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

Guideline

Subject: Information Technology (IT) & Outsourcing

Effective Date: July 1, 2022

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 Information Technology (IT) and Outsourcing Guidelines better define DGCM's expectations on how a cu/caisse can comply with the SSBP with respect to managing its IT and outsourcing risks.

The section on Outsourcing (Section 6.0) is designed to provide general guidance on managing outsourcing risk and is not restricted to IT outsourcing.

These Guidelines draw upon standards published by other Canadian regulators and guidance issued by the Credit Union Prudential Supervisors Association (CUPSA) and is not intended to be exhaustive. CUPSA is an interprovincial association of Canadian credit union deposit insurers and prudential supervisors.

Application to CUCM
DGCM is the prudential oversight body for Credit Union Central of Manitoba (CUCM). DGCM has issued Prudential Standards applicable to CUCM. These Guidelines also better define DGCM's expectations on how CUCM can comply with the Prudential Standards with respect to managing its IT and outsourcing risk.

2.0 IT Governance and IT Risk Management

There is an increasing recognition among cu/caisse stakeholders that effective governance and management of IT is critical to cu/caisse sustainability and success. As a result, boards and senior management must ensure the corporate governance framework includes IT Governance. These Guidelines provide Manitoba specific guidance on two topics: IT Governance and IT Risk Management.

IT Governance

IT Governance is a subset of a cu/caisse's corporate governance framework. The objective of IT Governance is to provide oversight and leadership of the cu/caisse's IT function and environment. Effective governance can align the IT function with the cu/caisse's business objectives and strategies.

IT Risk Management

A cu/caisse's IT Governance framework should prioritize the management and mitigation of IT risk. IT Risk Management is the collection of policies, controls, and practices that safeguard a cu/caisse's IT assets and information in order to ensure continuity of service and operations. IT risk is discussed in Standard #3 – Risk Management.

3.0 IT Governance

3.1 IT Governance Principles

DGCM supports CUPSA's Information Technology (IT) Governance Guidance (see Communiqué 15-2014). This document lists five Guiding Principles that are designed to help a cu/caisse build an appropriate IT Governance framework.

Guiding Principle 1 – Strategic Alignment
A cu/caisse should have a strategy that aligns its IT resources and investments with the cu/caisse's business objectives. As a best practice, IT should be included in the cu/caisse's strategic planning process: e.g. annual strategic planning sessions, regular board meetings and in planning documents.

Sound long-term planning will allow a cu/caisse to capitalize on business opportunities and adapt to changes in the marketplace. The goal of this Principle is to elevate IT strategy to the senior management and board level.

Guiding Principle 2 – Value Delivery
Investments in technology infrastructure and services represent one of the most significant expenditures for a cu/caisse. As with any major investment or new project, the success of the project depends on selecting investments wisely and managing them throughout their life cycle.

For all major IT investments, senior management should identify the drivers and goals of the investment, and the cost implications. Effective reporting to the board will enable it to fulfill its oversight role and align investments with strategy.

Guiding Principle 3 – Risk Management
Effective Risk Management ensures that IT assets and information are safeguarded, including through the implementation of a robust information security framework. Risk Management is discussed in detail in Section 4.0 of these Guidelines. A cu/caisse should prioritize this Principle. Under the Standards, the recommended risk management framework is Enterprise Risk Management (ERM).

Guiding Principle 4 – Resource Management
Efficient use of IT resources will contribute to an effective IT function that supports a cu/caisse's business objectives.

The board of a cu/caisse plays an important leadership and oversight role in ensuring that IT resources (which include people and IT assets) are used wisely. An important component of resource management is the issue of outsourcing, including the management of outsourced services.

Guiding Principle 5 – Performance Management
Performance Management allows the board to monitor the implementation of the cu/caisse's IT strategy and the success of IT projects.

Senior management may provide the board with performance reports on IT services. Reports may monitor customer satisfaction, monitor whether expected service levels are maintained, and identify areas for improvement.

