



# REGULATORY GUIDELINE AND PRUDENTIAL STANDARD Technology and Cyber Risk Management

**SYSTEM COMMUNICATION NUMBER 2024-03**

**APPLICABLE TO Credit Unions and SaskCentral**

**ISSUE DATE**  
NOVEMBER 2024

## TABLE OF CONTENTS

I.	Introduction .....	1
II.	Purpose .....	1
III.	Scope and Application.....	1
	Definitions.....	3
IV.	Governance and Risk Management .....	4
	Accountability and Organization Structure .....	4
	Technology and Cyber Strategy .....	4
	Technology and Cyber Risk Management Framework .....	5
V.	Technology Operations and Resilience.....	5
	Technology Architecture.....	5
	Technology Asset Management .....	6
	Technology Project Management .....	7
	System Development Life Cycle .....	7
	Change and Release Management .....	7
	Patch Management.....	8
	Incident and Problem Management.....	8
	Technology Service Measurement and Monitoring.....	9
	Disaster Recovery .....	9
VI.	Cyber Security .....	10
	Identify .....	10
	Defend .....	11

	Detect .....	13
	Respond, Recover, and Learn .....	13
VII.	Reporting of Technology and Cyber Security Incidents .....	14
	Criteria for Reporting .....	14
	Initial Notification Requirements.....	15
	Subsequent Reporting Requirements .....	15
	Failure to Report .....	15
	Appendix A – Examples of Reportable Incidents .....	16
	Appendix B – Technology and Cyber Incident Reporting Form .....	17

## I. INTRODUCTION

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

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

## II. PURPOSE

The purpose of this Guideline and Standard is to communicate the Corporation's expectations with respect to technology and cyber risk management. It is applicable to all Saskatchewan Credit Unions and SaskCentral, collectively referred to as Provincially Regulated Financial Institutions (PRFIs).

These expectations aim to support PRFIs, in developing greater resilience to technology and cyber risks. In cases where third parties are relied upon for technology and cyber risk management, the responsibility still lies with the PRFI to hold their third-party vendors accountable to these requirements.

This Guideline and Standard should be reviewed, and implemented, from a risk-based perspective that allows PRFIs to compete effectively and take full advantage of digital innovation, while maintaining sound technology and cyber risk management.

The Corporation expects PRFIs to be proactive and aware of best practices related to technology and cyber risk management that are applicable to their institution. Where appropriate, the institution is expected to adopt these best practices.

## III. SCOPE AND APPLICATION

### STRUCTURE

This Guideline and Prudential Standard is organized into three domains that broadly align with the concepts of technology and cyber risk management. Each domain contains principles that set expectations and describe best practices for developing greater resiliency to technology and cyber risk. Under each principle, there are specific topics that are used to further illustrate and clarify expectations. These topics support PRFIs in meeting the expectations of the principle, and subsequently, the domain.

- **Section IV. Governance and risk management** – Principles 1 to 3 sets the Corporation’s expectations for the formal accountability, leadership, organizational structure, and framework used to support risk management and oversight of technology and cyber security.
- **Section V. Technology operations and resilience** – Principles 4 to 13 sets the Corporation’s expectations for oversight of risks related to the design, implementation, management, and recovery of technology assets and services.
- **Section VI. Cyber security** – Principles 14 to 17 sets the Corporation’s expectations for management and oversight of cyber risk.

## OUTCOMES AND APPLICATION

The Corporation recognizes there is no “one-size fits all” approach to technology and cyber risks. Given the unique risks and vulnerabilities that vary across PRFIs, this Guideline and Prudential Standard uses principles as the foundation for regulatory guidance. Principles communicate the spirit of the expectation, without prescribing the form by which the principle is achieved. As a result, PRFIs should review, and implement, this Guideline and Prudential Standard from a risk-based perspective, giving consideration to both the principles described in this document and the risk profile of the institution. This includes the nature, scope, and complexity of operations of the PRFI.

There are three desired outcomes for all PRFIs to achieve through the application of this Guideline and Prudential Standard. These desired outcomes are based on the domains of technology and cyber risk management, and include:

- Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.
- A technology environment that is stable, scalable, and resilient. The environment is kept current and supported by robust and sustainable technology operating and recovery processes.
- A secure technology posture that maintains the confidentiality, integrity, and availability of the PRFIs technology assets. PRFIs need to be able to proactively identify, defend, detect, respond, and recover from external and insider cyber security threats.

