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

Information Technology (IT) and Information Security Guidelines

Subject: High level principles and specific DGCM requirements

Effective Date: September 1, 2024

Revision History

Section	Date	Description of Revisions
	September 2016	Original Guidelines Released
4.3.4	June 2019	Addition of reporting requirement to DGCM re. “Reportable Incidents” – re. Communiqué #07-2019. Addition of a recommendation to regularly test incident management processes.
5.2	June 2019	Clarify that conducting an IT audit based on the ISO/IEC 27002 standard would meet minimum expectations.
1.0	July 1, 2022	Revisions due to amendments to *The Credit Unions and Caisses Populaires Act* (Act). Changes describe the new legal framework under the Act and the primary role of DGCM’s SSBPs. This document is now described as an interpretive guide to assist credit unions/caisse in complying with the SSBPs. Note added re. application of these Guidelines to Credit Union Central of Manitoba (CUCM).
1.0	April 30, 2024	Addition of applicability statement in replacement of previous section “7.0 Differential Requirements Based on Size and Complexity”
2.0		Addition of statement to clarify the applicability of controls mentioned across the Guideline for the cu/caisse.
3.1		Revised headings for “Guiding Principles” to align with IT requirements.
3.2		Clarified the roles and responsibilities of the Board and Management in providing oversight and managing IT.
3.3		Clarified the requirements for Board level and management level IT policies.
4.2		Clarified the process of IT risk assessment and requirement for IT Risk Assessment.
4.3.1		Added additional requirements for Access Management Policy and Access Controls.
4.3.2		Addition of System Hardening requirements
4.3.4		Addition of requirements for security incident response playbooks
4.3.7		Section name changed from 4.3.7 Disaster Recovery Plan (DRP) to 4.3.7 IT Disaster Recovery Plan. Addition of requirements to incorporate the results of business impact assessments (BIA) of the cu/caisse’s Business Continuity Plan

		Addition of requirements to consider dependency on third-parties and cloud service providers (CSP) while formulating ITDR Plans
4.4		Addition of new section in replacement of previous section “6.0 Outsourcing”
5.1		Clarified the role of cu/caisse’s Internal Audit functions role in the IT audits. Clarified the requirements pertaining to test of design and operating effectiveness in IT audits. Addition of guidance on selection of external IT audit service providers.
5.2		The scope of IT audit has been changed from section 4.3 of the previous guideline to Section 4.0 of this new guideline
Appendix A		Addition of appendices (A.1 and A.2) to summarize the minimum requirements for IT Audits and Banking System Audits.
Appendix B		Addition of a glossary to describe the terminologies used in this guideline.

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

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.

The ITIS Guideline sets out both high level principles and specific DGCM requirements. The implementation of the ITIS Guideline should be applied in a risk-based and proportionate manner and will vary given differences in the nature, scope, complexity, systemic importance, and risk profile of the cu/caisse.

In most cases, cu/caisse should apply the entirety of this Guidance document to their operations. DGCM may recommend additional IT and/or Information Security controls be implemented consistent with a risk-based and proportionate supervisory approach.

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 Information Security risks.

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 a cu/caisse's sustainability and success. As a result, Boards and Senior Management must ensure the corporate governance framework includes IT Governance. This Guideline provides Manitoba-specific guidance on two topics: IT Governance and IT Risk Management.

IT Governance

i. IT governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives and strategies. IT Governance must be a subset of a cu/caisse's corporate governance. The objective of IT Governance is to provide oversight and leadership of the cu/caisse's IT function and environment.

IT Risk Management

i. A cu/caisse's IT Governance Framework should prioritize the management IT and Information Security risks. IT Risk Management consists of the procedures, policies, and tools to identify and assess potential threats and vulnerabilities in IT infrastructure. IT risk is discussed in Standard #3 – Risk Management of the SSBP Guidance Framework.

3.0 IT Governance

3.1 IT Governance Principles

The following five Guiding Principles are designed to help a cu/caisse build an appropriate IT Governance Framework.

Guiding Principle 1 – Strategic Alignment of IT

i. 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 planning documents.

ii. 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 of Technology Investments

i. Investments in technology infrastructure, information security 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.

ii. For all major IT investments, Senior Management should identify the drivers and goals of the investment, and the cost implications. Cost benefit analysis should be performed for all major IT investments. Effective and timely reporting to the Board will enable it to fulfill its oversight role and align investments with strategy.

Guiding Principle 3 – IT Risk Management

i. Effective Risk Management ensures that IT assets and information are safeguarded, including through the implementation of a robust information security framework. IT Risk Management is discussed in detail in Section 4.0 of this Guideline.

ii. A cu/caisse should prioritize this Principle. Under the SSBP Guidance Framework, Management monitors and manages IT risks according to risk tolerances established by the Board using an Enterprise Risk Management (ERM) Framework.