3.2 Roles and Responsibilities

Board
Under Standard #1 – Corporate Governance, the role of the cu/caisse's board is to provide leadership and oversight. These concepts should be understood and applied in the context of IT Governance:

> **Leadership**
> It is the duty of the board of directors to establish strategic direction, and to set the foundation for and ensure ongoing effective governance of the cu/caisse.
>
> **Oversight**
> It is the duty of the board of directors to evaluate and periodically review the cu/caisse's policies, compliance with regulation, and the performance of the CEO.

A cu/caisse's board should provide strategic direction and oversight of the cu/caisse's IT function and environment using the five CUPSA Guiding Principles. DGCM recognizes that in performing its oversight function, board members will need to rely on senior management to prepare effective reports and recommendations, including regular risk assessments.

Under these Guidelines, IT Risk Management, which includes information security, must be prioritized. The board plays an important oversight role in confirming that management is monitoring and managing IT risks according to risk tolerances established in its ERM framework.

The board must ensure management has appropriate information security policies and procedures that align with the information security objectives of the cu/caisse. For example, the board may establish a targeted maturity level for information security and monitor management's progress. The board may also measure a cu/caisse's maturity against established information security industry standards.
As part of its oversight of the IT function, the board should ensure that independent audits reviews of the cu/caisse's IT Risk Management controls and governance framework are undertaken: see Section 5.0.

Senior Management
Senior management drives the IT function. Senior management should implement board strategy and provide sufficient reports for the board to meet its oversight function. Reports should include risk assessments and IT audits.

Senior management ensures the cu/caisse implements an IT Governance framework that follows the five Guiding Principles. In particular, senior management must ensure the cu/caisse meets appropriate standards for information security and, if applicable, reaches a maturity level set by the cu/caisse. Information security controls are described in Section 4.0.

3.3 IT Policy

The cu/caisse's board must approve an IT Policy that supports the IT Governance framework and ensures the policy is reviewed and updated on a regular basis.

Among other things, the IT Policy should define how the cu/caisse will manage IT risk, particularly information security. The IT Policy should identify the areas where management should put in place appropriate controls. In addition, the IT Policy should assign responsibility and accountability to specified individuals or departments responsible for IT functions: see Section 3.4 below.

The IT Policy should be supported by a series of specific information security policies and processes that are developed and approved by senior management and IT staff and reviewed and updated on a regular basis. DGCM's minimum expectation is that a cu/caisse's IT policies and processes will address the information security areas and controls listed in Section 4.3 of these Guidelines.

A cu/caisse's IT Policy and related information security policies and processes may be assessed against existing industry standards to identify any information security areas that are not currently covered. For example, ISO/IEC 27002 is a well-recognized standard that can assist a cu/caisse to identify gaps in its IT Policy and related processes.

3.4 Organization, Reporting, and Expertise

Organization and Reporting
A cu/caisse's IT Policy and governance framework should set out roles and responsibilities for IT Risk Management, allocate specific roles to departments or individuals, and ultimately establish accountabilities. While specific duties can be outsourced, accountability must rest with a specific individual(s) in the cu/caisse at a sufficiently senior level.

As a best practice, the cu/caisse may assign accountability of the IT function to a single responsible senior manager, such as a Chief Information Officer (CIO), and the IT Policy may set a functional reporting relationship between the CIO and the board. As a cu/caisse grows in size and complexity, it may wish to strike an IT subcommittee of management that would report to the board, regularly monitor compliance with the IT Policy, perform risk assessments, and implement the cu/caisse's IT strategy.

Expertise
A cu/caisse's board should collectively have an understanding of IT risks to provide leadership and oversight of the IT function. The cu/caisse's board and management should consider what level of experience and expertise the board as a whole should possess and identify any gaps.

The board should ensure that appropriate resources, including ongoing training, are provided to assist the board in fulfilling its mandate. Training plans for board members should include IT governance training if gaps are identified.

Given the complexity of this area, as a best practice, a cu/caisse should examine the benefit of having a board member who has an IT background, either through education, training, or work experience.

At the management and staff level, the cu/caisse should ensure that the individual(s) responsible for the information security function has sufficient knowledge and understanding of IT Risk Management (e.g. an experienced information security professional). IT staff should be provided with the opportunity and funding to attend information security related educational events, conferences, and courses.