When reviewing the PRFIs compliance with this Guideline and Prudential Standard, the Corporation will focus supervisory efforts on the inherent and residual risks posed by technology and cyber risk – as opposed to the technology itself. The Corporation’s expectations and level of supervisory intensity at each PRFI, will factor in risk profile, complexity of technology operations, and the extent to which PRFIs are achieving the desired outcomes listed above. To the extent possible, the Corporation will apply consistent expectations across PRFIs with similar characteristics.

## INCIDENT REPORTING

The technology and cyber security incident reporting requirements outlined in this Guideline and Standard, support a coordinated and integrated approach to the Corporation’s awareness of, and response to technology and cyber security incidents at PRFIs. PRFIs are required to provide timely notification to the Corporation when incidents relating to their operations occur. PRFIs need to refer to section VII of this document for these requirements.

## RELATED GUIDANCE AND INFORMATION

Technology and cyber risks are dynamic and intersect with other risk areas. PRFIs should review this Guideline and Prudential Standard in conjunction with other guidelines, standards, and communication issued by the Corporation.

The Corporation recognizes that other internationally recognized standard setters have established frameworks and guidance for managing technology systems and assets. While the Corporation does not endorse any particular framework, PRFIs are still encouraged to refer to these frameworks and utilize their guidance. This helps PRFIs remain aware of and develop greater resilience to technology and cyber risk. PRFIs should ensure the use of any framework is best suited to their business context.

## DEFINITIONS

- **Technology** - is broadly referred to as "Information Technology" (IT) in this Guideline and Prudential Standard, which includes the hardware, software, communication, and other facilities used to input, store, process, transmit, and output data in whatever form.
- **Cybersecurity** - Is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.
- **Technology Asset** - Is something tangible (e.g., hardware, infrastructure) or intangible (e.g., software, data, information) that needs protection and supports the provision of technology services.
- **Technology Architecture** - Refers to the structural design of IT hardware, software, networks, and data resources, and the synchronization of these resources with the business needs of an organization.
- **Technology Risk** - Includes "cyber risk" and refers to the risk arising from the inadequacy, disruption, destruction, failure, damage from unauthorized access, modifications, or malicious use of information technology assets, people or processes that enable and support business needs, and can result in financial loss and/or reputational damage.
- **Technology or Cyber Security Incident** - Refers to an incident that has an impact, or the potential to have an impact on the operations of a PRFI including its confidentiality, integrity or the availability of its systems and information. Examples of the characteristics of a technology or cyber incident can be found in section VII Reporting of Technology and Cyber Incidents.
- **Forensic Investigation** - The formal process of examining, preserving, and analyzing data collected from various data sources (e.g., files, operating systems, network traffic, applications, etc.) on IT or cybersecurity incidents and reporting of the results (e.g., root causes, perpetrators, actions, recommendations etc.) of the analysis for purposes including court cases, insurance claims, and regulatory audits.

## IV. GOVERNANCE AND RISK MANAGEMENT

Outcome: Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.

### ACCOUNTABILITY AND ORGANIZATION STRUCTURE

**Principle 1:** Senior Management is responsible for managing technology and cyber risks. The organizational structure should allow for proper oversight for managing these risks and Senior Management should ensure adequate resourcing is in place for managing technology and cyber risks across the PRFI.

#### 1.1 Senior Management and Board accountability

Senior Management is accountable for directing the PRFI's technology and cyber security operations and should assign clear responsibility for technology and cyber risk governance. Adequate oversight of third parties who provide technology and cyber management is also required. The Corporation expects the Board to ensure management is monitoring and managing technology and cyber risks according to risk tolerances established in its Enterprise Risk Management (ERM) framework.

#### 1.2 Appropriate structure, resources, and training

To ensure appropriate structure, resources, and training are provided, PRFIs should:

- Establish an organizational structure for managing technology and cyber risks across the institution, with clear roles and responsibilities, adequate people and financial resources, and appropriate subject-matter expertise and training.
- Include among its Senior Management ranks persons with sufficient understanding of technology and cyber risks. The level of understanding needs to be commensurate with the risk profile of the PRFI.
- Ensure the Board has sufficient knowledge and information of technology and cyber risk to understand the decisions, plans, and policies being implemented by Senior Management.
- Promote a culture of risk awareness in relation to technology and cyber risks throughout the institution.

### TECHNOLOGY AND CYBER STRATEGY

**Principle 2:** PRFIs should define, document, approve and implement a strategic technology and cyber plan(s). The plan(s) should align to business strategy and set goals and objectives that are measurable and evolve with changes in the PRFI's technology and cyber environment.

