskatchewan Credit Unions.

Saskatchewan Credit Unions and SaskCentral, collectively referred to as Provincially Regulated Financial Institutions (PRFIs) often engage in business and strategic arrangements with external parties—entities or individuals (also known as third parties) to perform business activities, functions, and services or obtain goods in support of their operations or their business strategy. Such arrangements can benefit the PRFI by introducing efficiencies, driving innovation, managing shifting operational needs, and improving services. Additionally, they help ensure compliance with acts and regulatory requirements, such as those related to audits.

Risks stemming from these third-party arrangements can pose threats to PRFI's operational and financial resilience, underscoring the critical need for effective risk management strategies. To mitigate these risks, PRFIs have the flexibility to configure their operations in the way most suited to achieving their business and strategic objectives.

II. PURPOSE AND SCOPE

The purpose of this Guideline and Standard is to communicate the Corporation's expectations for managing risks associated with third-party arrangements. These expectations aim to support various aspects of third-party risk management, ensuring that PRFIs can systematically identify, assess, and mitigate risks associated with third-party arrangements.

The Corporation expects PRFIs to manage risk related to all third-party arrangements and emphasizes that the PRFI retains accountability for business activities, functions, and services outsourced to a third-party.

This Guideline and Standard should be read, and implemented, from a risk-based perspective that allows PRFIs to compete effectively and take full advantage of efficiency, expertise, and capabilities of its third-party arrangements.

The Corporation expects PRFIs to be proactive and aware of best practices related to third-party risk management that are applicable to their institution.

III. APPLICATION

STRUCTURE

This Guideline and Standard outlines six key outcomes and eleven principles. Under each principle, there are specific topics that are used to further illustrate and clarify expectations. These topics support PRFIs in meeting the expectations of the principle.

- **Section IV. Governance** – Outlines expectations for formal accountability, leadership, organizational structure, and a framework to support risk management and oversight of third-party arrangements.
- **Section V. Management of Third-Party Risk** – Outlines risk management activities such as approach, identification, assessment, mitigation, monitoring, and reporting.
- **Section VI. to Section VIII** – Leverages previously outlined principles and clarifies expectations on special arrangements, external auditor arrangements, and technology and cyber risk in third-party arrangements.

In applying this Guideline and Standard, PRFIs should understand the risk and criticality of all its third-party arrangements in a manner that is proportionate to both:
- The risk and criticality of each third-party arrangement.
- The nature, scope, complexity of operations, and risk profile of the PRFI.

The Corporation expects PRFI to manage third-party risks with a level of intensity that reflects both the criticality of the arrangement and the associated risks. It is essential for PRFIs to prioritize the most critical risks and ensure that the necessary resources and attention are appropriately devoted to addressing them.

It is recognized that in some instances, terms of a third-party arrangement may be limited. In such cases, the Corporation nonetheless expects the PRFI to manage risk, as appropriate, through monitoring, business continuity measures, contingency planning, and other resiliency mechanisms.

OUTCOMES

There are six desired outcomes for all PRFIs to achieve through the application of this Guideline and Standard. When applied collectively, these outcomes enhance operational and financial resilience:
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 PRFI's risk appetite framework.
4. Third-party performance is monitored and assessed, and risks and incidents are proactively addressed.
5. The PRFI's third-party risk management program allows the PRFI 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.

RELATED GUIDANCE AND INFORMATION

Third-party risk management spans across business and strategic objectives, intersecting critical aspects of governance, risk management, business continuity, and technology and cyber risk management. PRFIs should review this Guideline and Standard in conjunction with other Guidelines, Standards, and communications issued by the Corporation.

DEFINITIONS

Concentration Risk is the risk of loss or harm to the PRFI resulting from overreliance on a single third-party, subcontractor or geography for multiple activities (also known as **Institution-Specific Concentration Risk**) or a risk arising from concentration in the provision of services by one third-party or geography to multiple PRFIs (also known as **Systemic Concentration Risk**).

Contingency Plan is a series of actions the PRFI may take to maintain critical operations in the event of an unplanned disruption at a critical third-party.