4.0 IT Risk Management

4.1 IT Risk Management and ERM

IT Risk Management, the third CUPSA Guiding Principle, helps to ensure that risks facing the cu/caisse's IT assets and information are identified, analyzed, and mitigated.

A cu/caisse should prioritize IT Risk Management. Under the Standards, the recommended risk management framework is ERM. Through an ERM framework, each cu/caisse should manage IT risk and have a low risk tolerance for threats to the confidentiality, integrity, and availability of information and services. For further information on ERM, consult DGCM's ERM Guidelines (see Communiqué 07-2016).

In order to understand current and emerging risks around IT, DGCM recommends that IT risk assessments be performed on a regular basis.

4.2 IT Risk Assessment

The cu/caisse should develop a formal IT risk assessment process to assist the board and senior management with identifying, analyzing, and mitigating IT risks.

DGCM recommends that an IT risk assessment be performed, at minimum, on an annual basis, and also when a new IT initiative is proposed. An IT risk assessment is a regular internal management review that can be conducted or led by the cu/caisse's CIO, IT subcommittee, or the individual(s) responsible for the IT function. The review may be part of the cu/caisse's overall ERM process, however, the review dives into greater technical detail in assessing IT risks.

An IT risk assessment identifies and analyzes reasonably foreseeable external and internal threats that could have a material impact to key business functions and sensitive IT systems (e.g. risk of hacking, breakdown or interruption of service). The risk assessment can identify information that, if compromised or lost, could lead to legal, reputational, or financial loss (e.g. member data, strategic plans, financial data).

An IT risk assessment should not be confused with IT audits which verify the adequacy of internal controls rather than identify threat scenarios.

If a cu/caisse is not currently conducting IT risk assessments, establishing the framework and process will require dedication of resources and start-up time, e.g. similar to establishing an ERM framework. Once a baseline has been established, a regular review and reporting process should be formalized.

4.3 Information Security

Every cu/caisse should have a robust information security control framework in place. Controls are not considered robust unless they are formalized in the cu/caisse's IT Policy and written management policies and processes.

A robust control framework will ensure that the cu/caisse's IT function can meet acceptable standards for:

- **Confidentiality:** Information, particularly member data, is maintained in a secure manner. IT systems and processes must ensure information is only disclosed to those who are authorized to view or access it.
- **Integrity:** Information and data must be accurate and reliable, and managed using appropriate quality control practices.
- **Availability:** Systems, data, and information are available to users at when required.

In preparing this section of the Guidelines, DGCM reviewed a number of different industry standards and documents produced by other regulators and industry leaders. In particular, the information security controls described in this section follow an industry standard from the International Organization of Standardization: ISO/IEC 27002.

In developing and assessing the adequacy and maturity of information security controls, cu/caisse may also benefit from using a self-assessment tool developed by the Office of the Superintendent of Financial Institutions (OSFI).

The OSFI tool, "Cyber Security Self-Assessment Guidance" can be found on their website at http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

In addition to establishing a robust control framework, the board and senior management should ensure appropriate resources are allocated to implement the framework. Resources should be dedicated towards a staff/company-wide security awareness program with appropriate training so that the cu/caisse is vigilant and aware of IT risks at all levels.

The following subheadings detail specific information security controls that are part of an appropriate information security control framework.

Access Control and User Management

The cu/caisse should formally document and implement policies and processes regarding access to and control of IT systems, assets, and information.

Access controls should identify the specific individuals who are authorized to have access to networks (see Section 4.3.4), information, and other key IT assets. Once users are authorized, the cu/caisse must ensure its processes require authorized users to provide authentication and valid identity to gain access.

The cu/caisse should consider the following when implementing access controls within its IT environment:

Administrative Controls

- Creating a formal access control policy which addresses the authorization, authentication, and audit of access controls.
- Granting access controls to ensure that users can only access systems that they are specifically authorized and required to access (least privilege).
- Establishing user creation, management, escalation, and removal authorizations and processes.
- Establishing security awareness and training programs for users.
- Regularly reviewing access rights and privileges.