#### 2.1 Proactive, comprehensive, and measurable strategy

A PRFI's strategic technology and cyber plan(s) should consider the following elements:

- Anticipate and evolve with potential changes in the PRFI's internal and external technology and cyber environment.
- Reference planned changes in the PRFI's technology environment.
- Clearly outline the drivers, opportunities, vulnerabilities, threats, and measures to report on progress against strategic objectives.
- Include risk indicators that are defined, measured, monitored, and reported on.
- Articulate how technology and cyber security operations will support the overall business strategy.

## TECHNOLOGY AND CYBER RISK MANAGEMENT FRAMEWORK

**Principle 3:** PRFIs should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks and define PRFIs processes and requirements to identify, assess, manage, monitor, and report on technology and cyber risks.

### 3.1 RMF is well aligned and continuously improved

PRFIs should establish a framework for managing technology and cyber risks in alignment with its ERM framework. PRFIs should regularly review and refresh its technology and cyber RMF to make continuous improvements based on implementation, monitoring, and other lessons learned (e.g., past incidents).

### 3.2 RMF captures key elements

PRFIs should consider the following elements of risk management when establishing the technology and cyber RMF:

- Accountability for Technology and Cyber Risk Management, including for the Board, Senior Management, and relevant Oversight Functions.
- Technology and cyber risk appetite and measurement (e.g., limits, thresholds, and tolerance levels).
- A technology and cyber risk taxonomy, i.e., system of classification.
- Control domains for technology and cyber security, i.e., the controls in place to mitigate risk.
- Policies, standards and processes governing technology and cyber risk, which are approved, regularly reviewed and consistently implemented enterprise-wide.
- Processes for identifying, assessing, managing, monitoring, and reporting on technology and cyber risks, including processes for managing exceptions.
- Management of unique risks posed by emerging threats and technologies.
- Reporting on technology and cyber risk appetite measures, exposures, and trends to inform the PRFIs current and emerging risk profile.

## V. TECHNOLOGY OPERATIONS AND RESILIENCE

Outcome: A technology environment that is stable, scalable, and resilient. The environment is to be kept current and supported by robust and sustainable technology operations and recovery processes.

## TECHNOLOGY ARCHITECTURE

**Principle 4:** PRFIs should implement a technology architecture framework, with supporting processes to ensure solutions are in line with business, technology, and security requirements.

### 4.1 Architecture framework ensures technology supports business needs

PRFIs should establish a framework of principles necessary to govern, manage, evolve, and consistently implement IT architecture across the institution in support of the enterprise's strategic technology, security and business goals, and requirements.

## 4.2 Architecture is comprehensive

The scope of architecture principles should be comprehensive (e.g., considers infrastructure, applications, emerging technologies, and relevant data). Using a risk-based approach that is commensurate with business needs, systems, and associated infrastructure should be designed and implemented to achieve availability, scalability, security, and resilience.

## TECHNOLOGY ASSET MANAGEMENT

**Principle 5:** PRFIs should maintain an updated inventory of all technology assets supporting business processes or functions. PRFIs asset management processes should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology.

### 5.1 Technology asset management standards are established

PRFIs should establish standards and procedures to manage technology assets.

### 5.2 Inventory is maintained, and assets are categorized, including asset configurations

PRFIs should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle. Based on the PRFI's risk tolerance, this may include assets owned or leased, and third-party assets that store or process PRFI information or provide critical business services. The asset management system should be supported by:

- Processes to categorize technology assets based on their criticality and/or classification. These processes should identify critical technology assets that are of high importance to the PRFI, or which could attract threat actors and cyber-attacks, and therefore require enhanced cyber protections.
- Documented interdependencies between critical technology assets, where appropriate. This is to enable proper change and configuration management processes, and to assist in response to security and operational incidents, including cyber-attacks.
- A system for recording and managing asset configurations. Processes should be in place to identify, assess, and remediate discrepancies from the approved baseline configuration, and to report on breaches.

### 5.3 Standards for safe disposal of technology assets are established

PRFIs should define standards and implement processes to ensure the secure disposal or destruction of technology assets.

### 5.4 Technology software and hardware is kept up-to-date

PRFIs are expected to continuously monitor the software and hardware assets used in the technology environment in support of business processes. It should proactively implement plans to mitigate and manage risks stemming from unpatched, outdated, or unsupported assets and replace or upgrade assets before maintenance ceases.

## TECHNOLOGY PROJECT MANAGEMENT

**Principle 6:** Ensure effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within the PRFIs risk appetite.

### 6.1 Technology projects are governed by an enterprise-wide project management framework

Technology projects should be governed by an enterprise-wide project management framework that provides for consistent approaches and achievement of project outcomes in support of the PRFIs technology strategy. The PRFI should measure, monitor, and periodically report on project performance and associated risks.

