Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

December 15, 2020

Sent via email to: Tech.Paper@osfi-bsif.gc.ca

TO: Office of the Superintendent of Financial Institutions Canada

RE: Discussion Paper -- *Developing Financial Sector Resilience in a Digital World: Selected Themes in Technology and Related Risks*

The Institute of Internal Auditors (IIA) and its affiliate, The Institute of Internal Auditors Canada (IIA Canada) appreciates the opportunity to comment on the September 2020 Discussion Paper – ***Developing Financial Sector Resilience in a Digital World: Selected Themes in Technology and Related Risks.***

The IIA's more than 200,000 members worldwide, including 7,400 in Canada, provide independent and objective insight and assurance on all facets of an organization's activities, performance, and position. The IIA is the global leader for the internal audit profession, encouraging strong governance, internal controls, leadership, rigout, and an enterprise-wide approach to risk management. As the internal audit profession's standard bearer for learning, training, and certification, our mandate is to foster transparency of all facets of an organization's activities, performance, and position. The IIA Canada serves and supports internal auditors throughout the country and across all industries and sectors. More than half of our members in Canada are based in Ontario.

We understand that OSFI's Strategic Plan 2019-2022 "aims for FRFIs and pension plans to be better prepared to identify and develop resilience to non-financial risks before they negatively affect their financial condition." The IIA is similarly committed to providing internal auditors with the information, skills, and knowledge to effectively advise FRFIs and pension plans per our Standard 2100 – Risk Management, as detailed in the International Professional Practices Framework (IPPF), which states that the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

To this end, The IIA has been working diligently over the past few years to produce a body of knowledge directly related to the risks that OSFI mentions. We are pleased to be offered the opportunity to share some of the insights from our recent Financial Services practice guides that we believe will be helpful to OSFI as it develops new and expanded guidance for financial services firms on technology risks.

Global Headquarters
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

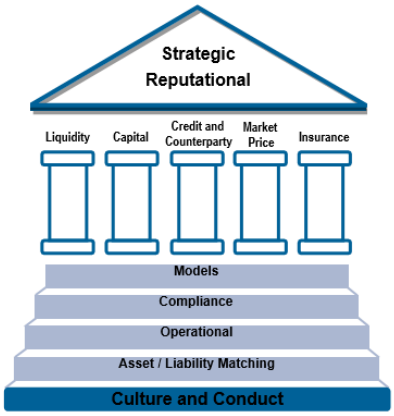
Specific Questions:

UNDERSTANDING TECHNOLOGY RISK

QUESTION 1

What is your view of the relationship between operational resilience, operational risk management (ORM) and technology risks? How should institutions integrate these concepts into their broader enterprise risk management?

A: We agree with OSFI that Technology Risk is considered a component of Operational Risk, which would roll up into the organization's overall Enterprise Risk Management framework (see The IIA's Financial Services Risk Framework below). We view Operational Resilience as a result or an outcome of effective technology risk management.



Source: The IIA

QUESTION 2

Can emerging technology risks be effectively managed through existing ORM principles and tools (e.g., the three lines of defence, scenario analysis)? What gaps exist with respect to current principles and tools, and how should they be addressed? Are there any leading practices OSFI should incorporate?

A: Emerging technology risks can be managed through existing ORM principles and tools as they simply represent different threats or provide new vulnerabilities to the achievement of business objectives. The principles in the document (e.g., confidentiality, integrity, availability under Cyber Security) can encompass emerging technology risks.

QUESTION 3

What factors influence the degree of financial loss exposure that may be generated by technology related risks?

A: According to Standard 2100 – Risk Management as it appears in the current IPPF, the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes. Internal auditors should be informed of the measures of financial loss exposure used within their organization and can contribute to discussions regarding the relevance and effectiveness of those measures.

QUESTION 4

What are your views on OSFI's proposed definition and scope for technology risk?

A: We agree with OSFI's definition and scope for technology risk. In The IIA's view, the definition, risk domains, and principles resonate and are enduring, particularly given the openness to integrating new principles such as "explainability" that arise from new technologies.

We also agree with OSFI's statements in Section 6.3 that current guidance could be expanded and modernized. We suggest:

- *Scope areas and principles should be expanded to include unique risks presented by cloud technology, such as data location and security and vulnerabilities within cloud service providers' infrastructure, in addition to the risks OSFI already notes in sections 6.8 to 6.13.*
- *In agreement with OSFI and given the growing partnerships with Fintechs, technology risks should be expanded to include risks within third party systems and how they are integrated into the banks' ecosystem.*
- *Because some key components of core banking systems at Canadian banks are based on legacy programming languages (e.g., COBOL), OSFI should give consideration to "resourcing risk" by asking the question, "Is there sufficient capability to maintain these systems?" Perhaps obsolescence risk should be called out specifically.*

QUESTION 5

Considering existing frameworks issued by technology standard-setters, how can OSFI provide value-added expectations in this area?