Criticality denotes importance to the PRFI's operations, strategy, financial condition, or reputation. It emphasizes the impact of a risk event, irrespective of the likelihood of such a risk event occurring.

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

Exit Plan is a series of actions the PRFI may 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.

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 the entity(ies) or individuals, by contract or otherwise.

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

Third-Party Risk is the risk to the PRFI due to a third-party failing to provide goods, business activities, functions and services, protect data or systems, or otherwise expose the PRFI to negative outcomes.

IV. GOVERNANCE

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

ACCOUNTABILITY

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

4.1 The PRFI retains accountability for services outsourced to a third-party and manages risk arising from all third-party arrangements

The PRFI has the flexibility to arrange its operations in a way that achieves its business and strategic objectives. However, the PRFI retains accountability for business activities, functions, and services outsourced to third parties. These include the following, and, are not limited to:

- Any risks from data exchanged with third parties.
- Any data to which third parties have access.
- Managing risk arising from third-party arrangements including subcontracting.

The PRFI's Senior Management should carry out its due diligence and 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.

Senior Management should ensure that third-party arrangements comply with PRFI's own internal policies, standards, and processes.

4.2 The PRFI's Board and Senior Management should also be satisfied that third-party arrangements are aligned with the PRFI's risk appetite and is managed proportionate to the level of criticality and risk

As set out in the Corporation's Corporate Governance Guideline and Standard, the Board or a committee of the Board is expected to ensure that the PRFI has appropriate risk management policies and practices, and that they are regularly reviewed. In terms of the specific risks arising from third-party arrangements, it is expected that the Board would periodically:

- Ensure Senior Management is monitoring and managing third-party risks according to the risk appetite established in its Third-Party Risk management Framework.
- Approve or reaffirm the policies that apply to third-party arrangements (e.g., risk philosophy, materiality criteria, risk management program, and approval limits).
- Review a list of all of the PRFI's material third-party arrangements (see section V - monitoring and reporting) and other relevant reports, when appropriate.

THIRD-PARTY RISK MANAGEMENT FRAMEWORK (TPRMF)

Principle: The PRFI should establish a TPRMF 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.

4.3 The TPRMF is enterprise-wide and governs the lifecycle of third-party arrangements

The PRFI should establish a TPRMF that provides an enterprise-wide view of its exposures to third parties. The TPRMF should reflect the PRFI's risk appetite and be consistent with its risk management framework.

The TPRMF 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 TPRMF should set out how the PRFI will identify and assess; manage and mitigate; and monitor and report on third-party risk.

A PRFIs approach in implementing the TPRMF should address the importance and adequacy of internal expertise and management frameworks to oversee and manage the outsourced activity and the relationship with the service provider.

The Corporation expects the PRFI to review and update its TPRMF on a regular basis to ensure it is relevant and appropriate and to make continuous improvements based on implementation, effectiveness, and past incidents.

4.4 The TPRMF establishes accountabilities, policies and processes for identifying, monitoring, and managing third-party risk, including, following expectations as appropriate

PRFIs will design a TPRMF to address accountability for third-party risk management, including for oversight functions. This should include clear roles and responsibilities for overseeing and managing third-party arrangements and associated risk management processes.

It should provide guidance on third-party risk appetite and measurement (e.g., limits, thresholds, and key risk indicators) and methodology for assessing the level of risk and criticality of third-party arrangements.

To ensure comprehensive oversight, PRFIs are expected to have policies that govern third-party risk management, which should be approved, regularly reviewed, and consistently implemented across the enterprise, aligning with its TPRMF.

TPRMF should also address 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).
- Aggregation of third-party risk exposures and trends to inform the PRFI's current and emerging risk profile.

V. MANAGEMENT OF THIRD-PARTY RISK

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

The Corporation expects the PRFI to manage third-party risks in a manner that is proportionate to the level of risk and complexity of the PRFI's third-party ecosystem. PRFIs are to assess third-party arrangements regularly, with higher-risk and more critical arrangements subjected to more frequent and thorough assessment and more robust risk management.