## SYSTEM DEVELOPMENT LIFE CYCLE

**Principle 7:** PRFIs should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition, and maintenance of technology systems that perform as expected in support of business objectives.

### 7.1 SDLC framework needs to guide system and software development

The SDLC framework should outline processes and controls in each phase of the SDLC to achieve security and functionality, while ensuring systems and software perform as expected to support business objectives. This includes ensuring:

- security requirements are embedded throughout the SDLC
- there is integration of development, security, and technology operations, in that new software and services can be delivered rapidly without compromising application security
- that acquired systems and software are assessed for risk and that systems implementation is subject to the control requirements as required by the SDLC
- coding principles, if applicable<sup>1</sup>, are defined and implemented

## CHANGE AND RELEASE MANAGEMENT

**Principle 8:** PRFIs should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment.

### 8.1 Changes to technology assets are conducted in a controlled manner

PRFIs should ensure that changes to technology assets in the production environment are documented, assessed, tested, approved, implemented, and verified in a controlled manner. The change and release management standard should clearly outline the key controls required throughout the change management process and define emergency change and control requirements.

---

<sup>1</sup> PRFIs that are programming their own systems or applications should implement best coding practices (e.g., secure coding, coding repositories and tools, etc.)

## **8.2 Segregation of duties controls against unauthorized changes**

PRFIs should implement segregation of duties as a key control for protecting assets from unauthorized changes. PRFIs should segregate duties in the change management process to ensure that the same person cannot develop, authorize, execute, and move code or releases between production and non-production technology environments.

## **8.3 Changes to technology assets are traceable**

Controls should be implemented to ensure traceability and integrity of the change record as well as the asset being changed (e.g., code, releases) in each phase of the change management process.

## **PATCH MANAGEMENT**

**Principle 9:** PRFIs should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws.

### **9.1 Patches are applied in a timely and controlled manner**

The patch management process should define clear roles and responsibilities for all stakeholders involved. Patching should follow the PRFIs existing change management processes, including emergency change processes. Best practice recommends patches should be tested before deployment to the production environment.

## **INCIDENT AND PROBLEM MANAGEMENT**

**Principle 10:** PRFIs should effectively detect, log, manage, resolve, monitor, and report on technology incidents and minimize their impacts.

## **Requirements for reporting of technology and cyber security incidents to the Corporation is described in section VII.**

### **10.1 Incidents are managed to minimize impact on affected systems and business processes**

PRFIs should define standards and implement processes for incident and problem management. Standards should provide an appropriate governance structure for timely identification and escalation of incidents, restoration and/or recovery of an affected system, and investigation and resolution of incident root causes.

### **10.2 Incident management process is clear, responsive, and risk-based**

Processes and procedures for managing technology incidents should include:

- Defining and documenting roles and responsibilities of relevant internal and external parties to support effective incident response.
- Establishing early warning indicators or triggers of system disruption (i.e., detection).
- Identifying and classifying incidents according to priority, based on their impacts on business services.
- Developing and implementing incident response procedures that mitigate the impacts of incidents, including internal and external communication actions that contain escalation and notification triggers and processes.
- Performing periodic testing and exercises using plausible scenarios in order to identify and remedy gaps in incident response actions and capabilities.
- Establishing and periodically testing incident management processes with third parties.
- Conducting post-incident reviews, root cause and impact diagnostics, and identification of trends or patterns in incidents.

## TECHNOLOGY SERVICE MEASUREMENT AND MONITORING

**Principle 11:** PRFIs should develop service and capacity standards and processes to monitor operational management of technology, ensuring business needs are met.

### **11.1 Technology service performance is measured, monitored and regularly reviewed for improvement**

PRFIs should establish technology service management standards with defined performance indicators and/or service targets that can be used to measure and monitor the delivery of technology services. Processes should also provide for remediation where targets are not being met.

### **11.2 Technology infrastructure performance and capacity are sufficient**

PRFIs should define performance and capacity requirements with thresholds on infrastructure utilization. These requirements should be continuously monitored against defined thresholds to ensure technology performance and capacity support current and future business needs.

## DISASTER RECOVERY

**Principle 12:** PRFIs should establish and maintain a Business Continuity Program (BCP) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

### **12.1 Disaster recovery program is established**

PRFIs should develop, implement, and maintain a BCP that sets out their approach to recovering technology services during a disruption. The BCP should clearly outline the:

- Accountability and responsibility for the availability and recovery of technology services, including recovery actions.
- A process for identifying and analyzing technology services and key dependencies required to operate within the PRFIs risk tolerance.
- Plans, procedures and/or capabilities to recover technology services to an acceptable level, within an acceptable timeframe, as defined and prioritized by the PRFI.
- A policy or standard with controls for data back-up and recovery processes, requirements for data storage and periodic testing.

