Guideline

Subject: Technology and Cyber Risk Management

Category: Sound Business Practices and Prudential Limits

No: B-13 **Date: November 2021**

A. Purpose and Scope

This Guideline establishes OSFI's expectations related to technology and cyber risk management and applies to all federally regulated financial institutions (FRFIs). These expectations aim to support FRFIs in developing greater resilience to technology and cyber risks.

FRFIs should implement the expectations in this Guideline commensurate with its size; the nature, scope and complexity of its operations; and risk profile. OSFI's expectations are technology-neutral, anticipating the need for FRFIs to compete effectively and take full advantage of digital innovation while maintaining a sound technology posture.

A.1 Definitions

"Technology risk" refers to the risk arising from the inadequacy, disruption, failure, loss or malicious use of information technology systems, infrastructure, people or processes that enable and support business needs and can result in financial loss.

"Cyber risk" or "cyber security risk" is the risk of financial loss, operational disruption or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification or destruction of an institution's information technology systems and/or the data contained therein.

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.

For the purpose of this Guideline, "technology" refers to "information technology" (IT). The term "cyber" also refers to "information security." FRFIs may maintain their own definitions or employ definitions published by recognized standard-setting bodies.

A.2 Structure

A.2.1 This Guideline is organized into five 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.

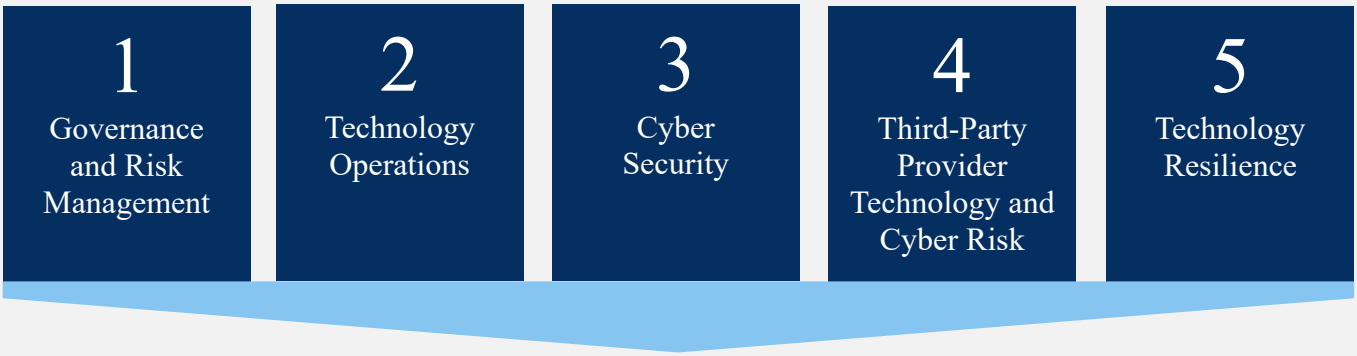
2. ***Technology Operations*** – Sets OSFI's expectations for management and oversight of risks related to the design, implementation and management of technology assets and services.

3. ***Cyber Security*** – Sets OSFI's expectations for management and oversight of cyber risk.

4. ***Third-Party Provider Technology and Cyber Risk*** – Expanding on OSFI's existing guidance for outsourcing and third-party risk, sets expectations for FRFIs that engage with third-party providers to obtain technology and cyber services and/or other services that give rise to cyber and/or technology risk.

5. ***Technology Resilience*** – Sets OSFI's expectations for capabilities to deliver technology services through operational disruption.

Domains for the sound management of technology and cyber risk



Greater resilience to technology and cyber risks

A.3 Outcomes

A.3.1 The five domains in this Guideline each express a desired outcome for FRFIs to achieve through managing risk. In turn, these outcomes 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 processes.
3. A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets.
4. Reliable and secure technology and cyber operations from third-party providers.
5. Technology services are delivered, as expected, through disruption.

