Cassels

OSFI Issues Final Version of Guideline B-13, Technology and Cyber Risk Management

Gordon Goodman

07/15/2022

In November of 2021 the Office of the Superintendent of Financial Institutions (OSFI) issued draft Guideline B-13, *Technology and Cyber Risk Management*, that focused on the management of technology and cybersecurity risks by federally regulated financial institutions (FRFIs). (See our previous analysis of the draft guidance here.) After a period of industry consultation on the draft guideline, on July 13, 2022, OSFI issued the final form of Guideline B-13, which remains largely unchanged from the draft version, with a few exceptions.

Parsing through the language, the reader can see that OSFI has amended the draft guideline to make the final version simpler to follow and less prescriptive, no doubt in response to the changing nature of technology and to give FRFIs flexibility in the measures they use to manage technology and cyber risk. Whereas the draft guideline set out five "domains" to be followed in managing the FRFI's resilience to technology and cyber risks, the final version of Guideline B-13 trims these five domains to the following three,[1] with their expected outcomes:

- **Governance and Risk Management** – Guideline B-13 requires FRFIs to govern technology and cyber risks through clear accountabilities and structures, and comprehensive strategies and frameworks.
- **Technology Operations and Resilience** – The FRFI is expected to operate a technology environment that is stable, scalable and resilient. The environment is expected to be maintained as "current" and supported by "robust and sustainable technology operating and recovery processes."
- **Cyber Security** – This domain requires FRFIs to employ a secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets.

Notwithstanding the reduction in the number of domains, Guideline B-13 continues to emphasize OSFI's expectation that FRFIs take steps to become resilient to technology and cyber risks, such as technology outages and data breaches, while preserving their ability to compete in a global marketplace.

The other major revision to the prior draft is that the final version of Guideline B-13 does not contain detailed provisions on managing technology and cyber risk of third-party vendors, including cloud service providers. The guidance on those issues has been moved to the revised draft of Guideline B-10, *Outsourcing of Business Activities Functions and Processes*,[2] which is currently the subject of a three-month industry consultation, ending on July 27, 2022.

Guideline B-13 becomes effective January 1, 2024, allowing FRFIs a fair amount of time to assess their current technology and cyber security programs and implement those changes necessary to bring them into compliance with OSFI's expectations. We will continue to follow and update our readers on these developments as they occur.

---

[1] Office of the Superintendent of Financial Institutions, Guideline B-13 – Technology and Cyber Risk Management (July 2022), Online: <https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b13-jul-let.aspx>.

[2] Office of the Superintendent of Financial Institutions, Guideline B-10 – Outsourcing of Business Activities Functions and Processes (Revised March 2009), Online: <https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx>.

This publication is a general summary of the law. It does not replace legal advice tailored to your specific circumstances.