### **12.2 Key dependencies are managed**

PRFIs should manage key dependencies required to support the BCP, such as:

- Information security requirements for data security and storage (e.g., encryption).
- Location of technology asset centres, backup sites, and service providers.
- Proximity to primary data centres and other critical technology asset and locations.

**Principle 13:** PRFIs should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected through disruption.

### **13.1 Disaster recovery scenarios are tested**

PRFIs should regularly validate and report on their disaster recovery strategies, plans, and/or capabilities against severe but plausible scenarios. These scenarios should be forward looking and consider, where appropriate:

- New and emerging risks or threats
- Material changes to business objectives or technologies
- Situations that can lead to prolonged outage
- Previous incident history and known technology complexities or weaknesses

PRFIs disaster recovery scenarios should test:

- The PRFIs backup and recovery capabilities and processes to validate resiliency strategies, plans and actions, and confirm the organization's ability to meet pre-defined requirements.
- Critical third-party technologies and integration points with upstream and downstream dependencies, including both on-and-off premises technology.

## **VI. CYBER SECURITY**

**Outcome:** A secure technology posture that maintains the confidentiality, integrity, and availability of PRFIs' technology assets. PRFIs need to be able to proactively identify, defend, detect, respond, and recover from external and insider cyber security threats.

### **IDENTIFY**

**Principle 14:** PRFIs should maintain a range of practices, capabilities, processes, and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors.

### **14.1 Security Risks are identified**

PRFIs should identify current or emerging cyber threats proactively using threat assessments to evaluate threats and assess security risk. This includes implementing information and cyber security threat and risk assessments, processes, and tools to cover controls at different layers of defence.

### **14.2 Intelligence-led threat assessment and testing is conducted**

PRFIs should adopt a risk-based approach to threat assessment and testing. These regularly performed tests should identify vulnerabilities or control gaps in the cyber security processes, controls, and programs (e.g., penetration testing) to mitigate current and emerging threats. The scope and potential impacts of such testing should be clearly defined by the PRFIs with effective risk mitigation controls throughout the assessment process.

### **14.3 Vulnerabilities are identified, assessed, and ranked**

PRFIs should establish processes to conduct regular vulnerability assessments of its technology assets (e.g., network devices, systems, applications). Processes should articulate the frequency with which vulnerability scans and assessments are conducted. Based on these assessments, PRFIs should assess and rank relevant cyber vulnerabilities and threats according to the severity of the threat and risk exposure to technology assets.

#### **14.4 Data is identified, classified, and protected**

PRFIs should ensure that adequate controls are in place to identify, classify, and protect structured and unstructured data based on their confidentiality classification. PRFIs should implement processes to perform periodic discovery scans to identify changes and deviations from established standards and controls to protect data from unauthorized access.

#### **14.5 Continuous situational awareness and information sharing are maintained**

PRFIs should maintain continuous situational awareness of the external cyber threat landscape and its threat environment as it applies to its technology assets. This includes subscribing to timely and reputable threat information sources and participating, where applicable, in information sharing forums.

#### **14.6 Threat modelling and hunting are conducted**

Where feasible, PRFIs should maintain cyber threat models to identify cyber security threats directly facing its technology assets and services. Threats should be assessed regularly to enhance the cyber security program, capabilities and controls required to mitigate current and emerging threats. PRFIs should use manual techniques to proactively identify and isolate threats which may not be detected by automated tools (e.g., threat hunting).

#### **14.7 Cyber awareness is promoted and tested**

PRFIs should enable and encourage its employees, Board, members, and third parties to report suspicious cyber activity to Senior Management, or the appropriate authority designated by the PRFI. PRFIs should create awareness of cyber-attack scenarios directly targeting employees, members, and relevant third parties. In addition, the PRFI should regularly test its employees to assess their awareness of cyber threats and the effectiveness of their reporting processes and tools.

#### **14.8 Cyber risk profile is monitored and reported on**

PRFIs should maintain, and report on a current and comprehensive cyber security risk profile to facilitate oversight and timely decision-making. The profile should draw on existing internal and external risk identification and assessment sources, processes, tools, and capabilities. PRFIs should also ensure that processes and tools exist to measure, monitor, and aggregate residual risks.

## **DEFEND**

**Principle 15:** PRFIs should design, implement, and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets.

#### **15.1 Secure-by design practices are adopted**

PRFIs should adopt secure-by-design practices to safeguard its technology assets, in which security is considered and built into the system at every layer, where feasible. PRFIs should regularly review security use cases with a view to strengthen reliance on preventive versus detective.

