# Guideline

| | |
|---|---|
| **Title** | Technology and Cyber Risk Management |
| **Category** | Sound Business and Financial Practices |
| **Date** | July 31, 2022 |
| **Sector** | Banks<br>Foreign Bank Branches<br>Foreign Insurance Branches<br>Life Insurance and Fraternal Companies<br>Property and Casualty Companies<br>Trust and Loan Companies |
| **No** | B-13 |

## Table of Contents


A. Purpose and scope

- A.1 Definitions[2]
- A.2 Structure
- A.3 Outcomes
- A.4 Related guidance and information

1. Governance and risk management

- 1.1 Accountability and organizational structure
- 1.2 Technology and cyber strategy
- 1.3 Technology and cyber risk management framework

2. Technology operations and resilience

- 2.1 Technology architecture
- 2.2 Technology asset management

- 2.3 Technology project management
- 2.4 System Development Life Cycle
- 2.5 Change and release management
- 2.6 Patch management
- 2.7 Incident and problem management
- 2.8 Technology service measurement and monitoring
- 2.9 Disaster recovery

3. Cyber security

- 3.0 Confidentiality, integrity and availability of technology assets is maintained
- 3.1 Identify
- 3.2 Defend
- 3.3 Detect
- 3.4 Respond, recover and learn


## A. Purpose and scope

This Guideline establishes OSFI's expectations related to technology and cyber risk management. It is applicable to all federally regulated financial institutions (FRFIs), including foreign bank branches and foreign insurance company branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada.[1] Expectations for branches are set out in Guideline E-4 on Foreign Entities Operating in Canada on a Branch Basis. These expectations aim to support FRFIs in developing greater resilience to technology and cyber risks.

> There is no one-size-fits-all approach for managing technology and cyber risks given the unique risks and vulnerabilities that vary with a FRFIs' size, the nature, scope, and complexity of its operations, and risk profile. This

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

## A.1 Definitions[2]

"Technology risk", which includes "cyber risk", refers to the risk arising from the inadequacy, disruption, destruction, failure, damage from unauthorised 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.

A "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" is broadly used in this Guideline to include "information technology" (IT), and "cyber" is broadly used to include "information security."

## A.2 Structure

This Guideline is organized into three domains. Each sets out key components of sound technology and cyber risk management.

1. **Governance and risk management** – Sets OSFI's expectations for the formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security.
2. **Technology operations and resilience** – Sets OSFI's expectations for management and oversight of risks related to the design, implementation, management and recovery of technology assets and services.
3. **Cyber security** – Sets OSFI's expectations for management and oversight of cyber risk.

## A.3 Outcomes

Each domain has a desired outcome for FRFIs to achieve through managing risks that contribute to developing FRFIs' resilience to technology and cyber risks.

1. Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks.
2. 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.
3. A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets.

### A.4 Related guidance and information

Technology and cyber risks are dynamic and intersect with other risk areas. FRFIs should read this Guideline in conjunction with other OSFI guidance, tools and supervisory communications, as well as guidance issued by other authorities applicable to the FRFI's operating environment; in particular:

- OSFI Corporate Governance Guideline;
- OSFI Guideline E-21 (Operational Risk Management);
- OSFI Guideline B-10 (Outsourcing);
- OSFI Cyber Security Self-Assessment Tool;
- OSFI Technology and Cyber Security Incident Reporting Advisory;
- Alerts, advisories and other communications issued by the Canadian Centre for Cyber Security; and
- Recognized frameworks and standards for technology operations and information security.

## 1. Governance and risk management

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

## 1.1 Accountability and organizational structure

**Principle 1:** Senior Management should assign responsibility for managing technology and cyber risks to senior officers. It should also ensure an appropriate organizational structure and adequate resourcing are in place for managing technology and cyber risks across the FRFI.

### 1.1.1 Senior Management accountability is established

Senior Management is accountable for directing the FRFI's technology and cyber security operations and should assign clear responsibility for technology and cyber risk governance to senior officers. Examples of such roles include: Head of Information Technology; Chief Technology Officer (CTO); Chief Information Officer (CIO); Head of Cyber Security or Chief Information Security Officer (CISO). These roles should have appropriate stature and visibility throughout the institution.