A.4 Related Guidance and Information

A.4.1 Technology and cyber security best practices are dynamic. Technology and cyber risks also intersect with other risk areas. As such, FRFIs are advised to 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 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.

Table of Contents

Page

1. Technology and Cyber 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. Such roles may comprise: 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.*** OSFI expects the FRFI to:

- 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 in regard to business strategy, risk appetite and operational, business, risk and crisis management policies.

1.2 Technology and Cyber Strategy

Principle 2: The FRFI should define, document, approve and implement a strategic technology and cyber plan(s). The plan(s) should align to the FRFI's 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.*** The FRFI's strategic technology and cyber plan(s) should, at a minimum:

- 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;
- Be accompanied by tools and processes that support enterprise-wide strategy implementation; and,
- Articulate the manner in which technology and cyber security operations will support the overall business strategy.

1.3 Technology and Cyber Risk Management Framework

Principle 3: The FRFI 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 what processes and requirements the FRFI utilizes to identify, assess, manage, monitor and report on technology and cyber risks.

1.3.1 ***RMF is well-aligned and continuously improved.*** The FRFI should establish a framework for managing technology and cyber risks, aligned with its enterprise risk management framework. OSFI expects the FRFI to 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.*** At a minimum, the technology and cyber RMF should establish and govern the following elements of risk management:

- 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 all domains of 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 adoption of less proven 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

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

2.1 Technology Architecture

Principle 4: The FRFI 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.*** The FRFI 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, considering such assets as: infrastructure; applications; emerging or less proven technologies; and relevant data. Systems and associated infrastructure should be designed and implemented to achieve availability, scalability, security (Secure-by-Design) and resilience (Resilience-by-Design). Resilience-by-Design requires consideration of the end-to-end flow of the business services or functions that they support, and associated internal and external dependencies. Architecture principles and controls should be embedded in the design phase of the System Development Life Cycle, prior to implementation.

2.2 Technology Asset Management

Principle 5: The FRFI should maintain an updated inventory of all technology assets supporting business processes or functions. The FRFI's asset management process 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 assets are managed according to established requirements based on their criticality.*** The FRFI should establish standards and procedures to manage technology assets according to their criticality and classification.

2.2.2 ***Asset inventory identifies and classifies technology assets.*** The FRFI should maintain a current and comprehensive asset management system, or inventory, that catalogues technology assets throughout their life cycle. The FRFI should implement processes to categorize technology assets based on criticality to the business and assign a security classification based on its sensitivity. This categorization should also identify critical technology assets that are

considered of high value to the FRFI, could attract threat actors and cyber attacks and therefore require enhanced cyber protections. The asset inventory should be sufficiently detailed to enable the prompt identification of an asset, its location, classification and ownership. Interdependencies between assets should be documented 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 captures all technology assets that support the business.*** A comprehensive inventory, and related processes, should capture both corporate assets and non-corporate assets that interface with the FRFI's technology infrastructure in supporting business services or functions. Such categories include:

- Assets owned, leased by, or otherwise entrusted to the FRFI;
- Assets owned by FRFI employees that are used in the course of business (e.g., assets authorized under "bring your own device" policies);
- Assets owned by third parties that are used to provide services to the FRFI; and,
- Assets owned by non-employees, including contractors and consultants that are used to provide services to the FRFI.

2.2.4 ***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. The system should record asset configuration attributes, including baseline configurations, and any subsequent, authorized changes. Processes should be in place to identify, assess and remediate discrepancies from the approved baseline configuration and report on breaches.

2.2.5 ***Safe disposal of technology assets is provided for.*** The FRFI should define standards and implement processes to ensure the secure disposal or destruction of assets at the end of their life cycle.

2.2.6 ***Technology currency is continuously assessed and managed.*** The FRFI 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 and required investment, and their 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. Project performance and associated risks should be measured, monitored and periodically reported on an individual and portfolio basis. Project risk appetite and measures are informed by the FRFI's technology and cyber RMF.