#### **15.2 Strong and secure encryption technologies are employed**

PRFIs should implement and maintain strong encryption technologies to protect the authenticity, confidentiality, and integrity of its technology assets. This includes controls for the protection of encryption keys from unauthorised access and regularly assessing its cryptography standard and technologies to remain effective against current and emerging threats.

### **15.3 Enhanced controls and functionality are applied to protect critical and external facing technology assets**

PRFIs should employ enhanced controls and functionality to defend critical technology assets, contain cyber security threats, and remain resilient against cyber attacks. This includes giving consideration to:

- identifying cyber security controls required to secure its critical technology assets
- designing application controls to contain and limit the impact of a cyber attack
- implementing, monitoring, and reviewing appropriate security standards
- deploying additional layers of security controls, as appropriate.

### **15.4 Cyber security controls are layered**

PRFIs should implement and maintain multiple layers of cyber security controls and defend against cyber security threats at every stage of the attack life cycle (e.g., from reconnaissance and initial access to executing on objectives). PRFIs should also ensure resilience against current and emerging cyber threats by maintaining defence controls and tools.

### **15.5 Data protection and loss prevention security controls are implemented**

PRFIs should implement risk-based controls for the protection of its data throughout its life cycle. This includes data loss prevention capabilities and controls for data at rest, data in transit, and data in use.

### **15.6 Security vulnerabilities are remediated**

To ensure security vulnerabilities are well managed, PRFIs should:

- Maintain capabilities to ensure timely risk-based patching of vulnerabilities, in vendor software and internal applications, that considers the severity of the threat and vulnerability of the exposed systems.
- Apply patches at the earliest opportunity, commensurate with risk and in accordance with established timelines.
- Implement compensating controls as needed to sufficiently mitigate risks when remediation options are not available.
- Regularly monitor and report on patching status and vulnerability remediation against defined timelines, including any backlog and exceptions.

### **15.7 Identity and access management controls are implemented**

PRFIs should implement a risk-based identity and access controls, including Multi-Factor Authentication (MFA) and privileged access management. Where feasible, PRFIs should consider:

- Enforcing the principles of least privilege, conducting regular attestation of access and maintaining strong complex passwords to authenticate employee, member, and third-party access to technology assets.
- Implementing MFA across external-facing channels and privileged accounts (e.g., members, employees, and third parties).
- Managing privileged account credentials using a secure vault.
- Logging and monitoring account activity as part of continuous security monitoring.
- Ensuring system and service accounts are securely authenticated, managed, and monitored to detect unauthorized usage.
- Performing appropriate background checks (where feasible) on persons granted access to the PRFIs systems or data, commensurate with the criticality and classification of the technology assets.

### **15.8 Security configuration baselines are enforced, and deviations are managed**

PRFIs should implement approved security configuration baselines for technology assets and security defence tools, including those provided by third parties. Where possible, security configuration baselines for different defence layers should disable settings and access by default. PRFIs should define and implement processes to manage configuration deviations.

### **15.9 Application scanning and testing capabilities are employed**

PRFIs should establish application scanning and testing capabilities to ensure new, and/or changes to existing, systems and applications are assessed for vulnerabilities prior to release into the production environment.

### **15.10 Physical access controls and processes are applied**

PRFIs should define and implement physical access management controls and processes to protect network infrastructure and other technology assets from unauthorized access and environmental hazards.

## **DETECT**

**Principle 16:** PRFIs should design, implement, and maintain continuous security detection capabilities to enable monitoring, alerting, and forensic investigations.

### **16.1 Continuous, centralized security logging to support investigations**

PRFIs should ensure continuous security logging for technology assets and defence tools. Central tools for aggregating, correlating, and managing security event logs should enable timely log access during a cyber event investigation. For any significant cyber threat or incident, the PRFIs investigation, including any forensic investigation, should not be limited, or delayed by disaggregated, inaccessible or missing critical security event logs. PRFIs should implement minimum security log retention periods and maintain cyber security event logs to facilitate a thorough and unimpeded investigation of cyber security events.

### **16.2 Malicious and unauthorized activity is detected**

PRFIs should maintain security information to ensure continuous detection and alerting of malicious and unauthorized user and system activity. Where feasible, advanced behaviour-based detection and prevention methods should be used to detect user and entity behaviour anomalies, and emerging external and internal threats.

### **16.3 High risk cyber security alerts are prioritized**

PRFIs should define roles and responsibilities to allow for the escalation of high-risk cyber security alerts to rapidly contain and mitigate significant cyber threat events before they result in a material security incident or an operational disruption.