### 1.1.2 Appropriate structure, resources and training are provided

FRFIs 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; and
- Promote a culture of risk awareness in relation to technology and cyber risks throughout the institution.

Please refer to OSFI's Corporate Governance Guideline for OSFI's expectations of FRFI Boards of Directors regarding business strategy, risk appetite and operational, business, risk and crisis management policies.

## 1.2 Technology and cyber strategy

**Principle 2:** FRFIs 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 FRFI's technology and cyber environment.

### 1.2.1 Strategy is proactive, comprehensive and measurable

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

- Anticipate and evolve with potential changes in the FRFI's internal and external technology and cyber environment;
- Reference planned changes in the FRFI'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; and
- Articulate how technology and cyber security operations will support the overall business strategy.

## 1.3 Technology and cyber risk management framework

**Principle 3:** FRFIs 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 FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.

### 1.3.1 RMF is well-aligned and continuously improved

FRFIs should establish a framework for managing technology and cyber risks in alignment with its enterprise risk management framework. FRFIs 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).

### 1.3.2 RMF captures key elements

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

- Accountability for technology and cyber risk management, including for relevant Oversight Functions;
- Technology and cyber risk appetite and measurement (e.g., limits, thresholds and tolerance levels);
- A technology and cyber risk taxonomy;
- Control domains for technology and cyber security;
- 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; and
- Reporting to Senior Management on technology and cyber risk appetite measures, exposures and trends to inform the FRFI's current and emerging risk profile.

Please refer to OSFI's Corporate Governance Guideline for OSFI's expectations in relation to FRFI Oversight Functions, which include Risk Management, Compliance, and Internal Audit.

## 2. Technology operations and resilience

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

### 2.1 Technology architecture

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

### 2.1.1 Architecture framework ensures technology supports business needs

FRFIs 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.

### 2.1.2 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, systems and associated infrastructure should be designed and implemented to achieve availability, scalability, security (Secure-by-Design) and resilience (Resilience-by-Design), commensurate with business needs.

## 2.2 Technology asset management

**Principle 5:** FRFIs should maintain an updated inventory of all technology assets supporting business processes or functions. FRFI's 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 currency.

### 2.2.1 Technology asset management standards are established

FRFIs should establish standards and procedures to manage technology assets.

### 2.2.2 Inventory is maintained and assets are categorized

FRFIs should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle. Based on the FRFI's risk tolerance, this may include assets owned or leased by a FRFI, and third-party assets that store or process FRFI information or provide critical business services. The asset management system, or inventory, 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 FRFI, or which could attract threat actors and cyber attacks, and therefore require enhanced cyber protections; and
- Documented interdependencies between critical technology assets, where appropriate, to enable proper change and configuration management processes, and to assist in response to security and operational incidents, including cyber attacks.

### 2.2.3 Inventory records and manages technology asset configurations

The technology inventory should also include a system for recording and managing asset configurations to enhance visibility and mitigate the risk of technology outages and unauthorized activity. Processes should be in place to identify, assess, and remediate discrepancies from the approved baseline configuration, and to report on breaches.

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

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

### 2.2.5 Technology currency is continuously assessed and managed

FRFIs should continuously monitor the currency of 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.

## 2.3 Technology project management

**Principle 6:** 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 FRFI's risk appetite.

### 2.3.1 Technology projects are governed by an enterprise-wide framework

Technology projects are often distinguished by their scale, required investment and importance in fulfilling the FRFI's broader strategy. As a result, they should be governed by an enterprise-wide project management framework that provides for consistent approaches and achievement of project outcomes in support of the FRFI's technology strategy. The FRFI should measure, monitor and periodically report on project performance and associated risks.

## 2.4 System Development Life Cycle

**Principle 7:** FRFIs 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.

### 2.4.1 SDLC framework guides system and software development

The SDLC framework should outline processes and controls in each phase of the SDLC life cycle to achieve security and functionality, while ensuring systems and software perform as expected to support business objectives.[3] The SDLC framework can include software development methodologies adopted by the FRFI (e.g., Agile, Waterfall).