Guiding Principle 4 – IT Resource Management

i. Optimum use of IT resources will contribute to an effective IT function that supports a cu/caisse's business objectives. Adequate budget and resources must be allocated to IT governance and IT risk management activities.

ii. 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 optimally. An important component of resource management is the issue of outsourcing, including the management of outsourced services.

Guiding Principle 5 – Performance Management of IT Investments

i. Performance Management allows the Board to monitor the implementation of the cu/caisse's IT strategy and the success of IT projects.

ii. Senior Management must provide the Board with performance reports on IT and information security. Reports should monitor customer satisfaction, whether expected service levels are maintained, effectiveness of information security and identify areas for improvement.

3.2 Roles and Responsibilities

Board

i. Under SSBP Guidance Framework 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.

ii. A cu/caisse's Board should provide strategic direction and oversight of the cu/caisse's IT function and environment using the five 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.

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

iv. The Board must ensure that Management has appropriate information security policies and procedures that align with the information security objectives of the cu/caisse.

v. The cu/caisse must establish a target maturity level with Board input for information security and monitor Management's progress.

vi. As part of its oversight of the IT function, the Board must ensure that independent audits and reviews of the cu/caisse's IT Risk Management controls and Governance Framework are undertaken as mandated in Section 5.0 in this Guideline.

Senior Management

i. Senior Management drives the IT function. Senior Management must implement Board strategy and provide performance reports for the Board to meet its oversight function. Reports should include, but are not limited to, results of risk assessments, third-party risk management and IT audits.

ii. Senior Management ensures the cu/caisse implements an IT Governance Framework that follows the five Guiding Principles.

iii. Senior Management must ensure the cu/caisse meets appropriate standards for information security and reaches a maturity level set by the cu/caisse. Information security controls are described in Section 4.3 of this Guideline.

iv. Senior Management must ensure that IT audits are executed to satisfy the requirements identified in Section 5.0 of this Guideline.

3.3 IT Policy

i. The cu/caisse's Board must approve a high-level IT policy that supports the enterprise level governance of IT, IT risk management and information security. This policy must be reviewed and updated on a regular basis.

ii. Management should ensure that these high-level policies are supported by Management-level policies, standards, and procedures that address relevant controls to reduce risk for the cu/caisse.

iii. DGCM's minimum expectation is that a cu/caisse's IT Policy, Management level policies, standards and procedures will address the IT risk and information security controls listed in Section 4.0 of this Guideline.

iv. A cu/caisse's IT policies and related information security policies and processes should be assessed against industry standards or frameworks to identify any areas that are not currently covered. For example, ISO/IEC 27001- Annex A, COBIT and ITIL are well-recognized frameworks that can assist the cu/caisse to identify gaps in its information technology and information security policies, standards, and procedures.

3.4 Organization, Reporting, and Expertise

Organization and Reporting

i. A cu/caisse's IT policy must assign roles and responsibilities for IT Governance, IT Risk Management, Information Security, 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.

ii. As a best practice, the cu/caisse should 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.

iii. As a cu/caisse grows in size and complexity, it may form an IT subcommittee of Management that works with and supports the IT leadership. The responsibilities of this subcommittee may include, but are not limited to:

   a. Aligning IT strategies with overall business objectives,

   b. Reviewing major IT initiatives and their potential impact on the cu/caisse's risk profile.

Expertise

i. A cu/caisse's Board must collectively understand IT risks to provide leadership and oversight of the IT function. The cu/caisse's Board and Management must consider the level of IT experience and expertise the Board should possess and identify any gaps.

ii. 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 must include IT governance and outsourcing and regular information security awareness sessions if gaps are identified.

iii. 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.

iv. At the Management and Staff level, the cu/caisse must 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).

v. IT Staff should be provided with the opportunity and funding to attend information security related educational events, conferences, and courses. IT Management and Staff should have access to regular threat intelligence to provide them with relevant information regarding threats to IT assets (e.g., Canadian Centre for Cyber Security subscriptions).

4.0 IT Risk Management

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

IT Risk Management must identify the risks that could lead to legal, reputational, or financial loss (e.g., member data, strategic plans, financial data).

