Deposit Guarantee Corporation of Manitoba
La Société d’assurance-dépôts du Manitoba

Guideline

Subject: Third-Party Risk Management

Effective Date: September 1, 2024

Revision History

Section	Date	Description of Revisions
	April 2024	New Third Party Risk Management Guidelines published. Previous versions of these Guidelines were housed in DGCM's IT & Outsourcing Guidelines.
2.2	April 2024	New section "Risk Based Approach". Integration with ERM Guidelines.
Schedule 1	April 2024	Revised Schedule designed to describe Material Outsourcing Contracts. In updating this Schedule, DGCM has included payment and clearance service entities as falling within the scope of these Guidelines.

Table of Contents

1.0 Overview

On July 1, 2022, DGCM issued new Standards of Sound Business Practice (SSBP) pursuant to s. 159.1 of *The Credit Unions and Caisses Populaires Act*. All credit unions and caisse (cu/caisse) must comply with SSBP that apply to them (s. 159.1). The SSBP are available at this link:

https://web2.gov.mb.ca/laws/regs/annual/2022/089.pdf

The SSBP contain rules respecting cu/caisse capital, liquidity, investments, lending, and other matters. The SSBP also contain a set of principles that assist cu/caisse to direct and manage their institution in a prudent, effective, and appropriate manner. These are further defined in DGCM's **SSBP Guidance Framework**.

The Third-Party Risk Management Guidelines better define DGCM's expectations on how a cu/caisse can comply with the SSBP with respect to managing its outsourcing risk.

2.0 Third Party Risk

Outsourcing occurs when a process or function that could be performed by a cu/caisse is delegated to a service provider. Outsourcing increases a cu/caisse's dependence on third parties which may increase risk.

Outsourcing to a third party can often be beneficial and bring efficiencies or improved services. However, new risks can arise from these arrangements. This "third party risk can be defined as:

> **"Third Party Risk"** is the risk to a cu/caisse of a third party failing to provide services or perform functions or failing to protect data or systems thereby exposing the cu/caisse to risks. Third-party risk can include:
>
> - Insolvency of the third party
> - Operational or external events that lead to disruption of third-party services
> - Information security issues as described in DGCM's Information Technology and Information Security Guidelines

2.1 Third-Party Risk Management Policies

The SSBP Guidance Framework states that a cu/caisse's board must review and approve appropriate and prudent third-party risk management policies. Third-party risk

management policies may address the following:

- Criteria for choosing outsourcing partners (due diligence)
- Privacy, confidentiality, and security of information
- Access to premises and technology resources
- Accuracy and timeliness of work performed
- Performance monitoring and scheduled reviews for material contracts
- Dispute settlements

In addition, third-party risk management policies should include criteria for determining whether an outsourced function is sufficiently material to be subject to additional controls such as the requirement for a formal written contract and right to audit.

Appropriate third-party risk management policies will direct management to identify, measure, mitigate, and control third-party risk. Policies should focus on maintaining the continuity of any outsourced business activities.

2.2 Risk-Based Approach

As with all other risks, third-party risk should be identified, assessed, and managed on a risk-basis. The cu/caisse should monitor risks associated with outsourcing through its enterprise risk management (ERM) framework. See DGCM's **ERM Guidelines** for more information.

A cu/caisse can determine the level of risk associated with specific outsourcing arrangements by considering:

- the probability of the third party or subcontractor failing to meet expectations, due to insolvency or operational disruption;
- the capacity of the cu/caisse to assess controls at the third party;
- the financial health of the third party;
- the third party's use of subcontractors and the complexity of the supply chain;
- the degree of cu/caisse reliance on third parties with elevated risk in the case that there is a concentration of risk with one service provider;
- the information management, data, cyber security and privacy practices of the third party; and

- any other relevant financial and non-financial risks (e.g. reputational risk) associated with the use of the third party.

2.3 Materiality

Management of any third-party risk will depend on the materiality of the outsourcing arrangement. These Guidelines apply to all material outsourcing arrangements including IT outsourcing.

Materiality can be determined based on a number of factors including:

- the impact on the cu/caisse's finances, reputation, and operations if the service provider fails to perform its function over a given period of time
- the ability of the cu/caisse to maintain internal controls and meet regulatory requirements if the service provider fails to perform its function
- the cost of the outsourced service and potential replacement cost of the service provider
- the difficulty and time required to find an alternative service provider or bring the business activity in-house
- the concentration risk which is the consequence of having one service provider perform multiple functions

Additional guidance for determining whether a contract is material is attached as Schedule 1 to these Guidelines.