For critical third-party arrangements and those that pose a high risk to the PRFI, the Corporation expects that all expectations set out in section V be considered as minimum expectations.

RISK-BASED APPROACH

5.1 Risk assessment criteria are comprehensive and scalable

The PRFI'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 PRFI should consider the following:

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

5.2 Level of risks of third-party arrangements are assessed

In determining the level of risk, the PRFI should consider:

- The probability of the third-party or subcontractor failing to meet expectations, due to insolvency or operational disruption.
- The ability of the PRFI 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 PRFI 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 PRFI'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.
- Any other relevant financial and non-financial risks associated with the use of the third-party.

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

The robustness and frequency of the PRFI'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.

RISK IDENTIFICATION AND MATERIALITY ASSESSMENT

Principle: The PRFI 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 PRFI should conduct materiality assessments to decide on third-party selection, (re)assess the risk and criticality of the arrangement, and plan for adequate risk mitigation and oversight.

The Corporation recognizes that the third-party arrangements undertaken by PFRIs will have differing degrees of materiality and may not be readily classified as either material or immaterial.

In general, the Corporation expects that PRFIs will design a TPRMF that applies to all its third-party arrangements, and that the risk mitigants employed under this framework will remain within the established risk appetite.

5.4 Risk assessment

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

The PRFI 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 (e.g., 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 PRFI may take this into consideration as part of its risk assessment.

The PRFI should conduct risk assessments:

- Prior to entering into the third-party arrangement (see sections 4.3 and 5.5).
- Regularly throughout the lifecycle of the arrangement, including renewal, at a frequency and scope proportionate to the level of criticality.
- Whenever there is a 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 PRFI's risk appetite for third-party risk and other relevant risks.
- Document the criticality of the arrangement.
- Establish the level of risk.

5.5 Due diligence

Principle: The PRFI 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.

The Corporation expects PRFIs to conduct internal due diligence to determine the nature and scope of the third-party, its relationship to the rest of the organization's activities, and how the activity is managed.

5.5.1 A due diligence process is established

The PRFI 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.

5.5.2 Due diligence is performed proportionately to the level of risk and criticality

The PRFI 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.
- 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 for high-risk and critical arrangements is set out in Appendix A.

5.5.3 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 PRFI should review the legal requirements of relevant jurisdictions, as well as the political, legal, data privacy, security, economic, environmental, social, and other risks that may impede the ability of the third-party to provide services.

5.6 Concentration Risk

To determine the appropriate level of mitigation, the PRFI 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 PRFI's business functions/units and legal entities, and across the PRFI's entire organization. To the greatest extent possible, PRFIs should also assess systemic concentration risk.

5.7 Subcontracting Risk

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

5.7.1 Risks introduced by subcontracting practices are identified and understood

The PRFI should assess risks arising from third-party subcontractors that could impact the PRFI. Prior to entering a third-party arrangement the PRFI 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 PRFI.
- Impact of subcontracting arrangements on the PRFI's own concentration risk (refer to section 5.6 above).

5.7.2 Monitor and manage subcontracting risks

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

- Prohibiting the use of subcontractors for certain functions.
- Requiring that the PRFI 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 PPFI to refuse a subcontractor.
- Allowing the PRFI to commission or conduct an audit of subcontractors.

RISK MANAGEMENT AND MITIGATION

Outcome: Risks posed by third parties are managed and mitigated within the PRFI's risk appetite framework.

Managing and mitigating risks posed by third parties is a critical component of the overall Risk Appetite Framework. This framework establishes the boundaries within which the organization is willing to accept risk and ensures that third-party risks are managed.

PRFIs should develop a plan, with appropriate intensity of monitoring and mitigating actions, to manage the arrangement within the PRFI's risk appetite.

5.8 Written agreements/contracting

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

5.8.1 Clear responsibilities are set out in the agreement

The Corporation 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 PRFI's legal counsel.