4.1 IT Risk Management and Enterprise Risk Management

i. Under the SSBP Guidance Framework, Management monitors and manages IT risks according to risk tolerances established by the Board using an ERM Framework.

ii. IT Risk Management should be a subset of the cu/caisse's Enterprise Risk Management (ERM) program to ensure that critical IT risks are elevated to the significant risks identified by the ERM program.

iii. The cu/caisse must formalize an IT Risk Management Framework that includes Management level policies and procedures to support IT Risk Management. This framework should include the processes and methodologies for identification, analysis, evaluation, and treatment of risks.

iv. As part of the IT Risk Management process, the cu/caisse must include regular review of technical and non-technical risks related to IT. For example:

   a. Cybersecurity
   b. Third-party Risk
   c. Privacy Risk
   d. Strategic Risk
   e. Compliance Risk
   f. Financial Risk
   g. Reputation Risk
   h. Supply Chain Risk
   i. Legal Risk

4.2 IT Risk Assessment

i. Through the IT Risk Management Framework, the cu/caisse must manage its IT operational and information security risks by considering threats to the confidentiality, integrity, and availability of assets, information, and services.

ii. An IT risk assessment identifies and analyzes reasonably foreseeable external and internal threats that could have a material impact to key business functions and critical IT systems (e.g., risk of hacking, breakdown, or interruption of service).

iii. The IT risk assessment may be part of the cu/caisse's overall ERM process; however, the assessment should dive into greater technical detail in assessing IT risks.

iv. An IT risk assessment can be 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. In the absence of an internal resource who is knowledgeable to conduct an IT risk assessment, the cu/caisse may engage a suitable third-party to perform the risk assessment.

v. The cu/caisse must also perform a comprehensive IT risk assessment when a new IT initiative is proposed or when a change is introduced that could alter the risk posture of the organization.

IT Risk Register

i. The results of the IT risk assessment must be documented in a formal IT risk register which should include identified risks, risk ratings, risk ownership and risk response strategies.

ii. The cu/caisse must elevate critical risks identified as part of the IT risk assessment into the ERM Register.

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

The cu/caisse may refer to industry standards and frameworks such as ISO27005, NIST SP800-37 or CIS RAM (Risk Assessment Method) to gather more information on IT Risk Management.

4.3 Information Security

Every cu/caisse must have an Information Security Policy that is supported by a robust Information Security Control Framework in place. Controls are not considered robust unless they are formalized as part of the cu/caisse's Information Security Policies.

A robust Information Security Control Framework will ensure that the cu/caisse's Information security function can meet acceptable standards for:

i. **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.

ii. **Integrity:** Information and data must be accurate and reliable, and managed using appropriate quality control practices which prevents unauthorized changes.

iii. **Availability:** Systems, data, and information are available to authorized users when required.

Information Security Maturity Assessment

i. In developing and assessing the adequacy and maturity of information security controls, the cu/caisse should regularly perform a self-assessment using a tool such as the Cyber Security Self-Assessment Guidance developed by the Office of the Superintendent of Financial Institutions (OSFI).

Information Security Resourcing

i. In addition to establishing a robust information security control framework, the Board and Senior Management should ensure appropriate resources are allocated to implement the framework.

ii. 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.

4.3.1 Access Control and User Management

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

ii. Access controls should identify the specific individuals who are authorized to have access to networks, information, business systems (e.g., banking application and loan originating system), and other key IT assets.

iii. The cu/caisse must ensure that its access control processes require all users to identify using a valid username or identity before they are authenticated to access authorized systems.

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

Administrative Controls

i. Create a formal access control policy which addresses the identification, authentication, authorization, and audit of access controls, including cu/caisse and third-party services.

ii. Restrict access of users only to systems that they are specifically authorized and required to access (least privilege).

iii. Establish processes for user management including creation, privilege allocation, user removal or deactivation, monitoring, and password management.

iv. Establish security awareness and training programs for users to include common user targeted attacks (for e.g. phishing, website spoofing and social engineering).

v. Perform access review of all accounts, including privileged users or administrative accounts, on a regular basis.

Physical Controls

i. Implement physical security controls as referred to in Section 4.3.5 of this Guideline.

Technical Controls

i. Create robust technical controls to restrict user and device access to systems, networks, and information.

ii. Restrict the use of local and domain level privileged or administrative accounts.

iii. Enforce Multi-Factor Authentication (MFA) for privileged user accounts in all cases including internal, remote access, and cloud service.

iv. Implement MFA for all remote logins and externally exposed applications.

v. Implement strong passwords or other authentication methods.

vi. Implement encryption to guard data from unauthorized access.

4.3.2 Asset Management and Operations Security

Operational Procedures

i. The cu/caisse should formally document and implement IT operating procedures to secure its information and the operation of its IT environment and facilities.

ii. Operational procedures should include the controls mentioned in Section 4.3 of this Guideline.

Asset & Information Management

i. The cu/caisse should establish and maintain an inventory of all networks, connected hardware, and mobile devices that have the ability to connect to the network or cloud resources, including mobile end-user devices. IT assets (hardware, software, and services), data, and information should be identified.

ii. The cu/caisse must establish asset and information classification policies and procedures to identify and classify all IT assets and data according to their sensitivity.

iii. Classification policies must contain guidelines to identify sensitive information that require more stringent protection controls. The cu/caisse should encrypt the data in rest and motion based on data classification and risk.

iv. IT assets may be managed through an asset management system, which tracks an asset’s introduction, assignment, maintenance, and destruction phases.