2.4 System Development Life Cycle

Principle 7: The FRFI 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 control activities and processes in each phase of the life cycle to achieve security, functionality and ensure that systems and software perform as expected in order to support business objectives. The SDLC phases generally comprise:

- Planning and defining requirements;
- Design, coding and implementation;
- Testing and acceptance; and,
- Deployment, maintenance and decommissioning.

2.4.2 ***Security requirements are embedded throughout the SDLC.*** In addition to the general technology processes and controls, the FRFI should establish control gates to ensure that security requirements and expectations are embedded in each phase of the SDLC. Sound security requirements and controls include, but are not limited to:

- Peer code reviews;
- Security scanning of code;
- Privileged access management and key management;
- Protection of data integrity and confidentiality;
- Removal of unnecessary services and programs;
- Authentication and authorization; and,
- Security logging and monitoring.

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[1] are employed, the FRFI 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, the FRFI should ensure that security risk assessments are conducted and that systems implementation is subject to the same control requirements as required by the FRFI's SDLC framework to obtain assurance on quality, performance and security controls.

[1] These practices are commonly referred to as DevSecOps.

2.4.5 ***Coding standards provide for secure and stable code.*** The FRFI should define and implement coding standards, which at a minimum should cover controls and practices surrounding:

- Secure coding;
- Use of third-party and open-source code, coding repositories and tools;
- Testing requirements;
- Timely remediation of bugs and vulnerabilities prior to production deployment; and
- Continuous education for internal developers, if applicable.

2.5 Change and Release Management

Principle 8: The FRFI should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are documented, assessed, tested, approved, implemented and verified 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.*** The FRFI 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 for all phases of 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 and should be exercised in the change management process to ensure that the same person cannot develop, 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: The FRFI 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 existing FRFI change management processes, including emergency change processes. All patches should be tested before deployment to the production environment.

2.7 Incident and Problem Management

Principle 10: THE FRFI 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.*** The FRFI should define standards and implement processes for incident and problem management. Standards should have the overall objective of timely identification and escalation of incidents, restoration and/or recovery of an affected system, and investigation and resolution of incident root causes, and provide an appropriate governance structure. The FRFI's incident management standards should complement its Enterprise Disaster Recovery Framework and contribute to its technology resilience (see Domain 5).

2.7.2 ***Incident management process is clear, responsive and risk-based.*** OSFI expects the FRFI to 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 and 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 technology 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 (e.g., deficiencies in internal and external resources, available skill sets, third-party services and support required); and,
- Establishing and periodically testing incident management processes (e.g., crisis communications) with third-party providers.

2.7.3 ***Problems are investigated, resolved and learned from.*** The FRFI should develop problem management processes that provide for the detection, categorization, investigation and resolution of suspected cause(s) of incidents. Processes should include post-incident reviews, root cause and impact diagnostics, and support identification of trends or patterns in incidents. Problem management activities and findings should inform related control processes, including change and release management, and be used to continuously improve incident management processes and procedures.

2.8 Technology Service Measurement and Monitoring

Principle 11: The FRFI 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.*** The FRFI should establish technology service management standards with defined performance indicators and service targets that can be used to measure and monitor the delivery of technology services. Processes should also provide for prompt remediation where targets are not being met. Services governed by these standards may include:

- Service desk;
- Incident and problem resolution;
- Service maintenance;
- Change management; and,
- Operations and network management.

2.8.2 ***Technology infrastructure performance and capacity are sufficient.*** The FRFI 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.

3. Cyber Security

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

3.0 ***Confidentiality, integrity and availability of technology assets is maintained***. The FRFI 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 12: The FRFI 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.*** The FRFI should identify current or emerging cyber threats proactively using threat assessments to evaluate threats and assess security risk. This should include cyber security risk in new business initiatives, technology projects and change management processes. The FRFI should assess and understand both the inherent and residual

security risks, after compensating controls are applied, to its critical technology assets. This includes implementing information and cyber security threat assessments, processes and tools to cover controls at different layers of defence.

