Bulletin | Cybersecurity, Privacy and Data Protection

August 2022

OSFI's new Guideline B-13 – Managing technology and cyber risks

On July 13, 2022, the Office of the Superintendent of Financial Institutions (OSFI) announced the final version of its new *Guideline B-13 – Technology and Cyber Risk Management*. The Guideline establishes OSFI's expectations for how federally regulated financial institutions ("FRFIs") manage technology and cyber risks. Many FRFIs will be required to make substantial changes to their information technology and cybersecurity policies, practices and procedures before the Guideline comes into effect on January 1, 2024. The Guideline is also an important summary of best practices for other kinds of organizations.

OSFI and cybersecurity

OSFI is an independent agency of the Government of Canada that regulates and supervises FRFIs, including banks, federally incorporated or registered trust and loan companies, insurance companies, and pension plans subject to federal oversight. Over the years, OSFI has emphasized the importance of cybersecurity and issued guidance and requirements to help FRFIs implement policies and practices to manage cyber risks and effectively respond to cyber incidents, including OSFI's *Cyber Security Self-Assessment* (issued in 2013 and updated in 2021) and OSFI's *Advisory on Technology and Cyber Security Incident Reporting* (issued in 2019 and updated in 2021). See BLG bulletins *OSFI Updates Technology and Cyber Security Incident Reporting Advisory* and *Regulatory Guidance for Cyber Risk Self-Assessment*.

In 2020, OSFI issued a discussion paper and began a consultation on technology risks and resilience in the financial sector. The process resulted in OSFI's new Guideline B-13 and will inform OSFI's proposed updated *Guideline B-10 – Third-Party Risk Management* (which will replace OSFI's current *Guideline B-10 – Outsourcing*).

Guideline B-13

Purpose and scope

OSFI's new *Guideline B-13 – Technology and Cyber Risk Management* (the "Guideline") establishes OSFI's expectations for FRFIs' management of technology risks and cyber risks. The Guideline broadly defines "technology risk", which is deemed to include "cyber risk", as referring 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". The Guideline broadly defines "technology assets" as both tangible and intangible assets, including data and information, that need protection and support the provision of technology services.

The Guideline applies to all FRFIs without exception, but acknowledges that "there is no one-size-fits-all approach for managing technology and cyber risks". The Guideline explains that it "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".

The Guideline also explains that it should be read in conjunction with other OSFI guidance, tools and supervisory communications, guidance from the Canadian Centre for Cyber Security, and other recognized frameworks and standards for technology operations and information security.

Layered approach – Outcomes, principles and controls

OSFI explained that the Guideline takes a "layered approach" to presenting OSFI's expectations. The Guideline is organized into three "domains" – Governance and Risk Management, Technology Operations and Resilience, and Cyber Security – with specified outcomes, which are supported by 16 general principles and 57 statements of recommended controls.

- The Governance and Risk Management domain sets OSFI's expectations for a FRFI's formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. The specified outcome is the governance of technology and cyber risks through clear accountabilities and structures, and comprehensive strategies and frameworks.
- The Technology Operations and Resilience domain sets OSFI's expectations for a FRFI's management and oversight of risks related to the design, implementation, management and recovery of technology assets and services. The specified outcome is a technology environment that is stable, scalable and resilient, kept current and supported by robust and sustainable technology operating and recovery processes.
- The Cyber Security domain sets OSFI's expectations for a FRFI's management and oversight of cyber risk. The specified outcome is a secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets.

Third-party provider risks

The Guideline does not expressly reference the management of third-party provider technology and cyber risks, which were included in the initial draft of the Guideline. OSFI explained that those risks were removed in response to consultation feedback, and will be addressed in OSFI's updated *Guideline B-10 – Third-Party Risk Management*.

Comments and recommendations

- **Three pillars:** The Guideline reflects the view that effective technology and cyber risk management is an enterprise-wide risk management and compliance challenge that requires a comprehensive, multidisciplinary approach based on three pillars – people, processes and technology.
- **Best practices:** The Guideline is generally consistent with current standards and best practices for managing technology and cyber risks, including OSFI's previous cybersecurity guidance, the BC Financial Services Authority's *Information Security Guideline*, the Canadian Centre for Cyber Security's *Baseline cyber security controls for small and medium organizations*, the New York Department of Financial Services' *Cybersecurity Regulation*, and cybersecurity standards issued by the National Institute of Standards and Technology.
- **Continuous improvement:** Compliance with the Guideline is not a one-time event. The Guideline requires FRFIs to establish processes and procedures to continuously monitor and improve their cybersecurity posture.
- **Time/effort for initial compliance:** Most FRFIs will likely be required to spend significant time and effort to achieve and document initial compliance with the Guideline. Many FRFIs will be required to make substantial changes to their information technology and cybersecurity policies, practices and procedures. FRFIs should begin that process as soon as possible so that required work can be identified and performed in a cost-effective manner before the Guideline comes into effect on January 1, 2024.
- **Resources for compliance:** FRFIs might be required to engage additional human resources (including technical consultants), and procure additional technologies and services (including legal advice), to achieve initial compliance with the Guideline. FRFIs should identify and address those resourcing requirements as soon as possible.
- **FRFI directors and officers:** A FRFI's directors and senior officers should have direct involvement in the FRFI's compliance with the Guideline, as set out in the Guideline and in OSFI's *Corporate Governance Guideline*. Their decisions should be made with

documented due care (i.e., based on accurate information and expert advice) to achieve the best outcome for the FRFI and to support the application of the "business judgment rule". See BLG bulletin *Cyber risk management guidance for Canadian corporate directors*.

- **Foreign entity branches:** The Guideline does not have any exceptions or special rules for foreign entities operating in Canada on a branch basis using information technologies and services provided by their home office or other affiliates. OSFI's *Guideline - Foreign Entities Operating in Canada on a Branch Basis* explains that management of a Canadian branch is responsible for effective adaptation, implementation and oversight of risk management policies and procedures, and related risk management controls, for the branch.
- **Third-party provider risks:** Compliance with the Guideline implicitly requires FRFIs to manage risks relating to the use of information technology services provided by third parties. This has significant implications for FRFIs and their service providers. (OSFI's expectations regarding third-party provider technology risks will be expressly set out in in OSFI's proposed updated *Guideline B-10 – Third-Party Risk Management*.)
- **Other legal requirements:** A FRFI's activities for compliance with the Guideline should be consistent with other legal requirements, including applicable private sector personal information protection laws (including the proposed *Consumer Privacy Protection Act*) and the proposed federal *Critical Cyber Systems Protection Act*. See BLG bulletin *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses*.
- **Legal privilege:** Compliance with the Guideline and other risk management activities may result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and legal proceedings unless the communications and documents are protected by legal privilege. Where appropriate, FRFIs should take steps to establish and maintain legal privilege over communications and documents relating to compliance with the Guideline. See BLG bulletins *Cyber Risk Management – Legal Privilege Strategy – Part 1* and *Cyber Risk Management – Legal Privilege Strategy – Part 2*.
- **Risk-based decisions:** The Guideline acknowledges that compliance will require FRFIs to make numerous risk-based decisions that reflect "the unique risks and vulnerabilities that vary with a FRFI's size, the nature, scope, and complexity of its operations, and risk profile". Each of those decisions should be fully informed (based on timely, complete and reliable information), made with the benefit of appropriate advice from independent and properly qualified technical experts and legal counsel, and properly documented. FRFIs should be prepared to justify each of those decisions, especially decisions to not fully implement recommended controls set out in the Guideline. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Eric Charleston
T 416.367.6566
echarleston@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in technology risk and cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.