Change Management

i. A formal change management process should be documented to ensure that changes introduced to the cu/caisse’s IT environment are performed in an authorized, structured, and orderly manner to minimize any impact on business services.

ii. Changes to IT processes or systems should be formally controlled with the use of secure development and testing environments.

iii. Only authorized personnel should be able to introduce or install new software, applications, or systems.

iv. Changes should be documented and approved by Management prior to implementation.

System Hardening

i. System hardening is the process of securing technology equipment (servers, workstations, and network) by reducing its attack surface and minimizing vulnerabilities through the implementation of patches, turning off non-essential services, and remediating configuration vulnerabilities. The cu/caisse must maintain a hardening standard for all technology equipment.

ii. The standard must be regularly reviewed for currency. Industry recognized configuration benchmarks such as CIS Benchmarks can be leveraged to establish a hardening security baseline for the systems.

iii. The cu/caisse should consider implementing allow-listing to restrict unauthorized applications or scripts from running in the environment as part of the server and workstation hardening configuration.

Vulnerability and Patch Management

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

ii. This process must include regular scanning for vulnerabilities and missing patches. The absence of robust controls as outlined in Section 4.3 of this Guideline will warrant more frequent vulnerability scanning.

iii. The patch management process must ensure all software and devices (mobile devices, endpoints, servers, and network devices) are 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.

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

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

vi. The cu/caisse must take a risk-based approach to remediate the identified vulnerabilities.

System Logging and Monitoring

i. System logging and monitoring processes must be established to detect operational and security events and unauthorized access to applications and systems.

ii. 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.

iii. System logs should be monitored on a regular basis to ensure security events do not go undetected within the cu/caisse’s IT environment. Use of automated tools should be considered to provide near real-time notification of detected events and vulnerability exploitation.

iv. Log files are critical evidence during forensics investigation if an incident happens. Log files must be securely stored to prevent modification or deletion as these logs provide critical troubleshooting and investigative information to diagnose system errors or intrusions.

v. Adequate retention policies should be implemented for storage of log files to ensure sufficient historical data is available to aid the investigations of a cyber breach.

Virus and Malware Protection

i. Detective and preventive controls must be established to protect a cu/caisse against malicious or unauthorized software.

ii. Anti-virus and malware detection software should be used to regularly scan computers, storage media, email, and webpages on a precautionary and routine basis.

iii. If a system is infected with viruses or malware which cannot be removed using the native features of the tool and has the potential to spread or cause wider impacts, the cu/caisse should invoke its incident management process discussed in Section 4.3.4 of this Guideline.

iv. The cu/caisse should upgrade their malware detection software to an Extended Detection and Response (XDR) to address the modern sophisticated malware that can evade traditional or outdated antivirus solutions.

Backup and Recovery

i. Backup policies and procedures must 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.

ii. The backup strategy should consider immutability of the backup to ensure that the data is encrypted and is unchangeable.

iii. Regular testing must be performed to confirm if the backup procedures meet the requirements of the cu/caisse’s incident handling process and disaster recovery plans.

iv. Copies of backups should be stored in a safe location, physically distant from the data processing center to facilitate disaster recovery efforts and to support immutability. The storage locations should provide adequate environmental protection and should be readily accessible.

v. When using third-party cloud service providers (CSP) for data backup, the cu/caisse should consider its data protection obligations. The cu/caisse should assess the adequacy of controls pertaining to access to the stored data, service-levels, data retention, destruction, and data residency requirements. All CSPs should be managed via the cu/caisse's Third-Party Risk Management Policy.

4.3.3 Network Management

i. A cu/caisse's network should be designed to allow only authorized devices to connect. Controls should be implemented to prevent unauthorized devices from connecting to the network.

ii. Network devices, such as routers, firewalls, and switches should be appropriately configured and implemented to protect connected systems, data, applications, and users.

iii. Where applicable, a wider range of network security appliances or applications (e.g., intrusion detection systems, intrusion prevention systems, content filtering) should be utilized to provide more layered security.

iv. The use of encryption technologies should be implemented for protecting sensitive data in transit.

v. A cu/caisse should implement network segregation when designing the IT environment, based on trust levels, business units, or a 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.

vi. The banking system network must be segregated from the cu/caisse's corporate network using adequate physical or logical segregation.

vii. Network infrastructure should be protected from unauthorized changes using strong access controls like complex device passwords, MFA, and separate management networks.