### 2.4.2 Security requirements are embedded throughout the SDLC

In addition to the general technology processes and controls, FRFIs should establish control gates to ensure that security requirements and expectations are embedded in each phase of the SDLC. For Agile software development methods, FRFIs should continue to incorporate the necessary SDLC and security-by-design principles throughout its Agile process.

### 2.4.3 Integration of development, security and technology operations

By integrating application security controls and requirements into software development and technology operations, new software and services can be delivered rapidly without compromising application security. When these practices[4] are employed, FRFIs should ensure they are aligned with the SDLC framework and applicable

technology and cyber policies and standards.

### 2.4.4 Acquired systems and software are assessed for risk

For software and systems that are acquired, FRFIs should ensure that security risk assessments are conducted, and that systems implementation is subject to the control requirements as required by the FRFI's SDLC framework.

### 2.4.5 Coding principles provide for secure and stable code

FRFIs should define and implement coding principles and best practices (e.g., secure coding, use of third-party and open-source code, coding repositories and tools, etc.).

## 2.5 Change and release management

**Principle 8:** FRFIs 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.

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

FRFIs 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 outline the key controls required throughout the change management process. The standard should also define emergency change and control requirements to ensure that such changes are implemented in a controlled manner with adequate safeguards.

### 2.5.2 Segregation of duties controls against unauthorized changes

Segregation of duties is a key control used in protecting assets from unauthorized changes. FRFIs 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.

### 2.5.3 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.

## 2.6 Patch management

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

### 2.6.1 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 FRFI's existing change management processes, including emergency change processes. Patches should be tested before deployment to the production environment.

## 2.7 Incident and problem management

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

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

FRFIs 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.

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

FRFIs should implement processes and procedures for managing technology incidents; elements may 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) that are informed by ongoing threat assessment and risk surveillance activities;
- 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;
- Conducting periodic exercises and testing of incident management process, playbooks, and other response tools (e.g., coordination and communication) to validate and maintain their effectiveness; and
- Establishing and periodically testing incident management processes with third parties.

### 2.7.3 Processes are established to investigate, resolve and learn from problems

FRFIs should develop problem management processes that provide for the detection, categorization, investigation and resolution of suspected incident cause(s). Processes should include post-incident reviews, root cause and impact diagnostics and identification of trends or patterns in incidents. Problem management activities and findings should inform related control processes and be used on an ongoing basis to improve incident management processes and procedures, including change and release management.

## 2.8 Technology service measurement and monitoring

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

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

FRFIs 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.

### 2.8.2 Technology infrastructure performance and capacity are sufficient

FRFIs 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.

## 2.9 Disaster recovery

**Principle 12:** FRFIs should establish and maintain an Enterprise Disaster Recovery Program (EDRP) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

### 2.9.1 Disaster recovery program is established

FRFIs should develop, implement and maintain an EDRP that sets out their approach to recovering technology services during a disruption. FRFIs should align the disaster recovery program with its business continuity management program. The EDRP should establish:

- 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 FRFI's 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 FRFI; and,
- A policy or standard with controls for data back-up and recovery processes, requirements for data storage and periodic testing.

### 2.9.2 Key dependencies are managed

FRFIs should manage key dependencies required to support the EDRP, such as:

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

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

### 2.9.3 Disaster recovery scenarios are tested

To promote learning, continuous improvement and technology resilience, FRFIs 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; and,
- Previous incident history and known technology complexities or weaknesses.

FRFIs' disaster recovery scenarios should test:

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

## 3. Cyber security

**Outcome:** A secure technology posture that maintains the confidentiality, integrity and availability of FRFIs' technology assets.

## 3.0 Confidentiality, integrity and availability of technology assets is maintained

FRFIs should proactively identify, defend, detect, respond and recover from external and insider cyber security threats, events and incidents to maintain the confidentiality, integrity and availability of its technology assets.

## 3.1 Identify

**Principle 14:** FRFIs 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.

### 3.1.1 Security risks are identified

FRFIs 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.

