cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Agenda Item 4(c)(vi)
November 23/21 EOC Meeting

OSFI launches consultation on a draft Technology and Cyber Risk Management Guideline

Accompanying Documents

- Draft Guideline

Document properties

- **Type of Publication:** Letter
- **Date:** November 9, 2021

Today, the Office of the Superintendent of Financial Institutions (OSFI) is launching a three-month public consultation on Draft Guideline B-13: Technology and Cyber Risk Management.

The proposed Guideline sets out OSFI's expectations for sound technology and cyber risk management across five domains. Each domain is guided by a desired outcome and related technology-neutral principles that collectively contribute to operational resilience. The proposed Guideline responds to feedback received as a result of OSFI's fall 2020 discussion paper on technology and related risks (see Annex).

Existing OSFI guidance, including Guidelines E-21 (Operational Risk Management) and B-10 (Outsourcing of Business Activities, Functions and Processes), as well as the recently updated Technology and Cyber Security Incident Reporting Advisory and Cyber Security Self-Assessment tool, will complement the proposed Guideline. In May 2021, through its Near-Term Plan of Prudential Policy, OSFI shared its plan to review existing guidance on outsourcing and operational risk management.

Developing guidance for technology and cyber risks requires continued stakeholder engagement and transparency, so that OSFI can strike the right balance between its prudential objectives and allowing financial institutions to compete. OSFI welcomes public comments on Draft Guideline B-13, and is particularly interested in feedback on:Footnote1

- 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.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

An information session for financial institutions is planned within the next few weeks to provide an overview of OSFI's Draft Guideline B-13 and an opportunity to raise questions.

Please submit comments to Tech.Cyber@osfi-bsif.gc.ca by February 9, 2022.

Annex - Responding to OSFI's 2020 Technology and Related Risks discussion paper feedback

In developing Draft Guideline B-13, OSFI considered the range of feedback received from stakeholders in response to the fall 2020 discussion paper, *Developing financial sector resilience in a digital world*. Below is a brief summary of key issues from the discussion paper consultation and how OSFI responded to each.

Respondent Feedback	OSFI Response
Operational Risk and Resilience	
• Technology risks are effectively managed within a broader non-financial risk and operational risk management context, integrated in a firm's enterprise risk management program.	• Paragraph 1.3.1 seeks alignment of the federally regulated financial institution's (FRFI's) technology and cyber risk management framework with its broader enterprise risk framework. FRFIs should refer to OSFI's Corporate Governance Guideline (section III: Risk Governance) for additional guidance.
• Operational resilience is an outcome of effective operational risk management (ORM), and technology is a key enabler of operations.	• Draft Guideline B-13 aims to develop FRFIs' resilience to technology and cyber risks. Domain 5 (Technology Resilience) highlights the importance of disaster recovery and draws linkages to other resilience capabilities throughout the Guideline (e.g., within Technology Operations and Cyber Security). • OSFI is reviewing additional feedback received from its July 2021 Letter on Operational Risk and Resilience. OSFI may consider future amendments to Draft Guideline B-13 to better

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

	integrate operational resilience expectations across the suite of its regulatory guidance. • OSFI welcomes FRFIs' views on the balance between resilience capabilities and preventive controls in the Draft Guideline.
Technology and Cyber Security	
• A principles-based, technology-neutral approach in which definitions, concepts, and expectations align with accepted global standards and existing guidance is most appropriate for technology risk management.	• Some respondents indicated that more prescription can be helpful in implementing effective risk management and controls, particularly in relation to cyber security. However, OSFI acknowledges that some FRFIs (e.g., larger, more complex institutions) may already exceed a number of the more detailed expectations or find them unnecessarily prescriptive. • To balance the current level of prescription in Draft Guideline B-13, a 'layered' approach was taken to presenting expectations. All FRFIs—regardless of size, complexity and maturity of risk management—should aim at achieving the five outcomes and associated principles in the Guideline. OSFI believes this affords flexibility while still providing sufficiently clear guidance to institutions that may benefit from it.
• Most respondents offered a range of suggestions to improve existing guidance, while some felt that OSFI's current guidance and tools (e.g., self-assessment tool, incident	• While OSFI's recently updated Cyber Self-Assessment tool and Incident Reporting Advisory are critical, OSFI does not view them as sufficient or complete in responding to existing and emerging risks. Draft Guideline B-13 aims to address this gap with broad

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

reporting advisory) are sufficient to address emerging risks.	coverage of both cyber and other technology risks. The Cyber Self-Assessment is a supplemental tool and is not regulatory guidance.
• In general, emerging risks can be managed effectively within a broader technology risk management framework. Quantum readiness requires collective action by government, industry, and academia. OSFI should continue to engage in such efforts.	• OSFI acknowledges this view. However, it is important that risk frameworks explicitly account for risks arising from emerging or less proven technologies (paragraph 1.3.2). In line with a technology-neutral approach, OSFI is not advancing expectations specific to quantum computing.
Third Party Risk	
• Most respondents did not believe that separate guidance for technology-related third-party arrangements was warranted, and that technology-related third party arrangements should be considered as part of OSFI's planned review of Guideline B-10.	• OSFI considered that limited guidance, supplementary to Guideline B-10, on technology and cyber risks arising from third party provider arrangements (Domain 4), is appropriate and necessary in view of the current risk environment. OSFI remains open to stakeholder feedback on how best to position these expectations, including in the context of OSFI's review of Guideline B-10.
• Most respondents indicated that separate guidance on cloud risk management was not warranted, and that any cloud-related provisions could be incorporated into Guideline B-10.	
Data	
• OSFI should not create additional data risk guidance, as existing law and standards provide sufficient coverage for FRFIs. Some respondents recommended that	• OSFI continues to consider data-related risks relative to existing standards and initiatives underway. OSFI views some aspects of data (e.g., protection and loss prevention) as

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

OSFI consider the Basel Risk Data Aggregation and Risk Reporting (RDARR) principles as a basis for any additional expectations that could apply to all FRFIs, beyond systemically important banks.	being inextricably linked to sound technology and cyber risk management and therefore merit inclusion in this guidance.
• Data risk intersects many other risk areas (e.g., cyber security, models), and respondents highlighted key aspects of data risk itself (i.e., quality, security, privacy).	

Footnotes

Footnote 1

OSFI's responses to the fall 2020 consultation (see Annex) expand on the approach taken to Draft Guideline B-13.

Return to footnote1

Modified Date:
2021-11-09