4.3.4 Incident Management

i. The scope of this section primarily addresses information security incidents that require a rapid response.

ii. The cu/caisse must maintain an incident management process. This process could include operational and technology incidents. The cu/caisse must have the ability to effectively and consistently respond to "information security incident", a term that describes events or threats that impacts the confidentiality, integrity, or availability of a cu/caisse's information systems, resulting in unauthorized disclosure, modification, destruction or disruption of data, information, or system(s).

iii. An information security incident could include ransomware, employee data breach, service interruption, virus, and malware infection, etc.

iv. The information security incident management process should include:

   a. A policy/process that defines roles and responsibilities.
   b. Procedures for reporting incidents and identified weaknesses in systems or services in a timely manner.
   c. Procedures for responding to and containing identified incidents and minimizing damage.
   d. Procedures for escalating and reporting to stakeholders when a critical incident has been identified (e.g., Senior Management, Board, and regulatory bodies).
   e. 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).
   f. A process for analyzing the incident and response after the incident has been resolved (e.g., root cause analysis, lessons learned).

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

vi. A cu/caisse must notify DGCM of any "Reportable Incident" as set out in DGCM's Technology and Cyber Security Reporting Requirements (see Communiqué # 08 – 2023). The cu/caisse's incident management process should have adequate procedures to address the DGCM incident reporting requirements.

vii. A cu/caisse's Information Security Incident Management Processes must be tested regularly to keep Staff familiar with what the cu/caisse would do in the event of an incident.

viii. The Information Security Incident Management Process should incorporate the use of scenario specific playbooks (for e.g., ransomware, credential compromise, DDoS, malware infection, etc.).

ix. The Information Security Incident Management Process should allow decision makers to escalate their response if the impact or risk is likely to cause a business continuity risk.

4.3.5 Physical and Environmental Security

i. Physical security controls must 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 including servers, workstations, networking infrastructure, data processing facilities, etc. and include adequate physical and environmental protection.

ii. Physical security should provide protection from:

   a. Environmental threats (e.g., floods, fires)
   b. Human threats (e.g., criminals, malicious employees, contractors, unauthorized parties)
   c. Power and utility interruption (e.g., electrical, HVAC)
   d. Unauthorized surveillance devices (e.g., cameras, keyloggers)

iii. 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:

   a. Outer Perimeter (areas outside the building, including the outside walls and doors of the building)
   b. Inner Perimeter (areas inside the building, offices, and meeting rooms)
   c. Core Perimeter (usually a server or systems room which houses sensitive infrastructure)

iv. Controls within each layer can range from swipe cards, security cameras, alarms, HVAC systems, fire suppression systems, and cabling closets.

v. A cu/caisse should consider a risk-based layered approach using a range of controls within each perimeter.

4.3.6 System Acquisition and Development

i. 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 planning, analysis, design and implementation of the new system or system change.

ii. Technology risk and Information Security requirements must be considered before introducing new systems or making changes to existing systems. If security requirements cannot be met within the newly acquired or developed/altered system, compensating controls must be implemented.

iii. For systems designed and built in-house, including custom developed applications, development should be performed following a secure development methodology.

iv. Changes to custom developed applications must be controlled, tested for functionality and security, and managed to ensure that new risks are not introduced to the cu/caisse.

v. For systems developed by a third-party, controls and monitoring processes should be put in place to ensure that these third-parties are developing applications and systems following a secure development methodology, and that technology risk and information security requirements are being met. (See Section 4.4 Third-Party IT Risk Management of this Guideline)

4.3.7 IT Disaster Recovery Plan

i. IT Disaster Recovery (ITDR) planning must be a part of the cu/caisse's overall business continuity regime. The ITDR should include planning for recovery of applications, data, hardware, communications (such as networking) and other IT infrastructure.

ii. The ITDR Plan should meet the requirements of business impact assessments (BIA) of the cu/caisse's Business Continuity Plan. Refer to SSBP Guidance Framework – Standard #3 for DGCM's expectations related to business continuity risk.

iii. The cu/caisse must have an ITDR Plan that details the 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.

iv. An ITDR Plan should include the following components:

   a. Identification of scenarios or incidents that may disrupt or slow down the cu/caisse's critical functions.

   b. An inventory and assessment of the cu/caisse's existing IT infrastructure required to support its critical functions. This assessment should include:

      - An inventory of computing resources, databases, storage, security, network components, personnel, and vendors (lists with key contact information).
      - Recovery Time Objectives and Recovery Point Objectives identified from the BIA.
      - An analysis of the failure of one or more components of the cu/caisse's IT infrastructure and its impact on a critical function.

c. Identification of available resources to respond to incidents or disruptions and the assignment of roles and responsibilities.

d. Identification of alternate sites (head office, alternate branches, data centers, etc.) for continuity of operations, including relocation and restoration procedures with particular emphasis on utilization of backups.

e. Recovery procedures including steps and resources to assess damage and execute the recovery of critical IT systems and information.

v. A cu/caisse's ITDR Plan must 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. The Plan should be updated based on the lessons learned from the ITDR test.

vi. Training should be provided to employees with responsibilities under the ITDR to ensure they understand the Plans and their roles.

vii. A cu/caisse must consider its dependency on third-parties and cloud service providers (CSP) while formulating ITDR Plans. The cu/caisse should ensure that the recovery timelines and expectations are formally agreed with the service providers.