3.1.2 ***Intelligence-led threat assessment and testing is conducted.*** The FRFI should adopt a risk-based approach to threat assessment and testing. The FRFI should set defined triggers, and minimum frequencies, for intelligence-led threat assessments to test cyber security processes and controls. In addition, the FRFI should use a cyber threat intelligence-led approach and regularly perform tests and exercises to identify vulnerabilities or control gaps in its cyber security programs (e.g., penetration testing and red teaming). The FRFI should also clearly define the scope and potential impacts of such testing and apply effective risk mitigation controls throughout the assessment to manage any associated potential inherent risks.

3.1.3 ***Vulnerabilities are identified, assessed and ranked.*** The FRFI 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. The FRFI 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, the FRFI 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.*** The FRFI should ensure that adequate controls are in place to identify, classify and protect structured and unstructured data, authorized and unauthorized data sources and environments, based on their confidentiality classification. The FRFI 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.*** The FRFI 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 which furnish information on areas such as: emerging threats, attack techniques, vulnerabilities and indicators of compromise. Cyber threat intelligence sharing should include relevant domestic and international authorities. The FRFI should ensure 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.*** The FRFI 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. The FRFI 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.*** The FRFI 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. The FRFI should create awareness of cyber attack vectors and techniques 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.*** The FRFI should maintain 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. The FRFI should also ensure that processes and tools exist to measure, monitor and aggregate residual risks. Additionally, the FRFI should report on the cyber security risk profile using relevant dimensions (e.g., business unit, function and geographic region).

3.2 Defend

Principle 13: The FRFI 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.*** The FRFI should adopt Secure-by-Design practices in all aspects of technology and data management, innovation and operations to safeguard its technology assets. Security defence controls should aim to be preventive and the FRFI should regularly review security use cases with a view to greater reliance on preventive versus detective controls. The FRFI should also define and implement a risk-based and timely process to ensure detection controls are changed into prevention controls. The FRFI should apply security defence controls to all technology assets. Standard security controls should be applied end-to-end, starting at the design stage, to applications, micro-services, and application programming interfaces (APIs) developed by the FRFI.

3.2.2 ***Strong and secure cryptographic technologies are employed.*** The FRFI 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. The FRFI should regularly assess its cryptography standard and technologies to ensure they remain effective against current and emerging threats.

3.2.3 ***Enhanced controls and functionality are applied to protect critical technology assets.*** The FRFI should employ enhanced controls and functionality to rapidly contain cyber security threats and to defend its critical technology assets and remain resilient against cyber attacks. The FRFI should also identify cyber security controls required to secure its critical technology assets that were identified per paragraph 2.2.2 of this Guideline. Application controls should be designed to contain and limit the impact of a cyber attack. Enhanced security standards, configuration baselines and security hardening requirements should be implemented, monitored

and reviewed to ensure ongoing confidentiality, integrity and availability of critical technology assets throughout their life cycle.

3.2.4 ***Cyber security controls are layered.*** The FRFI 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). The FRFI should also ensure resilience against current and emerging cyber threats by maintaining defence controls and tools, and ensuring continuous operational effectiveness of controls by minimizing false positives.

3.2.5 ***Data protection and loss prevention security controls are implemented.*** Starting with clear information classification of its data, the FRFI should design and implement controls for the protection of its data throughout its life cycle. Specifically, the FRFI should:

- Define and implement risk-based data protection controls for data residing in all FRFI environments (e.g., development, testing, production, backup) and data hosted by its third parties, including Cloud Service Providers (CSPs);
- Protect backup data from cyber attacks (e.g., ransomware);
- Implement multi-layered controls for the encryption of data at rest, data in transit and data in use; and,
- Implement risk-based data loss prevention capabilities and controls, informed by use cases for high-risk data loss channels.

