CUPSA | ASPC

COMMUNIQUE

17-COM-001 July 18, 2017

Release of Information Technology Outsourcing Guidance

The Credit Union Prudential Supervisors Association (CUPSA) has released Information Technology (IT) Outsourcing Guidance, which outlines sound principles and practices for oversight of outsourcing arrangements at a Canadian credit union or caisse populaire. The guidance is consistent with international standards and is intended to be scalable to the relative size, scope, complexity and risk profile of an institution.

CUPSA encourages Canadian credit unions and caisses populaires to consider incorporating the principles, practices and roles and responsibilities outlined in the guidance into their IT risk management frameworks.

Each CUPSA member jurisdiction may choose to apply the guidance in its current or amended form at its own discretion. CUPSA will continue to monitor national and international research and guidance related to IT risk management.

About CUPSA

The Credit Union Prudential Supervisors Association (CUPSA) is an interprovincial association composed of credit union prudential supervisors across Canada. CUPSA works toward maintaining a sound and sustainable credit union sector through joint actions. For more information, visit CUPSA's website at www.cupsa-aspc.ca.

Information Technology Outsourcing Guidance

Introduction

Outsourcing occurs when a process or function that could be performed by a credit union or caisse populaire is delegated to a service provider. Since it increases a credit union or caisse populaire's dependence on third parties, risk may be increased. Outsourcing cannot replace a credit union or caisse populaire's ultimate responsibility over the IT function.

This guidance paper was developed to increase awareness of outsourcing concepts within the context of information technology, and to assist senior managers when considering the use of outsourced resources within their organizations. This guidance applies to material IT outsourcing arrangements.

This guidance is intended to be scalable to the relative size, scope, complexity and risk profile of an institution. In addition to this paper, CUPSA encourages credit unions and caisses populaires to refer to guidance papers that have been created by other regulatory bodies.

IT Outsourcing Principles and Practices

Credit union and caisse populaire Board and senior management are ultimately accountable for all outsourced IT functions and services. Senior management must also ensure that all IT outsourced arrangements comply with legal and regulatory requirements.

Outsourcing Policy

Credit unions and caisses populaires should establish an outsourcing policy which 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, an outsourcing policy 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.

An appropriate outsourcing policy will direct management to identify, measure, mitigate, and control outsourcing risk. In particular, it should ensure the continuity of any outsourced business activity.

Materiality

Management of any outsourcing risk will depend on the materiality of the outsourcing arrangement. Materiality can be determined based on a number of factors including:

- The impact on the credit union or caisse populaire's finances, reputation, and operations if the service provider fails to perform its function over a given period of time;
- The ability of the credit union or caisse populaire 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 this guidance.

Due Diligence

Material outsourcing arrangements should be subject to appropriate due diligence. Credit unions and caisses populaires 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. This review should be updated if outsourcing arrangements are renegotiated or renewed.

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.

Credit unions and caisses populaires should monitor outsourcing arrangements to ensure service providers fulfill their contractual conditions and provide levels of service as expected.

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 credit union/caisse populaire's culture and philosophy (e.g. do they share a similar commitment to risk management?)

Contractual Arrangements

One of the key methods for managing all types of outsourcing risks is to have a clear written contract with the service provider. All material outsourced activities, at a minimum, must be subject to a formal written contract. [1]

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.

[1] Additional information is available in the "Key Attributes of Effective Resolution Regimes for Financial Institutions" document from the Financial Stability Board dated October 15, 2014.

When an IT function is outsourced, particularly a banking function, a credit union or caisse populaire should focus on the following contractual issues to ensure security and continuity of the service:

Confidentiality, Privacy, and Security

The contract should address which party is responsible for ensuring the security and privacy of credit union or caisse populaire data and member data. This includes:

- Scope and definition of the information to be protected;
- The parties' respective security obligations including procedures;
- Liability for losses resulting from a security breach;
- Notification processes in the event of a breach.

In order to ensure privacy and security of data, the contract may detail measures to segregate credit union or caisse populaire data and functions from other data and functions of the service provider.

Business Contingency Planning

The contract should include details about the service provider's measures and resources for ensuring the continuity of the outsourced function. The credit union or caisse populaire may require the service provider to perform regularly scheduled disaster recovery tests. For a credit union or caisse populaire that outsources its banking system functions, special attention to contingency planning is required. For more information, please refer to CUPSA guidance on Disaster Recovery Planning.

Ownership, Access, and Audit Rights

The contract should clarify who has ownership rights of relevant assets, such as source code, applications, and reports (including assets derived from credit union or caisse populaire data).

The contract should also clarify the service provider's right to use credit union or caisse populaire assets, including member data, and the credit union's or caisse populaire's right to access its own assets. The parties' right to audit each other may also be clarified. For critical functions such as banking systems, the contract must include the right of the credit union or caisse populaire to audit or obtain audit results of the service provider's internal control environment.

Subcontracting

The contract should clarify rules and limitations on whether functions can be subcontracted. If subcontracting is permitted, the contract must stipulate that all privacy, security, access and audit obligations apply to the subcontractor.

IT Outsourcing Roles and Responsibilities

A sound understanding of appropriate roles and responsibilities is essential to outsourcing business functions in an effective manner. CUPSA has identified key roles and responsibilities[2] as follows:

Board of Directors/Audit Committee

- Approve and regularly review policies that apply to outsourcing;
- Maintain awareness of material outsourcing contracts;
- Ensure management follows up on major findings from relevant reports that examine outsourcing arrangements;
- Review management reporting around outsourced arrangements including internal audit findings and effectiveness of control environment reports from third party providers.

Senior Management

- Determine the most effective method of delivering critical business functions (in-house vs outsource decision);
- Understand the inter-relationship between third party banking service providers (e.g. companies with whom the credit union or caisse populaire has a direct contractual relationship) and other key banking service providers providing integrated/related support and solutions (e.g. companies with whom the credit union or caisse populaire does not have a direct contractual relationship);
- Develop outsourcing policies for board approval, and implement policies and procedures around outsourcing and contracts;
- Provide the board with reports on significant IT outsourcing risks on a timely basis.

[2] Roles and responsibilities outlined should be applied based on the size, scope and complexity of individual credit unions or caisses populaires.

Internal Audit

- Since internal audit must be able to examine all key processes and significant business activities, all outsourced functions should be subject to appropriate reviews.

Third Party Service Providers

- Providing assurance and, where required, audit reports on products and services that they offer to credit unions and caisses populaires.

Regulators

- Providing guidance and oversight best practices for outsourcing arrangements.

CUPSA | ASPC

Schedule 1 – Examples of Material Outsourcing Contracts

* Based on Office of the Superintendent of Financial Institutions (OSFI) B-10 Guidelines.

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);
- 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:

- Clearing and settlement arrangements between members or participants of recognized clearing and settlement systems;
- 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;
- Credit background and background investigation and information services;
- Repair and maintenance of fixed assets;
- Maintenance and support of licensed software;
- Temporary help and contract personnel;
- Specialized recruitment.