The Corporation 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 VI of this Guideline and Standard for the Corporation's expectations related to such third-party arrangements.

5.8.2 The third-party is expected to comply with PRFI's provisions

To manage the risks associated with each third-party arrangement, the PRFI should structure its written agreement with the third-party in a manner that allows it to meet the expectations set out in this Guideline and Standard. The Corporation expects the PRFI to include in written agreements for high-risk and critical arrangements provisions that are set out in Appendix 2 of this Guideline[1].

5.9 Data security and controls (including data location)

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

5.9.1 Responsibilities for the 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 PRFI and the Corporation, upon request.
- Controls and monitoring over the third party's use of the PRFI'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.
- Notification requirements if there is a breach of security.

As appropriate, these agreements should also specify that the PRFI's data and records be isolated from 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 PRFI.

5.9.2 Record-keeping requirements are established

PRFIs are required to assess and adhere to all relevant regulations and acts to ensure compliance with record-keeping and confidentiality standards. In accordance with provincial legislation, certain records[2] of entities carrying on business in Canada should be maintained in Canada.

5.10 Information rights and audit

Principle: The PRFI's third-party arrangements should allow the PRFI timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks. The PRFI should also have the right to conduct or commission an independent audit of a third-party.

[1] Except for those contracts where section VI applies.
[2] Section 28 (1) & (2) of *the Credit Union Act, 1998*.

5.10.1 The third-party provides the PRFI with information and reporting

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

5.10.2 The third-party reports events that could materially impact the PRFI

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

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

The agreement should give the PRFI the right to evaluate the risk management practices related to the service provided. Specifically, the PRFI should be able to evaluate the risks arising from the arrangement or appoint independent auditors to evaluate the risk management practices related to the services provided. The PRFI should also be able to access audit reports in respect of the service(s) being performed.

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

5.11 Business continuity planning and testing

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

5.11.1 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 PRFI.
- Notify the PRFI of test results.
- Address any material deficiencies.

Among other things, the PRFI'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.
- Ensure the PRFI has in its possession, or can readily access, all necessary records to allow the PRFI to sustain business operations, meet statutory obligations, and provide all information as may be required by the Corporation, in the event of disruption to third-party services.

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

5.12 Contingency and exit strategy/planning

The third-party agreement is to 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 disaster, and other reasonably foreseeable events.

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

The PRFI should establish contingency and exit plans proportionate to the level of risk and criticality of individual third-party arrangements to ensure the continuity of the PRFI's operations through normal and stressed times. PRFIs 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 exits, 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) to allow rapid execution.
- 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.

MONITORING AND REPORTING

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

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

5.13 Oversight of third-party provider

PRFIs should develop, implement and oversee procedures to monitor and control risks arising from third-party arrangements in accordance with its TPRMF and risk-management policies.

5.13.1 The PRFI monitors its third-party arrangement

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

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

5.13.2 Metrics are established to confirm residual risk remains within risk appetite

The PRFI should establish processes to confirm regularly that the residual risk of their third-party arrangements, individually and in the aggregate, remains within the PRFI's risk appetite. To facilitate this outcome, the PRFI 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 PRFI's escalation process. This information should be reflected in the documentation delivered to the PRFI's Board.

5.14 Incident management and reporting

Principle: Both the PRFI and its third parties should have documented processes in place to effectively identify, investigate, escalate, track, and remediate incidents to maintain risk levels within the PRFI's risk appetite.

5.14.1 The third-party has clearly defined incident management processes

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

5.14.2 Incident reporting and notification requirements of the third-party support PRFI's compliance with the Corporation's incident reporting requirements

The PRFI should ensure that its written agreements with third parties contain adequate provisions to enable the PRFI to comply with its reporting requirements under the Corporation's Technology and Cyber Security Incident Reporting Guideline and Standard. Such provisions could include, among other things, requirements to promptly notify the PRFI of technology and cybersecurity incidents (at the third-party or the subcontractor) including providing information on each incident aligned with the incident reporting requirements.

5.14.3 Internal incident management process is established

The PRFI 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 PRFI and triggers for escalation within the PRFI.