3.2.6 ***Security vulnerabilities are remediated.*** To ensure security vulnerabilities are well managed, The FRFI should:

- Maintain capabilities to ensure timely risk-based patching of vulnerabilities in vendor software and internal applications that consider the severity of the threat and vulnerability of the exposed systems;
- Set minimum risk-based timelines to apply patches from the time a vulnerability is identified and assessed. Patches should be applied at the earliest opportunity, commensurate with the risks. For example, a vulnerability that is classified by the FRFI as being critical (i.e., poses the highest risk) should be remediated within 48 hours. Similar timelines should be established for less critical vulnerabilities;
- Implement additional compensating controls as needed to sufficiently mitigate risks or when there is no viable patch 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.*** The FRFI should implement risk-based identity and access controls, including Multi-Factor Authentication (MFA)[2] and privileged access management. At a minimum, consideration should be given to:

- Enforcing the principles of least privilege, need to know and segregation of duties;
- Regular recertification of access and permissions and prompt removal of access;

[2] 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, c) **is**, such as biometrics or behaviour.

- Maintaining strong and complex passwords, commensurate with risk, to authenticate employee, customer and third-party access to technology assets;
- Implementing MFA across all 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 processes;
- Ensuring system and service accounts are securely authenticated, managed and monitored to detect unauthorized usage; and,
- Performing appropriate background checks on persons granted access to FRFI systems or data, commensurate with the criticality and confidentiality of the technology assets.

3.2.8 ***Security configuration baselines are enforced; deviations are remediated.*** The FRFI 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. Additionally, the FRFI should:

- Enforce, and restrict changes to, approved secure operating system images, patterns and baselines to limit deviations and reduce the risk of misconfiguration;
- Detect and remediate configuration deviations in a timely manner following established processes;
- Monitor security configuration deviations and report on any approved exceptions;
- Prioritize any deviations or exceptions on a risk basis if timely remediation is not possible; and,
- Report, and obtain approval for, any deviations or exceptions to inform the FRFI's cyber risk profile.

3.2.9 ***Application scanning and testing capabilities are employed.*** 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 2.4.3).

3.2.10 ***Additional security controls are applied for external-facing services***. For external-facing application services and network infrastructure, the FRFI should implement additional layers of security controls to protect these services from cyber attacks such as volumetric, low/slow network and application business logic attacks. For cyber security services delivering and protecting critical online services, the FRFI should regularly test controls, runbooks and playbooks.

3.2.11 ***Cyber security defence controls maintained for hosts, endpoints and mobile devices.*** The FRFI should maintain multiple layers of cyber security defence controls for hosts, endpoints and mobile devices. In particular, the FRFI should:

- Leverage a combination of allow/deny lists including file hash/signature and indicators of compromise, in addition to advanced behaviour-based protection capabilities that are continuously updated; and,
- Apply defence controls and mitigation capabilities for virus, malware, data loss and intrusion detection and prevention to all relevant technology assets.

3.2.12 ***Networks are protected.*** The FRFI should protect all of its networks, including external-facing services, from threats by minimizing its attack surface. The FRFI should define authorized logical network zones and apply controls to segregate and limit, or block access and traffic to and from network zones. OSFI expects the FRFI to maintain intrusion prevention, monitoring and alerting tools on its network perimeter.

3.2.13 ***Physical access controls and processes are applied.*** The FRFI should define and implement physical access management controls and processes to protect network infrastructure and other technology assets from unauthorized access and environmental hazards. Physical areas may include office premises, data centres, network equipment rooms, data backup/storage sites, servers and workstations. Some sound practices include:

- Implementing user provisioning processes to provide access to authorized persons, periodically recertifying access and promptly revoking access when not required;
- Protecting network equipment and other technology assets from environmental threats and hazards; and,
- Disabling network access points and hardware ports when not in use, to prevent unauthorized access.