Physical Controls

- Using physical security controls referred to in Section 4.3.5.

Technical Controls

- Creating robust technical controls to control user and computer access to systems, networks, and information.
- Using strong passwords or other authentication methods.
- Using encryption to guard data from unauthorized access.

Asset Management and Operations Security

Operational Procedures

The cu/caisse should formally document and implement IT operating procedures to secure its information and the operation of its IT facilities. Changes should require management approval on a risk basis.

Under ISO/IEC 27002: “documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room, and mail handling management and safety”.

Change Management

Cu/caisse operating procedures should address the concept of change management. Changes to IT processes or systems should be formally controlled, often with the use of secure

development and testing environments. Only authorized persons should be able to introduce or install new software, applications, or systems.

A formal change process will ensure that improvements introduced into the cu/caisse's IT environment are done in a structured and orderly manner, to minimize any impact on business services.

Vulnerability/Patch Management

A comprehensive vulnerability and patch management process should be established to ensure that every device is appropriately configured and consistently patched to close newly discovered vulnerabilities.

The patch management process should ensure off-the-shelf software (e.g. Microsoft, Adobe, etc.) is regularly updated through service packs and patches. This process should also address in-house developed software and systems to ensure vulnerabilities and issues are fixed promptly.

Patches and fixes should be tested to determine if they are effective and do not introduce system side-effects, such as instability or errors. If software patches are unable to address a vulnerability, other compensating controls should be put in place.

Technical vulnerability and penetration testing should be regularly performed on internally and externally-facing systems to discover vulnerabilities, exploits, and stale software versions.

System Logging

System logging and monitoring processes should be established to detect security violations and improper use of or access to software and systems. Log monitoring systems should be configured to allow system administrators to find security-related events and alerts, and to properly manage logs. Without proper management, log files can grow quickly and become difficult to use.

In addition, it is important to protect system log files in order to prevent modification or deletion as these logs provide critical troubleshooting and investigative information to diagnose system errors or intrusions.

Virus and Malware Protection

Prevention and detection controls should be established to protect a cu/caisse against malicious or unauthorized software. Anti-virus and malware detection software should be used to regularly scan computers, storage media, email, and webpages on a precautionary and routine basis.

If a system is infected with viruses or malware which cannot be removed easily, the cu/caisse should enact its incident handling process discussed in Section 4.3.4.

Asset & Information Management
The cu/caisse should identify and classify all of its IT assets and data according to their sensitivity and implement procedures to protect those assets and data. Information classification policies and procedures should also be established to control the treatment of information. Classification policies can identify sensitive information that requires more stringent protection controls.

IT assets, data, and information should be controlled throughout their lifecycle. Information assets, such as databases and data files, should be effectively managed through the creation, storage, transmission, and deletion stages. Physical assets, such as hardware and other systems, should be handled through an asset management system, which tracks an asset's introduction, assignment, maintenance, and destruction phases.

Backup and Recovery
Backup policies and procedures should be established to regularly backup information and systems. These procedures should ensure that backups and information are retained, protected, or deleted in an orderly manner taking into consideration the sensitive nature of the information. Regular testing will confirm if the backup procedures meet the requirements of the cu/caisse's incident handling process and disaster recovery plans.

Backup copies of information, software, and systems images should be taken and tested regularly. Backup information, software, and systems should be stored in a remote location with adequate environmental protection, and should be readily accessible.

Network Management

A cu/caisse's network should be designed to allow only authorized users to connect. Authorization privileges should only allow authenticated users to connect to specific information and systems.
Network devices, such as routers, firewalls, and switches, should be appropriately configured and implemented to protect connected systems, data, applications, and users. Where applicable, a wider range of network security appliances or applications (e.g. intrusion detection systems, intrusion prevention systems, content filtering) may be utilized to provide a more layered approach.

The use of encryption technologies should be strongly considered for protecting data in transit. Encryption is commonly used in virtual private network (VPN) services and wireless connectivity, but can be extended to other network applications.