2.4 Roles and Responsibilities

Board
A cu/caisse's board must approve and review third-party risk policies. In addition, the board should be aware of all the cu/caisse's material outsourcing contracts and major findings from relevant reports that examine those arrangements. Reliance on management reporting and advice is expected.

Senior Management
Senior management is responsible for developing policies for board approval. Senior management must also implement the policies and procedures and review their

effectiveness. This includes undertaking proper due diligence of service providers when outsourcing.

2.5 Due Diligence

A cu/caisse should assess whether a service provider has the capability, expertise, and track record to undertake the outsourced function. This review should include both qualitative (e.g. operational) and quantitative (e.g. financial) factors.

The due diligence process will vary depending on the materiality of the outsourced function. For example, the highest level of scrutiny is required where a service provider performs critical banking functions.

Factors to be considered in the due diligence process may include:

- The experience and technical competence of the service provider. This could include reputation (e.g. complaints, pending litigation), accuracy, security, privacy, and confidentiality.

- The viability of the service provider. This may include:
  - Financial strength (e.g. recent audited financial statements)
  - Internal controls and monitoring
  - Business resumption and contingency measures; the impact of non-performance should be considered.

- Business philosophy and culture of the service provider and how this aligns with the cu/caisse's culture and philosophy (e.g. do they share a similar commitment to risk management?). This issues includes reputation risk.

- Comparative analysis – IT Risk: is there evidence that the third-party is subject to similar IT risk-management rules as the cu/caisse.

The Office of the Superintendent of Financial Institution (OSFI) has published an Annex to its Third-Party Risk Management Guidelines that contains further examples of due diligence. Consult the OSFI list if your cu/caisse is reviewing due diligence processes.

2.6 Contractual Arrangements

One of the key methods for managing all types of third-party risks is to have a clear written contract between a cu/caisse and the service provider. All material outsourced activities, at a minimum, must be subject to a formal written contract.

Contracts with service providers may include the following:

- Nature and scope of service
- Subcontracting issues
- Performance measures and reporting requirements
- Dispute resolution process including default and termination
- Ownership of and access to assets
- Audit and access rights
- Confidentiality, privacy, and security
- Pricing and insurance

2.7 Subcontracting

Prior to entering into a new outsourcing arrangement, the cu/caisse should identify the third-party's subcontracting rights and practices. Understanding the number of subcontractors and criticality of their work or functions performed may lead the cu/caisse to follow the same risk management practices as they would for their primary service provider.

A cu/caisse should ensure they receive appropriate information on their third-party's use of subcontractors so that the cu/caisse can evaluate the risk. Mitigating subcontractor risk can often be achieved through provisions of outsourcing contracts including:

- prohibiting the use of subcontractors for certain functions;
- clarifying rights of audit or access to information and clarifying ownership of assets; and
- requiring that the cu/caisse be informed when a subcontractor is retained.

2.8 Monitoring & Reporting

Prior to entering into a new outsourcing arrangement, the cu/caisse should identify the third-party's subcontracting rights and practices. Understanding the number of subcontractors and criticality of their work or functions performed may lead the cu/caisse.

Schedule 1 – Examples of Material Outsourcing Contracts

Examples of material outsourcing may include:

- Information system management and maintenance (e.g. data entry and processing, data centres, facilities management, end-user support, local area networks, help desks);
- Payment and clearance service arrangements;
- Document processing (e.g. cheques, credit card slips, bill payments, bank statements, other corporate payments);
- Application processing (e.g. insurance policies, loan originations, credit cards);
- Loan administration (e.g. loan negotiations, loan processing, collateral management, collection);
- Investment management (e.g. portfolio management, cash management);
- Back office management (e.g. electronic funds transfer, payroll processing, custody operations, quality control, purchasing);
- Human resources (e.g. benefits administration, recruiting).

The guidance on managing outsourcing risk generally would not apply to the following:

- Courier services, printing services, regular mail, utilities, telephone;
- Procurement of specialized training;
- Advisory services such as: legal opinions, certain investment advisory services that do not result directly in investment decisions, independent appraisals, trustees in bankruptcy;
- Purchase of goods, wares, commercially available software, and other commodities;
- Repair and maintenance of fixed assets;
- Maintenance and support of licensed software;
- Temporary help and contract personnel;
- specialized recruitment.