Cassels

Resilience is Key – OSFI Issues Draft Technology and Cyber Risk Guidance

Gordon Goodman

November 17, 2021

On November 9, 2021, the Office of the Superintendent of Financial Institutions (OSFI) released a draft guideline[1] focused on the management of technology and cyber security risks by federally regulated financial institutions (FRFIs). This draft guideline establishes a comprehensive framework to guide accountability, planning, prevention, monitoring and continuous improvement of information technology structures and processes within FRFIs in order to appropriately manage technology and cyber security risks, based on the FRFI's size, nature, scope and complexity of its operations and risk profile.

This draft guideline is the next step in an evolution of technology and cyber risk guidance issued by OSFI in recent years, no doubt a response to ongoing and more frequent cyber-attacks affecting businesses generally. OSFI's initial foray into the cyber security field took the form of its "Cyber Security Self-Assessment" tool,[2] published in October 2013 and updated on August 13, 2021. This tool was developed to help FRFIs assess their level of cyber security preparedness and to improve their cyber security posture. The Cyber Security Self-Assessment tool was followed by OSFI's Technology and Cyber Security Incident Reporting Advisory[3] which was published on January 24, 2019 (updated on August 13, 2021) that established a cyber incident reporting requirement for FRFIs based on a "reportable incident" having one or more of the various characteristics described in the Advisory. In the fall of 2020 OSFI issued a discussion paper on technology and related risks[4] and received stakeholder feedback. This draft guideline is the latest step by OSFI to ensure that FRFIs are paying close attention to technology and cyber risks within their organizations and are managing them appropriately.

The draft guideline attempts to differentiate between technology risk and cyber risk, although the definitions appear to overlap a great deal and the draft guideline refers to them in combination and not in isolation. Broadly speaking, OSFI sees cyber risk as potentially resulting in financial loss, operational disruption or reputational damage whereas its definition of technology risk relates only to financial loss.

Technology and cyber risks interact with other areas of risk. Accordingly, OSFI recommends that guidance, tools and communication from this draft guideline be viewed in conjunction with existing OSFI guidance and other authorities on risk management within the FRFI space, such as OSFI'S B-10 guideline[5] that is focused on the outsourcing of business activities, functions and processes. Within the draft guideline OSFI announced that there would be updates to the B-10 guideline in the future. The updates will broaden the scope of B-10 to encompass and capture third-party provider arrangements beyond the guidance given around outsourcing agreements.

Five Domains and Associated Principles

The draft guideline is organized into the following five domains, each of which is meant to express a desired outcome with the overall goal of resilience to technology and cyber risk: Technology and Cyber Governance and Risk Management, Technology Operations, Cyber Security, Third-Party Provider Technology and Cyber Risk, and Technology Resilience. Eighteen principles are then presented under the five domains, and these principles give specific actionable frameworks to assist FRFIs in fulfilling the requirements set out in the draft guideline.

The 5 domains and their associated 18 principles are set out in the table below.

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.

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.
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.
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.

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.

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.

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.

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.

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.

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.

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.

Incident and Problem Management **Principle 10**: THE FRFI should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts.
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.

3. Cyber Security

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

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.
Defend **Principle 13**: The FRFI should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets.
Detect **Principle 14**: The FRFI designs, implements and maintains continuous security detection capabilities to enable monitoring, alerting, and enable forensic cyber security incident investigations.
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.

4. Third-Party Provider Technology and Cyber Risk

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

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.

5. Technology Resilience

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

Important Takeaways from the Draft Guideline

The comprehensive nature of the draft guideline, once finalized and published, will mean that FRFIs will need to take a close and critical look at their information technology governance structures, processes, policies, operations and risk tolerances. Sophisticated FRFIs may already have these elements in place to meet these demanding requirements. For those that fall short of the requirements, the draft guideline will mean identifying gaps, investing resources in remediation and ensuring compliance on a go forward basis. We have listed below some key issues to consider.