## **RESPOND, RECOVER, AND LEARN**

**Principal 17:** PRFIs should respond to, contain, recover, and learn from cyber security incidents impacting their technology assets, including incidents originating at third-party providers.

### **17.1 Incident response capabilities are integrated and aligned**

PRFIs should ensure the alignment and integration between their cyber security, technology, crisis management, and communication protocols. This should include capabilities to enable comprehensive and timely escalation and stakeholder coordination (internal and external) in response to a major cyber security event or incident.

### **17.2 Cyber incident classification is defined**

PRFIs should clearly define and implement a cyber incident taxonomy. This taxonomy should include specific cyber and information security incident classification, such as severity, category, type, and root cause. It should be designed to support the PRFI in responding to, managing, and reporting on cyber security incidents.

### **17.3 Cyber security incident management process and tools are maintained**

PRFIs should maintain a cyber security incident management process and playbooks to enable timely and effective management of cyber security incidents.

### **17.4 Timely response, containment, and recovery capabilities are established**

PRFIs should establish a cyber incident response team with tools and capabilities available on a continuous basis to rapidly respond, contain, and recover from cyber security events and incidents that could materially impact the PRFIs technology assets, members, and other stakeholders.

### **17.5 Forensic investigations and root cause analysis are conducted, as necessary**

PRFIs should collect, preserve, analyze, and present evidence on all security breaches where the PRFIs technology assets may have been materially impacted for the purpose of investigation and legal proceedings. For high-severity incidents, the PRFI should conduct a detailed post-incident assessment of direct and indirect impacts (financial and/or non-financial), including a root cause analysis to identify remediation actions, address the root cause and respond to lessons learned. The root cause analysis should assess threats, weaknesses and vulnerabilities in its people, processes, technology, and data.

## **VII. REPORTING OF TECHNOLOGY AND CYBER SECURITY INCIDENTS**

The following outlines the expectations for reporting incidents to the Corporation.

### **CRITERIA FOR REPORTING**

PRFIs are required to provide timely notification to the Corporation when technology and cyber security incidents relating to their operations occur. PRFIs should define priority, materiality, and severity levels within their incident management framework. The incidents reported to the Corporation should be those determined to be of high priority, materiality, and/or severity.

When in doubt about whether to report an incident, PRFIs should consult their Lead Supervisor.

A reportable incident may have **any one or more** of the following characteristics:

- Impact has potential consequences to other PRFIs or the Saskatchewan and by extension, the Canadian financial system.
- Impact to PRFI systems affecting financial market settlement, confirmations, or payments (e.g., Financial Market Infrastructure), or impact to payment services.
- Impact to PRFI operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity, or availability of member information.
- Disruptions to business systems and/or operations that have a material impact on PRFI, including but not limited to utility, data centre outages, loss or degradation of connectivity.
- Operational impact to key/critical systems, infrastructure, or data.
- Disaster recovery teams or plans have been activated or a disaster declaration has been made by a third-party vendor that impacts the PRFI.

- A PRFI's technology or cyber incident management team or protocols have been activated.
- Operational impact to internal users, and that poses an impact to external members or business operations.
- Number of external members impacted is growing; negative reputational impact is imminent (e.g., public and/or media disclosure).
- Impact to a third party affecting the PRFI.
- An incident that has been reported to the Board of Directors or Senior/Executive Management.
- A PRFI incident has been reported to:
  - The Office of the Privacy Commissioner of Canada
  - Another federal government department (e.g., the Canadian Center for Cyber Security)
  - Other regulatory organizations or agencies
  - Any law enforcement agencies
  - Has invoked internal or external counsel.
- A PRFI incident for which a cyber insurance claim has been initiated. This excludes incidents where the PRFI is notifying the underwriter for the purposes of sharing information.
- Technology or cyber security incidents that breach internal risk appetite or thresholds.
- For incidents that do not align with or contain the specific criteria listed above, or when a PRFI is uncertain, notification to the Corporation is encouraged as a precaution.

## **INITIAL NOTIFICATION REQUIREMENTS**

PRFIs must report a technology or cyber security incident to the Corporation within 24 hours. The Technology and Cyber Security Incident Reporting Form is to be submitted through the Regulatory Reporting Submission Portal, found on the Corporation's Intranet. In the event the PRFI does not have access to the Corporation's Intranet during an incident, the form can be submitted directly to the Lead Supervisor.

Where specific details are unavailable at the time of the initial report, the PRFI must indicate information not yet available. In such cases, the PRFI must provide best estimates and all other details available at the time including their expectations of when additional information will be available.

## **SUBSEQUENT REPORTING REQUIREMENTS**

The Corporation expects PRFIs to provide regular updates (e.g., daily, weekly) as new information becomes available, and until all details about the incident have been provided.