A cu/caisse should consider network segregation when designing the IT environment, based on trust levels, business units, or combination of both. Network segregation helps to enforce least privilege access for users and systems, and potentially reduces the exposure of the entire network during virus outbreaks or system compromise.

Network infrastructure should be protected from unauthorized changes through the use of complex device passwords, or local-only access.

Incident Management

The cu/caisse must have the ability to consistently and effectively respond to “information security incidents”, a term that describes events or threats to cu/caisse IT systems or information that may impair business operations. An incident could include an employee data breach, service interruption, customer fraud incident, virus infection, etc.

Information security incidents and responses under this section should not be confused with the type of events that would lead to a Business Continuity or Disaster Recovery scenario. However, any incident management plan should allow decision makers to escalate their response if the impact or risk so warrants.

The cu/caisse should have a documented incident-handling process in place. This may include:

- A policy/process that defines roles and responsibilities.
- Procedures for reporting incidents and identified weaknesses in systems or services in a timely manner.
- Procedures for responding to and containing identified incidents and minimizing damage.
- Procedures for escalating reporting, responses, and authority (e.g. senior management and board).
- A communication plan, including a crisis communication plan, (internal and external) for identified scenarios (e.g. customer notification of service interruption or external breach/data loss).
- A process for analyzing the incident and response after the fact (post- mortem).

The cu/caisse should ensure staff are aware of their responsibility to report events. Staff should also be encouraged to red flag any potential shortcomings in information security and may be obligated to do so.

A cu/caisse must notify DGCM of any “Reportable Incident” as set out in DGCM’s Technology and Cyber Security Reporting Requirements – (see Communiqué #07 – 2019).

A cu/caisse’s incident management processes should be tested regularly to keep staff familiar with what the cu/caisse would do in the event of an incident.

Physical Security

Physical security controls should be put in place at each cu/caisse location. Physical protection of IT assets should be given similar consideration as financial assets. Controls should protect all IT physical assets: this applies to servers, workstations, networking infrastructure, etc.

Physical security should provide protection from:

- Environmental threats (e.g. floods, fires)
- Human threats (e.g. criminals, employees, unauthorized parties)
- Supply interruption (e.g. electrical)

Security Perimeters should be defined, and protection mechanisms should be implemented that meet the security requirements of the assets within each perimeter. Perimeters can be defined as:

- Outer Perimeter (areas outside the building, including the outside walls and doors of the building)
- Inner Perimeter (areas inside the building, offices, and meeting rooms)
- Core Perimeter (usually a server or systems room with access to sensitive infrastructure)

Controls within each layer can range from swipe cards, security cameras, and alarms to HVAC systems, fire suppression systems, and cabling closets. A cu/caisse should consider a risk-based layered approach, using a range of controls within each perimeter.

System Acquisition and Development

If a cu/caisse acquires or develops a new information system, or makes changes to existing systems, information security requirements should be included in the analysis and implementation of the new system or system change.

Security requirements must be considered before introducing new systems or redeveloping/altering existing systems. If security requirements cannot be met within the newly acquired or developed/altered system, compensating controls should be put in place.

For systems designed and built in-house, including custom developed applications, development should be performed in a secure environment. Changes to custom developed applications must be controlled, tested and managed to ensure that new risks are not introduced to the cu/caisse.

For systems developed by an outsourced party, controls and monitoring processes should be put in place to ensure that these third-parties are developing applications and systems in a secure environment (see Section 6.0 on Outsourcing).

Disaster Recovery Plan (DRP)

The cu/caisse should have a Disaster Recovery Plan (DRP) that details procedures for the recovery of IT information and continuity of IT systems and services critical to the business operations in the event of a critical incident.

A DRP may include the following components:

- Identification of scenarios or incidents that may disrupt or slow down the cu/caisse's critical functions.
- An inventory and assessment of the cu/caisse's existing IT infrastructure required to support its critical functions. An assessment of this nature, which may be referred to as a Technology Impact Assessment, has two components:
    - An inventory of computing resources, databases, storage, security, network components, personnel, and vendors (lists with key contact information).
    - An analysis of the failure of one or more components of the cu/caisse's IT infrastructure and its impact on a critical function.
- Identification of available resources to respond to incidents or disruptions and the assignment of roles and responsibilities.
- Identification of alternate sites (head office, alternate branches, data centres, etc.) for continuity of operations, including relocation and restoration procedures with particular emphasis on utilization of back-ups.
- Recovery procedures: steps and resources to assess damage and execute the recovery of critical IT systems and information.

