OSFI ADDS TO ITS EXISTING TECHNOLOGY AND CYBER RISK REQUIREMENTS WITH GUIDELINE B-13

Posted on July 26, 2022

Categories: Insights, Publications

On July 13, 2022, the Office of the Superintendent of Financial Institutions ("**OSFI**") issued its final *Guideline B-13 – Technology and Cyber Risk Management* ("**Guideline B-13**").[1] Guideline B-13 is intended to help federally regulated financial institutions ("**FRFIs**") develop greater resilience to technology and cyber risks, and is in addition to OSFI's *Technology and Cyber Security Incident Reporting Advisory*[2] (requiring, *inter alia*, notification to the FRFI's Lead Supervisor and OSFI's Technology Risk Division in writing of any reportable technology and cyber security incidents within 24 hours or sooner) and *Cyber Security Self-Assessment*[3] (used to assess an FRFI's level of cyber security preparedness), both issued in August of 2021.

OSFI issued a draft version of Guideline B-13 in November 2021, and subsequently developed the guideline through a consultation process with key stakeholders. As compared with the November 2021 draft, Guideline B-13 is more streamlined, less prescriptive in its expectations, and provides more clarity in its definitions and expectations.[4]

Guideline B-13 focuses on the following three domains:

1. **Governance and Risk Management**. This domain sets out OSFI's expectations for FRFI's to have clear responsibilities and structures, as well as comprehensive strategies and frameworks governing technology and cyber risk (i.e., 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). The emphasis of this domain is on having a proper risk management framework and organizational structure so that there is a clear accountability system. More specifically, Guideline B-13 notes that 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. In addition, OSFI directs FRFIs to be proactive in anticipating the risks and prepare for new challenges as technology evolves.
2. **Technology Operations and Resilience**. This domain sets out OSFI's expectations for FRFIs to have a technology environment that is stable, scalable and resilient. The technology environment should also be

monitored to ensure it is current and supported by robust and sustainable technology operating and recovery processes. This domain deals with a number of topics, including technology architecture, asset management, project management, system development life cycle, implementation and patch management, problem management, monitoring, and disaster recovery.

3. **Cyber Security**. This domain sets out OSFI's expectations for a secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets. OSFI directs FRFIs to take a proactive approach in identifying risks and threats rather than reacting passively, and sets out the requirements to satisfy this objective. It also lists measures that should be in place to detect and defend against technology and cyber threats (for example, using strong cryptographic technologies), as well as to respond, recover and learn from security incidents.

The Guideline acknowledges that there is no one size fits all approach, and accordingly there can be flexibility in how FRFIs choose to achieve the objectives under each domain commensurate with the FRFI's size, risk profile, and the nature, scope, and complexity of the FRFI's operations.

Guideline B-13 will be effective on January 1, 2024, giving FRFIs time to self-assess and ensure compliance. FRFIs should carefully review Guideline B-13 to determine the extent to which their current policies and procedures conform with the Guideline, and whether any amendments are necessary to remain compliant when the new Guideline comes into effect.

Note that similar requirements have been developed for provincially regulated financial institutions over the last few years as well (for instance, those found in British Columbia's *Information Security Guideline*[5] or Saskatchewan's *Cyber Security Self-Assessment Questionnaire*[6]).

If you have any questions about Guideline B-13 or how to develop effective cyber security programs and policies, a member of McMillan's Privacy and Data Security Group would be pleased to assist you.

[1] "Technology and Cyber Risk Management", online: Office of the Superintendent of Financial Institutions (last modified July 13, 2022).
[2] "Technology and Cyber Security Incident Reporting", online: Office of the Superintendent of Financial Institutions (last modified September 3, 2021).
[3] "Cyber Security Self-Assessment", online: Office of the Superintendent of Financial Institutions (last modified August 16, 2021).
[4] "OSFI response to draft Guideline B-13 consultation feedback – Technology and Cyber Risk Management", online: Office of the Superintendent of Financial Institutions (last modified June 9, 2022).
[5] "Information Security Guideline", online: British Columbia Financial Services Authority (last modified February 18, 2021).

[6] "Cyber Security Self-Assessment Questionnaire", online: Financial and Consumer Affairs Authority of Saskatchewan.

by Darcy Ammerman, Robbie Grant, ZiJian Yang (Summer Law Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2022