3.3 Detect

Principle 14: The FRFI designs, implements and maintains continuous security detection capabilities to enable monitoring, alerting, and enable forensic cyber security incident investigations.

3.3.1 ***Continuous, centralized security logging to support investigations.*** The FRFI should ensure continuous security logging for all technology assets and different layers of defence tools. Central tools for aggregating, correlating and managing security event logs by risk 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. For technology assets and services, the FRFI 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.*** The FRFI should maintain security information and event management capabilities to ensure continuous detection and alerting of malicious and unauthorized user and system activity. Advanced behaviour-based detection and prevention should be used to detect user and entity behaviour anomalies, and emerging external and internal threats that may be difficult to detect using predefined security rules or policies. The

latest threat intelligence and indicators of compromise should be used to continuously enhance FRFI monitoring tools. For high-risk use cases, the FRFI should inspect encrypted data in motion to enhance its continuous monitoring and detection capabilities.

3.3.3 ***Cyber security alerts are triaged.*** The FRFI 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 15: The FRFI should triage, respond to, contain, recover and learn from cyber security incidents impacting its technology assets, including incidents originating at third-party providers.

3.4.1 ***Incident response capabilities are integrated and aligned.*** The Technology Operations domain sets out the foundational expectations for the FRFI's incident and problem management capability. OSFI expects the FRFI to ensure the alignment and integration between its technology, cyber security, and 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.*** The FRFI 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.*** OSFI expects the FRFI to maintain a cyber security incident management process and playbooks to enable timely and effective management of cyber security incidents. Such playbooks should involve internal and external FRFI roles when material activities are outsourced or involve third-party providers, including vendors, suppliers, managed services providers or CSPs.

3.4.4 ***Timely response, containment and recovery capabilities are established.*** The FRFI 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. Where such security services are outsourced to a third party, the FRFI should clearly define timely notification and escalation thresholds to management.

3.4.5 ***Forensic investigations and root cause analysis are conducted, as necessary.*** The FRFI should conduct an expert forensic investigation for incidents where there is potential for material exposure to its technology assets. For high-severity incidents, the FRFI should conduct a detailed post-incident assessment of direct and indirect impacts (financial and 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.

3.4.6 ***Testing and simulation to continuously improve response.*** Further to expectations in section 2.7 of the Technology Operations domain, the FRFI should conduct periodic exercises and testing of its incident management process, playbooks, and other response tools (e.g., coordination and communication) to maintain and validate their effectiveness.

4. Third-Party Provider Technology and Cyber Risk

Outcome: Reliable and secure technology and cyber operations from third-party providers.

This domain should be read in conjunction with principles articulated in Guideline B-10, which advances OSFI's general expectations for the sound management of outsourcing and third-party risks, including that FRFIs retain ultimate accountability for outsourced activities.[3] Accordingly, in addition to expectations articulated in Guideline B-10, the FRFI should consider additional controls to manage technology and cyber risks at all third-party providers (TPPs) including, but not limited to, CSPs and managed service providers.

4.1 General

Principle 16: The FRFI should ensure that effective controls and processes are implemented to identify, assess, manage, monitor, report and mitigate technology and cyber risks throughout the TPP's life cycle, from due diligence to termination/exit.

4.1.1 ***Clear responsibilities in TPP arrangements.*** While the FRFI retains ultimate accountability for outsourced activities, the FRFI should clarify its responsibilities, and those of TPPs, in managing technology and cyber risks. As such, a formal agreement between the TPP and the FRFI should be defined, accepted by all parties and implemented at the time of onboarding to limit ambiguity regarding responsibilities for technology and cyber controls.