5.14.4 Incidents are investigated, analysed and results are shared

To ensure that remediation actions are sufficient, the PRFI 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 PRFI. The PRFI should also perform its own root cause analysis, as appropriate. Remediation actions should be monitored by the PRFI.

VI. SPECIAL ARRANGEMENTS

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

STANDARDIZED CONTRACTS

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

PRFIs should ensure that the risks of third parties with standardized contracts are managed. Where standardized contracts must be used, the Corporation expects the PRFI's third-party risk management program to address the relationship. The PRFI'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 PRFI may consider are the development of redundancies, workarounds, business continuity measures, and other resiliency mechanisms.

NO WRITTEN CONTRACT

PRFIs should assume that third parties with no written contracts still carry risks. To this end, the absence of a written arrangement, formal contract or agreement does not imply the absence of a third-party arrangement and third-party risk. While the PRFI may not have direct relationships with all third parties they interact with, the Corporation expects the PRFI's third-party risk management program to address these relationships.

VII. THIRD-PARTY ARRANGEMENTS WITH THE EXTERNAL AUDITOR

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

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

Prior to obtaining management consulting services from its external auditor, the PRFI should assure itself that its external auditor would be in compliance 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.

7.2 The PRFI does not obtain 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 PRFI's financial statements, the PRFI should not obtain any internal audit services from its external auditor. This includes any internal accounting controls, financial systems, or financial statements of the PRFI.

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.

VIII. TECHNOLOGY AND CYBER RISK IN THIRD-PARTY ARRANGEMENTS

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

The Corporation recognizes that technology and cyber risks in third-party arrangements present elevated vulnerabilities to the PRFI. In addition to the expectations articulated earlier in this guideline and prudential standard, the PRFI should consider additional controls to manage technology and cyber risks stemming from its third-party arrangements.

8.1 Clear roles and responsibilities are established for technology and cyber controls

As set out earlier in this guideline, and emphasized in Appendix B, establishing clear roles and responsibilities between the PRFI 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 PRFI should consider the risk and criticality of its arrangement. Where necessary, the PRFI should establish more granular descriptions of the roles, responsibilities, and procedures that apply to each party when managing the configuration of technology assets.

8.2 Third parties comply with the PRFI's technology and cyber standards

Where necessitated by risk and/or criticality, the PRFI should establish processes to ensure that third parties with elevated levels of technology and cyber risk comply with recognized industry standards.

At minimum, the adopted industry standards should address the outcomes and principles outlined in the Corporation's Technology and Cyber Risk Management Guideline and Standard.

In the event PRFI's require more stringent standards, it should ensure that these expected standards are met for mitigating risk, notably in the areas of access management and data security and protection.

8.3 Cloud-specific (e.g., technology and cyber operations) requirements are established

PRFIs should establish cloud-specific requirements that ensure effective and secure cloud adoption. This may involve but is not limited to cloud-specific requirements such as implementing robust security controls, managing data privacy and compliance, and defining clear service level agreements and expected management practices. These requirements should address risk management, data management, integration, data governance, performance, and cost management to align cloud services with organizational needs and industry standards.

The PRFI should develop such requirements to ensure that cloud adoption occurs in a planned and strategic manner. These specific requirements should optimize interoperability while remaining consistent with the PRFI's stated risk appetite. They should also augment existing PRFI controls and standards, notably in the areas of data protection, cryptographic or encryption key management, and container management or software environments.

These requirements should be accompanied by robust technology and cyber risk governance to provide proper oversight and monitoring of compliance with the PRFI's risk management practices and alignment to the broader technology strategy.

8.4 Cloud (e.g., technology and cyber operations) portability is considered

In addition to planning appropriate exit strategies (see section 5.12), the PRFI 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, PRFI should assess the benefits and risks of portability and mitigants in the absence of portability.

The PRFI should consider strategies (e.g., multi-cloud design) to build resilience and mitigate cloud service provider concentration risk (see section 5.6).