Depending on the severity, impact, and velocity of the incident, the Corporation may request that a PRFI change the method and frequency of subsequent updates.

Until the incident is contained/resolved, the Corporation expects PRFIs to provide situation updates, including any short-term and long-term remediation actions and plans.

Following incident containment, recovery, and closure, the PRFI should report to the Corporation on its post-incident review and lessons learned.

## **FAILURE TO REPORT**

Failure to report incidents as outlined above may result in increased supervisory oversight or other steps as determined by the Corporation.

## APPENDIX A – EXAMPLES OF REPORTABLE INCIDENTS

Scenario Name	Scenario Description	Impact
Cyber Attack	Account takeover botnet campaign is targeting online services using new techniques, current defenses are failing to prevent member account compromise	<p>High volume and velocity of attempts</p> <p>Current controls are failing to block attack</p> <p>Members are locked out</p> <p>Indication that member account(s) or information has been compromised</p>
Service Availability & Recovery	Technology failure at data center	<p>Critical online service is down, and alternate recovery option failed</p> <p>Extended disruption to critical business systems and operations</p>
Third-Party Breach	A material third party is breached, PRFI is notified that third party is investigating	<p>Third party is designated as material to the PRFI</p> <p>Impact to PRFI data is possible</p>
Extortion Threat	PRFI has received an extortion message threatening to perpetrate a cyber attack (e.g., DDoS for Bitcoin)	<p>Threat is credible</p> <p>Probability of critical online service disruption</p>

## APPENDIX B –TECHNOLOGY AND CYBER INCIDENT REPORTING FORM

<b>CUDGC Technology and Cyber Incident Report Form</b>	
<b>1. Contact Information</b>	
Name of Institution:	
Key Contact's Name:	Key Contact's Position:
Key Contact's Email:	Key Contact's Phone Number:
<b>2. Incident Information</b>	
Incident Name or Identifier:	
Date and Time Discovered/Detected:	Date and Time Occurred:
Name of Business Line (s) or Function (s) Affected:	
Technology Asset (s) Affected:	
Site/Location Affected:	
<b>3. Description of Risk and Incident</b>	
Incident Category	Where did the Incident Occur?
<input type="checkbox"/> Technology <input type="checkbox"/> Cyber <input type="checkbox"/> Other (specify below)	<input type="checkbox"/> Within your institution <input type="checkbox"/> Third Party <input type="checkbox"/> Supply Chain <input type="checkbox"/> Other (specify below)
If other, please specify:	If other, please specify:
Provide the Incident Type	<input type="checkbox"/> Technology asset* outage <input type="checkbox"/> Malware - Other <input type="checkbox"/> Technology asset* degradation/delay <input type="checkbox"/> Malware Campaign <input type="checkbox"/> ABM Jackpotting <input type="checkbox"/> Online Extortion

	<input type="checkbox"/> Account take-over <input type="checkbox"/> Distributed Denial of Service (DDoS) <input type="checkbox"/> Data breach/leak <input type="checkbox"/> Insider Threat <input type="checkbox"/> Cyber Crime  * A "technology asset" is something tangible (e.g., hardware, infrastructure) or intangible (e.g., software/application, data, information) that needs protection and supports the provision of technology services	<input type="checkbox"/> Phishing <input type="checkbox"/> Ransomware <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Loss/theft of equipment <input type="checkbox"/> Other (specify below)
If other, please specify:		
Provide additional details below including current state, known direct and indirect impacts, actions completed and pending, with estimated timelines to address the remediation of the incident:		
Add description of root cause, if known:		
<b>4. Sensitivity of Data/ Information Involved</b>		
Provide description of sensitive information compromised or at risk. If no sensitive information is at risk, please indicate N/A:		

Provide details on the tactics, techniques and procedures involved in the incident:	Provide the indicators of compromise:
<b>5. Internal and External Notifications</b>	
Are members of your institution aware of the incident?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has Senior Management been notified?  Date and time Senior Management was notified (if applicable):	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has the Board of Directors been notified?  Date and time Board of Directors was notified (if applicable):	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have other regulators or supervisory agencies been notified?  Name of notified regulatory or supervisory agencies and the date/ time they were notified (if applicable):	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have any law enforcement agencies been notified?  Name of notified law enforcement agencies:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have any cyber insurance providers been notified?  Name of cyber insurance providers used:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has a cyber and/ or insurance policy claim been initiated?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has a breach coach been engaged?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has internal or external legal counsel been engaged?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has an external forensics firm been engaged?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Please provide any additional information that you believe may be important but has not been provided elsewhere:	