4.1.2 ***TPPs to comply with the FRFI's standards.*** The FRFI should establish mechanisms to ensure that TPPs comply with its technology and cyber standards as developed in accordance with the Technology Operations and Cyber Security domains of this Guideline. For example:

- TPPs' privileged access should be managed and closely monitored. When connecting to the FRFI, controls should be defined and implemented to prevent and detect unauthorized access and activities through any mechanism. The FRFI's access to its information assets located at TPPs must also be managed, monitored and reviewed according to FRFI standards.

[3] OSFI Guideline B-10 is in the process of being updated and its scope will be expanded to capture other third-party provider arrangements beyond outsourcing.

- FRFI standards for data classification, protection and secure destruction of FRFI information should apply to TPPs that store, use, modify or transmit FRFI information.
- TPPs should be subject to FRFI change and configuration management standards as applicable to FRFI information and information systems.
- Centralized logging and monitoring processes should be implemented to detect anomalies and proactively implement controls across all TPP assets including cloud, with the capability to conduct consolidated analysis and reporting on security posture across platforms.

4.2 Cloud Computing

4.2.1 ***Cloud-specific requirements are established.*** The FRFI should develop cloud-specific requirements to ensure that cloud adoption occurs in a structured and measured way that optimizes interoperability while operating within the FRFI's stated risk appetite. These requirements should augment existing FRFI controls and standards, including but not limited to areas such as:

- Identity and Access Management;
- API management;
- Containers and orchestration;
- Data protection;
- Management of vulnerabilities; and
- Cryptographic key management.

These requirements should be accompanied by robust cloud governance to provide proper oversight and monitoring of compliance with risk management practices at the FRFI. Cloud-specific requirements should guide decision-making and help ensure alignment of solutions to the FRFI's broader technology strategy.

4.2.2 ***Cloud portability is considered at design and implementation stage.*** In addition to planning appropriate exit strategies, the FRFI should also consider portability (i.e., the FRFI has the ability to move applications and data from one CSP to another) as part of the design and implementation process in cloud adoption.

5. Technology Resilience

Outcome: Technology services are delivered, as expected, through disruption.

This domain focuses on the FRFI's disaster recovery capabilities, which support the FRFI's ability to deliver technology services through operational disruption. This domain is complemented by related expectations set out in Domains 2-4 that contribute to technology resilience, including Technology Architecture, Incident and Problem Management and Cyber Security.

5.1 Disaster Recovery

Principle 17: The FRFI should establish and maintain an Enterprise Disaster Recovery Framework (EDRF) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

5.1.1 ***Disaster recovery framework established.*** OSFI expects the FRFI to develop, implement and maintain an EDRF that sets out the FRFI's approach to recovering technological services during a disruption. The FRFI should align the EDRF with its business continuity management program. At a minimum, the EDRF 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;
- Procedures and capabilities to recover technology services to an acceptable level, within an acceptable timeframe, during disruption; and,
- A strategy, policy and processes for system and data backup that address, among other things: data retention periods; back-up processes and frequency; data storage and destruction processes; and periodic testing.

5.1.2 ***Key dependencies are managed.*** OSFI expects the FRFI to manage key dependencies required to support the EDRF, including:

- 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 asset locations.

Principle 18: The FRFI should perform scenario testing on disaster recovery capabilities to confirm its technology services operate as expected through disruption.

5.1.3 ***Disaster recovery scenarios are tested.*** To promote learning, continuous improvement and technology resilience, OSFI expects the FRFI to validate and report on its disaster recovery strategies and plans regularly against severe but plausible scenarios. These scenarios should be forward-looking and incorporate, where appropriate:

- New and emerging risks or threats;
- Material changes to business objectives or technologies; and,
- Previous incident history and known technology complexities or weaknesses.

The FRFI's disaster recovery scenarios should test:

- The FRFI's backup and recovery capabilities and processes in order to validate resiliency strategies, plans and actions, and confirm the organization's ability to meet pre-defined requirements, including through live execution and/or simulation by walk-through; and,

- Critical third-party technologies and integration points with upstream and downstream dependencies, including both on- and off-premises technology.