A cu/caisse's DRP should be tested regularly to keep contact information and recovery procedures up-to-date. Testing, for example, can ensure that estimates/timelines for recovery are realistic, staff are familiar with the plan and procedures, and alternate sites or infrastructure perform as required. Training should be provided to employees with responsibilities under the DRP to ensure they understand the plans and their roles.

4.4 Additional Considerations – Banking System Controls

A cu/caisse should identify the IT systems that form part of its core banking system and ensure that appropriate controls are designed and implemented to insulate the banking system from possible threats.

The controls that a cu/caisse should put in place to ensure that their core banking system is secure may not be different than the controls described above in Section 4.3. However, banking system controls will vary depending on the framework and infrastructure of each cu/caisse including whether the banking system is outsourced.

Outsourced Banking System

A cu/caisse that outsources all or most of its banking system functions should identify whether any specific banking system controls should be put in place at the cu/caisse that are over and above those described in Section 4.3.

For example, recent CSAE 3416 reports regarding Celero's eroWORKS system include Section 3 titled "User entity control considerations" which describes controls that are the responsibility of the cu/caisse.

In-house Banking System

For cu/caisse with in-house controlled banking systems, identifying and implementing specific banking system controls can be aided through use of regular risk assessments. As an example, the types of information security controls for an in-house banking system would be similar to all of the controls described in a CSAE 3416 report.

5.0 IT Audits

5.1 Audit Committee and Internal Audit

DGCM's **Audit Committee and Internal Audit Guidelines** state that a cu/caisse's internal audit function should be able to examine all key processes or significant business activities.

A cu/caisse's Audit Committee should ensure that independent IT audits are included in internal audit planning. The scope and frequency of IT audits must be determined on a risk basis unless otherwise specified in these Guidelines.

IT audits may require specialized knowledge not available in-house, therefore, an IT audit may need to be outsourced. If an IT audit is outsourced, the person responsible for the internal audit function at the cu/caisse must ensure there is appropriate oversight and follow-up.

5.2 Scope and Frequency of IT Audits

As mentioned earlier in Section 4.0, DGCM's minimum expectation is that a cu/caisse will put in place robust information security controls described in Section 4.3. A cu/caisse may choose to conduct wide-scoped audits that look at all information security controls at once or focus on specific areas at a time. Regardless of the approach, all information security controls described in Section 4.3 must be audited with reasonable frequency.

DGCM's expectation is that, at minimum, all information security controls described in 4.3 of the Guidelines must be audited at least every three years. For clarity, an IT audit based on the ISO/IEC 27002 standard would meet this minimum expectation.

Beyond audits of information security controls, a cu/caisse should consider expanding the scope of audits to examine IT governance and risk management practices. In November 2015, DGCM circulated an IT paper from CUPSA that focused on the audit function: "Information Technology (IT) Audit Guidance" (see Communiqué 2015-16). In the paper, CUPSA noted:

> "This guidance paper was developed for cu/caisse to increase awareness of IT audit concepts, and to assist senior managers when considering the use of an IT audit within their organizations."
>
> "Defining the purpose and scope of the IT audit is critical to receiving the assurance required by the board of directors and management."

Each cu/caisse, when planning IT audits, may wish to consult CUPSA's IT Audit Guidance for assistance in defining the various areas that may be audited. The audits defined in CUPSA's guidance include:

- Business/IT Strategic Alignment Review
- Systems Administration Review
- Application Review
- Network Security Assessment
- Business Continuity Review
- Data Integrity Review
- Physical Security Review
- Project Management and Change Management Review

5.3 Audits of Banking Systems

A cu/caisse's core banking system is critical to its business. There should be a low risk tolerance for any threats or disruption to the core banking system. Therefore, DGCM's minimum expectation is that each cu/caisse will obtain an annual IT audit of its core banking system.