4.4 Third-party IT Risk Management

This Section of the Guideline is intended to be read and interpreted in conjunction with the DGCM's Third-Party Risk Management Guideline.

Outsourcing technology services to third-party service providers is a common practice among cu/caisse. This practice includes outsourcing of banking applications, application development, loan origination systems (LOS), cloud services providers (CSP) for backup etc., managed IT service providers (MSP), and IT Audit Service providers, etc.

4.4.1 Outsourcing of IT Functions

Third-Party Governance

i. The cu/caisse must establish a third-party risk management policy that defines and governs the risk management related to third-party relationships.

ii. The cu/caisse must maintain oversight of its third-party arrangements. This oversight includes ensuring strict adherence to the agreed-upon terms and conditions. The Board should be provided with information about the extent to which the cu/caisse's IT services has been outsourced.

iii. The cu/caisse should perform a risk assessment to identify the risks that the organization might be exposed to while engaging the third-party's services.

iv. All material third-party arrangements must be supported by a formal contract.

4.4.2 Contractual Arrangements

Provision of Services

i. Service levels associated with each service must be identified and formally agreed between all stakeholders via a Service Level Agreement (SLA).

ii. Roles and responsibilities for information security controls that are mentioned in Section 4.3 of this Guideline should be formally agreed with the third-party.

iii. The cu/caisse should ensure that the competency of resources allocated to provide the services are adequate to ensure the quality of services.

Confidentiality, Privacy, and Security

i. The contract should address which party is responsible for ensuring the confidentiality, security, and privacy of cu/caisse data and member data. This includes:

   a. Scope and definition of the information to be protected.

   b. Third-party's respective security obligations including procedures.

   c. Liability for losses resulting from a security breach, and

   d. Notification processes in the event of a breach

ii. To ensure privacy and security of data, the contract should detail measures to segregate cu/caisse data and functions from other data and functions of the service provider.

iii. Data security and compliance requirements including data lifecycle management and data residency requirements where applicable should be identified and formally agreed through the contract.

Ownership and Access

i. The contract should clarify who has ownership rights of relevant assets, such as data, devices, source codes, logs, applications, and reports (including assets derived from cu/caisse data).

ii. The cu/caisse must consider the risk of contract termination on the data portability and should consider data off-boarding in the exit strategy.

iii. 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.

iv. The third-party access to the cu/caisse's IT environment must follow the principle of least-privilege. All access provisioning and de-provisioning must follow the cu/caisse's Access Management Policy.

Contingency Planning

i. The cu/caisse must review the continuity commitments from the third-party to ensure that they are adequate to support the cu/caisse's own continuity requirements.

ii. The contract should include details about the service provider's measures and resources for ensuring the continuity of the outsourced function.

iii. The cu/caisse should require the service provider to perform regularly scheduled testing of Business Continuity and Disaster recovery requirements.

iv. Incident management and reporting requirements for operational and information security incidents should be identified and agreed with the third-party.

v. Expectations regarding cyber insurance coverage and forensic investigation capabilities should be identified and agreed with the third-parties.

Monitoring, Reporting and Audit Rights

i. Logging and monitoring processes for the services provided must be identified and documented in the contract. This should include coverage of assets and services logged and log retention periods.

ii. All reporting requirements including service levels, incidents, and other operational performance reporting requirements must be agreed with the third-party via formal SLA in the contract.

iii. The right to audit each other may also be clarified in the contract.

iv. For critical functions such as banking systems and managed security services, 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

i. The cu/caisse must identify whether functions are subcontracted by its third-parties.

ii. If subcontracting is permitted, the cu/caisse's contract with the service provider must stipulate that all privacy, security, access, and audit obligations also apply to the subcontractor.