### 3.1.2 Intelligence-led threat assessment and testing is conducted

FRFIs should adopt a risk-based approach to threat assessment and testing. FRFIs should set defined triggers, and minimum frequencies, for intelligence-led threat assessments to test cyber security processes and controls. FRFIs should also regularly perform tests and exercises, to identify vulnerabilities or control gaps in its cyber security programs (e.g., penetration testing and red teaming) using an intelligence-led approach. The scope and potential impacts of such testing should be clearly defined by the FRFI with effective risk mitigation controls applied throughout the assessment to manage any associated inherent risks.

### 3.1.3 Vulnerabilities are identified, assessed and ranked

FRFIs should establish processes to conduct regular vulnerability assessments of its technology assets, including but not limited to network devices, systems and applications. Processes should articulate the frequency with which vulnerability scans and assessments are conducted. FRFIs should assess and rank relevant cyber vulnerabilities and threats according to the severity of the threat and risk exposure to technology assets using a standard risk

measurement methodology. In doing so, FRFIs should consider the potential cumulative impact of vulnerabilities, irrespective of risk level, that could present a high-risk exposure when combined.

### 3.1.4 Data are identified, classified and protected

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

### 3.1.5 Continuous situational awareness and information sharing are maintained

FRFIs should maintain continuous situational awareness of the external cyber threat landscape and its threat environment as it applies to its technology assets. This could include participating in industry threat intelligence and information sharing forums and subscribing to timely and reputable threat information sources. Where feasible, FRFIs are encouraged to provide timely exchange of threat intelligence to facilitate prevention of cyber attacks, thereby contributing to its own cyber resilience and that of the broader financial sector.

### 3.1.6 Threat modelling and hunting are conducted

Where feasible, FRFIs 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. FRFIs should use manual techniques to proactively identify and isolate threats which may not be detected by automated tools (e.g., threat hunting).

### 3.1.7 Cyber awareness is promoted and tested

FRFIs should enable and encourage its employees, customers and third parties to report suspicious cyber activity, recognizing the role that each can play in preventing cyber attacks. FRFIs should create awareness of cyber attack scenarios directly targeting employees, customers and relevant third parties. In addition, the FRFI should regularly test its employees to assess their awareness of cyber threats and the effectiveness of their reporting processes and tools.

### 3.1.8 Cyber risk profile is monitored and reported on

FRFIs 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. FRFIs should also ensure that processes and tools exist to measure, monitor and aggregate residual risks.

## 3.2 Defend

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

### 3.2.1 Secure-by-design practices are adopted

FRFIs should adopt secure-by-design practices to safeguard its technology assets. Security defence controls should aim to be preventive, where feasible, and FRFIs should regularly review security use cases with a view to strengthen reliance on preventive versus detective controls. Standard security controls should be applied end-to-end, starting at the design stage, to applications, micro-services and application programming interfaces developed by the FRFI.

### 3.2.2 Strong and secure cryptographic technologies are employed

FRFIs should implement and maintain strong cryptographic technologies to protect the authenticity, confidentiality and integrity of its technology assets. This includes controls for the protection of encryption keys from unauthorised access, usage and disclosure throughout the cryptographic key management life cycle. FRFIs should regularly assess its cryptography standard and technologies to remain effective against current and emerging threats.

### 3.2.3 Enhanced controls and functionality are applied to protect critical and external-facing technology assets

FRFIs should employ enhanced controls and functionality to rapidly contain cyber security threats, defend its critical technology assets and remain resilient against cyber attacks by considering the following:

- 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, configuration baselines and security hardening requirements; and
- Deploying additional layers of security controls, as appropriate, to defend against cyber attacks (e.g., volumetric, low/slow network and application business logic attacks).

### 3.2.4 Cyber security controls are layered

FRFIs 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). FRFIs should also ensure resilience against current and emerging cyber threats by maintaining defence controls and tools. This includes ensuring continuous operational effectiveness of controls by minimizing false positives. Where feasible, FRFIs should:

- Protect networks, including external-facing services, from threats by minimizing its attack surface;
- Define authorized logical network zones and apply controls to segregate and limit, or block access and traffic to and from network zones;
- Leverage a combination of allow/deny lists, including file integrity checks (e.g., file hash/signature) and indicators of compromise, in addition to advanced behaviour-based protection capabilities that are continuously updated; and
- Apply defence controls and capabilities for intrusion prevention and detection on its network perimeter in addition to controls for data loss, malware and viruses.