Audits of banking systems will vary depending on whether or not a cu/caisse outsources its banking functions. In defining a "core banking system", each cu/caisse should consider what IT systems, hardware, software, applications, etc., are critical to the functioning of its core banking system.

Senior management should identify, as part of ongoing IT risk assessments, other critical IT functions that are either controlled in-house or outsourced and require the same level of scrutiny as the banking systems.

Senior management must also understand the interrelationship between third party banking service providers (e.g. companies with whom the cu/caisse has a direct contractual relationship) and other key banking service providers providing integrated or related support and solutions (e.g. companies with whom the cu/caisse does not have a direct contractual relationship).

There is wide variation among cu/caisse as to the degree of outsourcing. As well, there is variation in the ownership of source code and proprietary rights.

The majority of cu/caisse in the Systems representing the majority of Systems assets currently use the eroWORKS banking system from Celero. After eroWORKS, the Infonancial system is the second most frequently used banking system. A few large cu/caisse use other banking systems.

There is no one-size-fits-all rule for banking system audit requirements. To provide clarity with respect to the types of banking system arrangements and DGCM's minimum audit requirements, we have prepared Table 1.

Table 1: Banking Systems – Outsourcing and Audit Requirements

Level of Outsourcing	Details	Audit Requirement
Fully Outsourced	Banking system owned and controlled by a third-party service provider. Third party provides critical IT support service.	Annual verification from service provider: **CSAE 3416.**
Partly Outsourced	Mixed ownership or control of banking system. Third party may provide critical IT support service or have licenced the use of their product. However, cu/caisse may: - retain ownership of source code - maintain data in-house - have degree of control over ongoing development, changes, or customization to the banking system, or - develop, in-house applications or systems that are integrated into the core banking system.	For third party controlled banking system functions: annual verification from service provider: **CSAE 3416.** For cu/caisse controlled banking system functions: annual IT audit of relevant banking system IT controls – CSAE 3416 equivalent.
In-House Control	Banking system owned and controlled by the cu/caisse. Ongoing cu/caisse control of management, development, and IT support.	Annual IT audit of relevant banking system IT controls – CSAE 3416 equivalent.

For a cu/caisse that uses eroWORKS or another banking system owned and controlled by a third party, the cu/caisse must ensure services of the third party are audited on an annual basis according to recognized audit standards for IT service providers. The current standard is the Canadian Standard on Assurance Engagements 3416 – Reporting on Controls at a Service Organization (CSAE 3416). The CSAE standards also provide guidance regarding qualification of audit professionals.

If the cu/caisse has identified other third parties that provide critical or integrated support and solutions to the banking system service provider, it must determine whether those other services form part of the cu/caisse's core banking system and therefore require an audit.

For a cu/caisse that partly outsources or has full in-house control of its banking system, the cu/caisse must ensure that its banking system internal controls are audited on an annual basis using a robust audit framework. At minimum, the banking system IT controls that are tested in the course of this audit should be similar to the controls examined in a CSAE 3416.

As an example, recent CSAE 3416 audits reports reviewed by DGCM focus on the following areas specific to the banking system being audited:

1. Organizational Security and Administration
2. System Access
3. System Software Change
4. Data Communications
5. Facilities
6. Computer Operations
7. Personnel
8. Back-up
9. Application Software Change

6.0 Outsourcing

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 cannot replace a cu/caisse's ultimate responsibility over the IT function.

Standard 3 – Risk Management – contains general guidance on the management of outsourcing risk. One of the main points from the Standards is that a cu/caisse's board must review and approve appropriate and prudent outsourcing policies.

6.1 Outsourcing Policy

As stated in the Standards, an outsourcing policy 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.

6.2 Materiality

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

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.

6.3 Roles and Responsibilities

Board
A cu/caisse's board must approve and review policies that apply to outsourcing. 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.

The board should be provided with information about the extent to which some or all of the cu/caisse's core banking system has been outsourced and understand the key details of the contracts.

Senior Management
Senior management is responsible for developing outsourcing 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.