5.0 IT Audits

5.1 Audit Committee and Internal Audit

i. 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.

ii. 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 this Guideline.

iii. IT Audits must be considered as part of the cu/caisse's Internal Audit function. IT Audits should not be confused with IT Risk Assessments (Section 4.2) and IT Maturity Assessments (Section 4.3) performed by Management as these serve different objectives.

iv. IT audits may require specialized knowledge and expertise 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 over the execution of the audit and follow-up process.

v. The cu/caisse must ensure that the IT audit includes test of design and operating effectiveness.

vi. Test of operating effectiveness focuses on evaluating whether the controls are functioning in practice and operating as intended to mitigate risks and achieve control objectives over a period of time (typically 12 months).

vii. While engaging with an external IT audit service provider, the cu/caisse should review the following information.

   a. The qualifications, certifications, skillset, and relevant experience of the personnel that will be performing the audit.
   b. The auditors understanding of the scope (Section 4.1 to 4.4) and testing requirements mentioned in this Guideline (Section 5.2 and 5.3).
   c. References from previous engagements of the auditor

5.2 Scope and Frequency of IT Audits

i. As mentioned earlier in Section 4.0, DGCM's minimum expectation is that a cu/caisse will implement controls described in Section 4.0. 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.

ii. DGCM's expectation is that, at minimum, all controls described in Section 4.0 (4.1 to 4.4) of this Guidelines must be audited at least every three years.

iii. Defining the purpose and scope of the IT audit is critical to receiving the assurance required by the cu/caisse Board and Management. The cu/caisse must ensure that the audit report adequately captures information pertaining to the scope of audit, framework used, and the period for which the operating effectiveness was tested.

iv. The report should contain adequate commentary from the auditor regarding the observations and deficiencies in control implementations.

v. Beyond the minimum requirements, the cu/caisse should consider expanding the scope of audits to include other areas such as:

   a. IT Governance
   b. Business/IT Strategic Alignment
   c. Project Management

5.3 Audits of Banking Systems

i. 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. Senior Management must have a robust understanding of the extent to which the cu/caisse's core banking system has been outsourced and its dependency on subcontractors.

ii. 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 services.

iii. DGCM's minimum requirement is that each cu/caisse that hosts their own banking system must perform an annual IT audit of the design and operating effectiveness of entity's internal controls over the core banking system that is equivalent to a CSAE 3416.

iv. In cases where a banking system is partially or fully outsourced to a third-party service provider, the cu/caisse must obtain an annual independent attestation that is CSAE 3416 or equivalent from the service provider for the outsourced component.

v. To gain clarity with respect to the types of banking system arrangements and DGCM's minimum audit requirements, refer to Table 1 below.

vi. While reviewing the third-party attestation reports, the cu/caisse must ensure that the section typically referred to in the report as "Complementary User Entity

Controls" is reviewed to ensure that the applicable controls are implemented at the cu/caisse's environment.

vii. When control deficiencies are identified, the cu/caisse is expected to assess these findings and determine if compensating controls are required.

Table 1: Banking Systems – Audit Requirements

Level of Outsourcing	Details	Audit Requirement
Fully In-House	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 or equivalent.
Partly Outsourced	Mixed ownership or control of banking system. Third-Party may provide critical IT support service or have licensed the use of their product. However, cu/caisse may: • Retain ownership of source code. • Maintain data in-house. • Host and manage components of the banking system 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 or equivalent**.** For cu/caisse entity-controlled banking system functions: annual IT audit of relevant banking system IT controls – CSAE 3416 or equivalent.
Fully Outsourced	Banking system owned and controlled by a third-party service provider. The third-party provides critical IT support service.	Annual verification from service provider: CSAE 3416 or equivalent

Appendix A – Audit Requirements Summary

A.1 IT Audit Requirements

The table below is intended to provide the cu/caisse with guidance on the minimum scoping and requirements of IT Audits pertaining to sections 5.2 of this Guideline.
The cu/caisse must exercise their own due diligence in the scoping and engagement of qualified IT auditors.

Audit Frequency	Every 3 years
Audit Scope	4.0 IT Risk Management
	4.2 IT Risk Assessment
	4.3 Information Security
	4.3.1 Access Control and user Management
	4.3.2 Asset Management and Operations Security
	4.3.3 Network Management
	4.3.4 Incident Management
	4.3.5 Physical and Environmental Security
	4.3.6 System, Acquisition and Development
	4.3.7 IT Disaster Recovery Plan
	4.4 Third-party IT Risk Management
	4.4.1 Outsourcing of IT Functions
Control Testing	Test of design and operating effectiveness of IT controls
Auditor Selection Criteria	• Qualifications, certifications, skillset, and relevant experience of the personnel that will be performing the audit. • Auditor’s understanding of the scope (Section 4.1 to 4.4) and testing requirements mentioned in this Guideline (Section 5.2). • References from previous engagements of the auditor
Audit Reporting Requirements	• Scope of Audit • Audit Framework • Period for which the samples were tested. • Observations and deficiencies in control implementations

A.2 Banking System Audit Requirements

The table below is intended to provide the cu/caisse with guidance on the minimum scoping and requirements for Banking System Audits pertaining to section 5.2 of this Guideline.
The cu/caisse must exercise its own due diligence in the scoping and engagement of qualified IT auditors.