Accountability

The draft guideline emphasizes that senior management of the FRFI remains accountable for directing the FRFI's technology and cyber security operations and that the FRFI should assign clear responsibility for technology and cyber risk governance to senior officers. In other words, this accountability is important and must remain with senior management. As an example, the accountability cannot be delegated to a mid-level IT manager. Accordingly, this obligation could lead some financial institutions to create specific senior leadership roles, such as Chief Technology Officer or Chief Information Officer, if they do not already exist within the organization.

Continuous Improvement

Throughout the draft guideline OSFI stresses the need for continuous evaluation, improvement and learning

with respect to technology and cyber risk management. FRFIs will need to focus heavily on updating their technology operations, as the draft guideline puts in place multiple new technology operating requirements. Principles four to nine highlight the multiple management and technology architectural frameworks that need to be employed to fulfill OSFI's requirements. FRFIs will have to invest resources and management capacity in implementing these new frameworks in a timely manner.

Relationships with Third-Party Providers

One of the challenges for FRFIs posed by the draft guideline will be the negotiation of contracts with third party technology service providers, which includes not only outsourced service providers, but cloud service providers and IT developers. The draft guideline makes it clear that the FRFI remains ultimately accountable for all outsourced activities and that effective controls must be implemented, even if the service is provided through a third party. As anyone who has been presented with a cloud services agreement knows, these low-cost services are frequently offered on an "as is" basis. Will third party service providers that provide services to the financial services industry adapt their practices and contracts to meet the draft guideline's requirements or will FRFIs be forced to purchase the services "as is" and work internally to develop compensating controls to meet the requirements? It is yet to be seen how the relationship between FRFIs and third-party service providers will fare with these new requirements.

Secure-by-Design/Resilience-by-Design

Interestingly, although the draft guideline refers to building systems with "Secure-by-Design" and "Resilience-by-Design" architecture, it does not refer to "Privacy-by-Design", which one would think goes hand in hand with "Secure-by-Design." Given recent initiatives in Canada towards the modernization of privacy laws, it would seem prudent and cost effective for FRFIs to also address the "Privacy-by-Design" aspect at the time a system is built, especially if these security and resiliency requirements are to be simultaneously addressed at the time of system construction.

Next Steps

OSFI is accepting comments on the draft guideline until February 9, 2022 and is conducting an information session on November 30, 2021. In particular, OSFI is seeking stakeholder input on:

- The clarity of OSFI's expectations, as set out in the draft guideline;
- The application of these expectations, commensurate with the institution's size, nature, scope, and complexity of operations;
- The balance between principles and prescriptiveness in OSFI's expectations; and
- Other suggestions that contribute to OSFI's mandate to protect depositors and policyholders, and

maintain public confidence in the Canadian financial system, while also allowing institutions to compete and take reasonable risks.[6]

We will continue to monitor and report to our readers on these developments as they occur.

The authors gratefully acknowledge the contributions of articling student Simi Solebo in the preparation of this article.

---

[1] Office of the Superintendent of Financial Institutions, *Draft Guideline - Technology and Cyber Risk Management* (November 2021), Online: OFSI <https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13.aspx>.

[2] Office of the Superintendent of Financial Institutions, *Cyber Security Self-Assessment* (August 2021), Online: OFSI < https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/cbrsk.aspx>.

[3] Office of the Superintendent of Financial Institutions, *Technology and Cyber Security Incident Reporting* (August 2021), Online: OFSI < https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx>.

[4] Office of the Superintendent of Financial Institutions, *Developing Financial Sector Resilience in a Digital World* (September 2020), Online: OSFI <https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/Pages/tchrsk-nr.aspx>.

[5] Office of the Superintendent of Financial Institutions, *Guidelines B-10 Outsourcing of Business Activities, Functions and Processes* (March 2009), Online: OFSI <https://www.osfi-bsif.gc.ca/Eng/Docs/b10.pdf>.

[6] Office of the Superintendent of Financial Institutions, *OSFI launches consultation on a draft Technology and Cyber Risk Management Guideline,* (November 2021), Online: OFSI <https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13-let.aspx>.