Senior management must have a strong understanding of the extent to which some or all of the cu/caisse's core banking system has been outsourced. Senior management should also understand the interrelationship between third party banking service providers (e.g. companies with whom the cu/caisse has a direct contractual relationship) and other key banking service providers providing integrated/related support and solutions (e.g. companies with whom the cu/caisse does not have a direct contractual relationship).

6.4 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?)

6.5 Contractual Arrangements

One of the key methods for managing all types of outsourcing 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

Contracts Involving IT Functions
When an IT function is outsourced, particularly a banking function, a cu/caisse 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 cu/caisse 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, and
- notification processes in the event of a breach

In order to ensure privacy and security of data, the contract may detail measures to segregate cu/caisse data and functions from other data and functions of the service provider.

- **Contingency Planning**
  The contract should include details about the service provider's measures and resources for ensuring the continuity of the outsourced function. The cu/caisse may require the service provider to perform regularly scheduled disaster recovery tests.

  For a cu/caisse that outsources its banking system functions, special attention to contingency planning is required.

- **Ownership, Access, and Audit Rights**
  The contract should clarify who has ownership rights of relevant assets, such as source codes, applications, and reports (including assets derived from cu/caisse data).

  The contract should also clarify the service provider's right to use cu/caisse assets, including member data, and the cu/caisse'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 cu/caisse 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.

7.0 Differential Requirements Based on Size and Complexity

Recognizing that the members of the cu/caisse Systems vary considerably, these Guidelines differentiate between “small” (<$200 million), “medium” ($200 million to $1 billion), and “large” (>$1 billion) institutions based on asset size. Differentiation based on size provides initial parameters; however, DGCM’s expectations may vary if a cu/caisse has a complex business model.

Guidance applicable to all cu/caisse

At minimum, each cu/caisse should adopt IT and outsourcing policies and establish formal information security processes. The resources dedicated to these processes will vary among cu/caisse depending on their size, complexity, and level of risk, as well as the degree to which they have outsourced key IT functions.

Information security controls must be subject to IT audits performed on a risk basis in accordance with Section 5.0 of these Guidelines including annual audits of the banking system.

Small institutions: Most small institutions outsource their banking system. They also outsource most IT services including IT support and maintenance. A robust outsourcing policy and compliance with Section 6.0 of these Guidelines is required.

For small institutions that fit this profile, one or more senior managers may be designated as having operational responsibility for IT governance and risk management. Those senior manager(s) must have the ability to review, understand, and advise the board regarding IT risks and third party reports that review IT functions.

Small institutions must obtain annual CSAE 3416 reports from their key IT service providers, particularly the banking system service provider.

Medium-sized institutions: In addition to the requirements for small institutions, DGCM expects medium-sized institutions to have a mature IT Governance structure that ensures the board is giving appropriate consideration to IT strategies, resources, and value delivery. In addition, medium-sized institutions should grow and develop their in-house IT capabilities.

Medium-sized institutions should plan for compliance with the requirements for large institutions as they grow in size and complexity. Further to Section 5.0, audit requirements will vary depending on whether the cu/caisse outsources its banking system.

Large institutions: DGCM expects large institutions to have established a mature IT Governance model and information security processes that incorporate the following:

- Additional staff and resources dedicated to IT functions including a senior level person (e.g. a CIO) with responsibility for the IT functions.
- Formal/regular resources and training provided to staff to stay current with emerging risks, new technology, and user expectations.
- Establishment of an IT subcommittee of management and staff to oversee the assessment of risk and the development of information security controls.
- Regular, at least annual, IT Risk Assessments that are performed in-house along with a Risk Assessment performed when new IT systems or processes are introduced.
- Functional reporting relationship established between the CIO or IT subcommittee and the board.
- IT Governance model integrated with the cu/caisse's ERM process.
- Regularly scheduled IT audits of areas as defined in the CUPSA IT Audit Guidance (see Section 5.2).
- A DRP that is robust and regularly tested with an established and tested backup site in place.

Further to Section 5.0, audit requirements will vary depending on whether the cu/caisse outsources its banking system.

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; and
- Specialized recruitment.