APPENDIX A - EXAMPLES OF DUE DILIGENCE CONSIDERATION

This appendix provides a non-exhaustive list of due diligence that PRFIs should consider before entering an arrangement with a third-party whether written or not—and on an ongoing basis thereafter. This due diligence should be proportionate to the risk and criticality of the third-party arrangement. In respect of its high-risk and critical arrangements at minimum, the PRFI should perform due diligence that consists of the following non-exhaustive factors:

a. 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.
b. Financial strength of the third-party to deliver successfully on the third-party arrangement.
c. Compliance with applicable laws, rules, regulations and regulatory guidance within Canada and other relevant jurisdictions.
d. Reputation risk associated with the third-party relationship or its services, including the existence of any recent or pending litigation, investigation or complaints against the third-party.
e. Strength of the third party's risk management programs, processes, and internal controls as well as the reporting environment (the PRFI should determine if there is alignment with the PRFI's risk management processes and controls).
f. The third party's capacity to:
    - Manage technology and cyber risks in accordance with the expectations outlined in the Corporation's Technology and Cyber Risk Management Guideline and Standard.
    - Provide the PRFI with sufficient and timely information to comply with the Corporation's Technology and Cyber Security Incident Reporting requirements.
g. Strength of the third party's information security programs including their alignment with the PRFI's programs.
h. 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.
i. The third party's reliance on, and capacity to, manage subcontractors.
j. Impact of the third-party arrangement, including its subcontractors, on concentration risk.
k. Geographic location of the third party's operations and that of its subcontractors.
l. Ability and ease of substituting the third-party with another third-party and impact of such substitution on the PRFI's operations.
m. Portability of applications/services provided by a third-party to another third-party or the PRFI.
n. Third party's insurance coverage.
o. Third party's values and business objectives, code of conduct and related policies, culture, and their alignment with those of the PRFI.
p. Political or legal risks related to the jurisdiction of the third-party, or the jurisdictions of subcontractors.

APPENDIX B – PROVISIONS FOR THIRD-PARTY AGREEMENTS

This appendix provides a non-exhaustive list of provisions that PRFIs 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.

a. 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.
b. Roles and responsibilities: The agreement should clearly establish the roles and responsibilities of the PRFI and the third-party and subcontractors, including for managing technology and cyber risks and controls.
c. Use of subcontractors: The agreement should establish parameters on the use of subcontractors and require the third-party to notify the PRFI of any subcontracting of services. The PRFI should have the ability to conduct due diligence, in order to evaluate the impacts of the service change.
d. Pricing: The agreement should set out the basis for calculating fees relating to the services being provided.
e. 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.
f. 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 PRFI's assets (e.g., data, hardware and software, system documentation, or intellectual property), including authorized users, and the PRFI's right of access to those assets.
g. Security of records and data: The agreements should govern the confidentiality, integrity, security, and availability of records and data.
h. Notifications to the PRFI: The agreement should require the third-party to notify the PRFI of:
    - incidents/events (at the third-party or a subcontractor) that impact or could impact services provided, the PRFI's customers/data or the PRFI's reputation
    - technology and cyber security incidents (at the third-party or a subcontractor) to enable the PRFI to comply with its reporting requirements under the Corporation's Technology and Cyber Security Incident reporting requirements
    - changes in ownership of the third-party
    - significant organizational/operational changes
    - material non-compliance with regulatory requirements (i.e., regulatory enforcement) or litigation
i. 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. The agreement should not contain any terms that inhibit CUDGC from carrying out their mandate in times of stress or resolution."
j. Regulatory compliance: The agreement should enable the PRFI to comply with all applicable legislative and regulatory requirements, including, but not limited to, the location of records and privacy of client information.
k. 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.

l. 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 PRFI's assets should be returned in a timely fashion. Any data and records should be returned to the PRFI in a format that allows the PRFI to sustain business operations without unreasonable expense. The agreement should not contain any terms that inhibit CUDGC from carrying out their mandate in times of stress or resolution.

m. 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 PRFI in the event of significant changes in insurance coverage.

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