Audit Frequency	Annual
Audit Scope	4.3 Information Security
	4.3.1 Access Control and user Management
	4.3.2 Asset Management and Operations Security
	4.3.3 Network Management
	4.3.4 Incident Management
	4.3.5 Physical and Environmental Security
	4.3.6 System, Acquisition and Development
	4.3.7 IT Disaster Recovery Plan
Control Testing	• Test of design and operating effectiveness of IT controls
Auditor Selection Criteria	• Qualifications, certifications, skillset, and relevant experience of the personnel that will be performing the audit • Auditor’s understanding of the scope (Section 4.3) and testing requirements mentioned in this Guideline (Section 5.2 and 5.3) • References from previous engagement of the auditor *Refer to section 5.3 of this Guideline for more information on audit of banking systems where outsourcing is involved.*
Audit Reporting Requirements	• Scope of Audit • Audit Framework • Period for which the samples were tested • Observations and deficiencies in control implementations

Appendix B – Glossary

Term	Definition
Allow-Listing	A security capability that reduces harmful security attacks by allowing only trusted files, applications, and processes to be run.
Audit Scope	The boundaries and objectives defined for an audit, outlining the specific areas, processes, or activities to be examined and evaluated.
Business Impact Assessment (BIA)	The process of determining the criticality of business activities, priority of recovery and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption.
Cloud Service Provider (CSP)	A third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services.
Core banking system	The primary IT platform used to manage core banking functions, including customer accounts, deposits, loans, payments, and other financial transactions.
Data off-boarding	The process of moving data from a third-party service provider or cloud service to self-managed storage (such as an on-site dedicated server or a private cloud).
Data Portability	The ability to efficiently transfer between different cloud services. It involves the seamless movement of digital assets, applications, and information, allowing businesses to maintain control and flexibility over their data.
De-provisioning	The part of the employee lifecycle in which access rights to software and network services are taken away, usually upon employment termination or role change.
Extended Detection and Response (XDR)	XDR solutions typically include components like endpoint detection and response (EDR), network detection and response (NDR), user and entity behavior analytics (UEBA), and threat intelligence, among others.
Immutable backup	A backup copy of data that is stored in a manner that prevents any modifications, deletions, or alterations to the backup data for a specified period of time.
Information Classification	The process of categorizing data assets based on their sensitivity, importance, and confidentiality requirements to help the CU/Caisse understand the required level of protection and controls.
Information Security Control Framework	A structured set of policies, procedures, standards, and guidelines designed to help organizations establish and maintain effective information security practices.
IT Subcommittee	A dedicated management subcommittee, consisting of leaders from business departments and the CIO, that examine technology opportunities in detail and ensure that business requirements are being met by IT strategic planning.
Keylogger	A form of malware or hardware that keeps track of, and records, your keystrokes as you type.
Least-privilege	An information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions
Logical Segregation	Partitioning computer systems, networks, or data into distinct domains or subnetworks with strict controls to limit security risks and unauthorized access.
Management Network	A segregated network segment for secure administration, monitoring, and configuration of IT assets, safeguarding critical management functions from user or production network risks.

Multi-factor Authentication (MFA)	A security mechanism that requires users to provide two or more authentication factors to verify their identity before granting access to a system, application, or resource.
Operating Effectiveness	An assessment of how well the established controls are functioning in practice by focusing on evaluating whether the controls are operating as intended to mitigate risks over a period of time, usually 12 months.
Penetration Testing	Also known as ethical hacking or "pen testing," is a controlled, simulated attack on an organization's IT systems, networks, or applications to identify security weaknesses and assess the effectiveness of existing security controls. Unlike vulnerability assessments, penetration testing involves attempting to exploit identified vulnerabilities to demonstrate their impact on the organization's security.
Subcontracting	The practice of hiring third-party vendors or subcontractors to perform specific tasks or deliverables outlined in the contract, often due to expertise or resource limitations within the contracted organization.
Technology Risk	The potential for adverse impacts on an organization resulting from the use, adoption, or reliance on information technology systems, infrastructure, applications, or processes.
Test of Design	The process of walking through, understanding and evaluating that the design of the business process and related controls within the process are effective in mitigating and managing risks without testing a sample to determine the operating effectiveness of the control.
Third-Party Vendor	An entity with which an organization has a business relationship and that has access to the organization's protected data assets that, if breached, could harm the cu/caisse's finances, reputation, or compliance. Third parties include IT suppliers, banking system providers, marketing partners, payroll vendors, and others.
Vulnerability Assessment	A systematic process of identifying, quantifying, and prioritizing vulnerabilities or weaknesses in an organization's IT environment using automated scanning tools and software to analyze networks, systems, and applications for known vulnerabilities, misconfigurations, or weaknesses that could be exploited by attackers.