Cassels

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

Bernice Karn, Gordon Goodman

November 17, 2021

1

2

3

4

5

Five Domains and Associated Principles

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

Accountability

Continuous Improvement

Relationships with Third-Party Providers

Secure-by-Design/Resilience-by-Design

Next Steps

- 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]

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>.