### 3.2.5 Data protection and loss prevention security controls are implemented

Starting with clear information classification of its data, FRFIs should design and 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.

### 3.2.6 Security vulnerabilities are remediated

To ensure security vulnerabilities are well managed, FRFIs 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 (e.g., "zero-day" attacks); and
- Regularly monitor and report on patching status and vulnerability remediation against defined timelines, including any backlog and exceptions.

### 3.2.7 Identity and access management controls are implemented

FRFIs should implement risk-based identity and access controls, including Multi-Factor Authentication (MFA)[5] and privileged access management. Where feasible, FRFIs should consider:

- Enforcing the principles of least privilege, conducting regular attestation of access and maintaining strong complex passwords to authenticate employee, customer and third-party access to technology assets;
- Implementing MFA across external-facing channels and privileged accounts (e.g., customers, 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; and
- Performing appropriate background checks (where feasible) on persons granted access to the FRFI's systems or data, commensurate with the criticality and classification of the technology assets.

### 3.2.8 Security configuration baselines are enforced and deviations are managed

FRFIs should implement approved, risk-based 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. FRFIs should define and implement processes to manage configuration deviations.

### 3.2.9 Application scanning and testing capabilities are employed

Where feasible, static and/or dynamic scanning and testing capabilities should be used to ensure new, and/or changes to existing, systems and applications are assessed for vulnerabilities prior to release into the production environment. Security controls should also be implemented to maintain security when development and operations practices are combined through a continuous and automated development pipeline (see paragraph 2.4.2).

### 3.2.10 Physical access controls and processes are applied

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

## 3.3 Detect

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

### 3.3.1 Continuous, centralized security logging to support investigations

FRFIs should ensure continuous security logging for technology assets and different layers of 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 FRFI's forensic investigation should not be limited or delayed by disaggregated, inaccessible or missing critical security event logs. FRFIs should implement minimum security log retention periods and maintain cyber security event logs to facilitate a thorough and

unimpeded forensic investigation of cyber security events.

### 3.3.2 Malicious and unauthorized activity is detected

FRFIs should maintain security information and event management capabilities 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. The latest threat intelligence and indicators of compromise should be used to continuously enhance FRFI monitoring tools.

### 3.3.3 Cyber security alerts are triaged

FRFIs should define roles and responsibilities to allow for the triage 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.

## 3.4 Respond, recover and learn

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

### 3.4.1 Incident response capabilities are integrated and aligned

Domain 2 sets out the foundational expectations for FRFIs' incident and problem management capabilities. FRFIs 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.

### 3.4.2 Cyber incident taxonomy is defined

FRFIs 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 FRFI in responding to, managing and reporting on cyber security incidents.

### 3.4.3 Cyber security incident management process and tools are maintained

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

### 3.4.4 Timely response, containment and recovery capabilities are established

FRFIs 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 FRFI's technology assets, customers and other stakeholders.

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

FRFIs should conduct a forensic investigation for incidents where technology assets may have been materially exposed. For high-severity incidents, the FRFI 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.

## Footnotes

1 Foreign bank branches refers to foreign banks authorized to conduct business in Canada on a branch basis under Part XII.1 of the *Bank Act*. Foreign insurance company branches refers to foreign entities that are authorized to insure in Canada risks on a branch basis under Part XIII of the *Insurance Companies Act*.

2 Informed by definitions used by recognized standard-setting bodies. For technical terms used throughout this Guideline, FRFIs may employ definitions published by recognized standard-setting bodies.

3 System Development Life Cycle (SDLC) is the overall process of developing, implementing and retiring information systems through a multistep process from initiation, analysis, design, implementation and maintenance to disposal (NIST Special Publication 800-100). Software development methodologies (e.g., Agile, Waterfall) focus on a specific component of system development, whereas SDLC is a more holistic process for the end-to-end life cycle of a system.

4 These practices are commonly referred to as DevSecOps.

5 MFA uses independent authentication factors which generally include something that the user: a) **knows**, such as a password or a PIN; b) **has** (possesses), such as a cryptographic identification device or token; and/or, c) **is**, such as biometrics or behaviour.