A: Given the multitude of existing frameworks that have overlapping scopes and similar objective, OSFI could seek to simply reinforce its expectation that the entities overseen have researched and leveraged current frameworks to optimize technology-related risk management in achieving the entities' objectives.

The IIA would note two areas not covered in any depth in any framework where OSFI may wish to issue guidance. In particular:

1. *Articulating and measuring Technology Risk Appetite: Technology risks, like other operational risks, are difficult to quantify unlike market risk, credit risk or underwriting risk. However, since technology is such a critical element in financial institutions' ability to do business (and that criticality is increasing), it may be valuable for OSFI to put out guidance on development of a Technology Risk Appetite as part of the institutions' overall Risk Appetite Framework. A potential approach may be to define key drivers of Tech Risk and develop a Risk Appetite against such metrics.*
2. *COVID-19 has caused significant, and potentially permanent, changes to how we work. There may be an opportunity to issue guidance on remote work arrangements and, in particular, the implications for information security and privacy.*

PRINCIPLES

QUESTION 6

Is OSFI's approach of principles-based regulation fit for purpose for this risk area? What form(s) of regulatory guidance would best advance sound technology risk management (e.g., high-level principles-based framework, comprehensive technology risk management guidance, detailed issue-specific guidance, etc.)?

A: The IIA has also chosen a principles-based approach in the IPPF, and we believe this approach is likely the most sustainable given the effort that would be required to sustain detailed guidance on technology risks. We also believe a principles-based approach ensures the responsibility for implementing appropriate risk management measures remains with the regulated entities. We do not envision this would preclude OSFI from its current practice of issuing bulletins on the state of practices in specific areas, particularly emerging risks where practices are in rapid evolution and broader guidance is not yet established.

CYBER SECURITY

QUESTION 7

Is OSFI's existing cyber security self-assessment and incident reporting guidance sufficient in view of emerging risks (e.g., quantum computing)? What gaps exist in OSFI's current guidance, and how should these gaps be addressed? Are there any leading practices OSFI should incorporate?

A: The IIA's recently published OnRisk 2021 report explores three related risks including Cybersecurity, Data Governance and Disruptive Innovation. According to OnRisk 2021, recommended actions related to Cybersecurity risks may include:

- *C-suite: Dedicate necessary internal and/or external resources to consistently evaluate emerging cyber threats, get complete perspectives on current status, and provide transparent and thorough updates to the board.*
- *Board: Ensure that appropriate time is allocated in meeting agendas for management, internal audit, and potentially outside subject matter experts to educate members of the board with a realistic perspective on emerging cyber threats, organizational efforts, and existing vulnerabilities.*
- *CAE: Identify opportunities to educate management and the board on emerging cyber risks and perform routine evaluations of all risk management functions related to cybersecurity.*

These actions could be considered leading practices in facilitating good risk governance and risk management regarding technology risk.

QUESTION 8

Beyond cyber security considerations, how should quantum computing be managed, as an emerging risk, in the context of broader technology lifecycle management?

A: Currently, cyber security considerations are the primary risk arising from quantum computing. Other associated risks such as the potential to compromise privacy by having a greater ability to "connect the dots" between different data sources are already covered through artificial intelligence-related risks. Quantum computing simply elevates the likelihood of these risks occurring.

ADVANCED ANALYTICS

QUESTION 9

Do the proposed principles appropriately capture elevated risks that come with the use of AI/ML techniques? Are there any additional principles or risks that OSFI should consider?

A: We believe the proposed principles are sufficiently broad so as to encompass the key risks.

QUESTION 10

With respect to AI/ML models, do you foresee any additional challenges with FRFI self-assessment against the principles of accountability, explainability and soundness (including auditability and fairness) that may be incorporated in future, revised guidance? Please elaborate.

A: The term, "Auditability," is not defined in this document. The IIA would propose that the definition of Assurance Services from the IPPF could serve as a basis for defining "auditability." The definition of Assurance Services is "An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements."

QUESTION 11

Can you describe what levels of explainability are appropriate across the range of AI/ML uses and/or underlying technique complexities?

A: According to The IIA's supplemental guidance, "Auditing Model Risk Management,"

> *Effective governance, policies, procedures, and controls are essential components of a successful MRM framework. Without proper oversight and guidelines, it is difficult to ensure that the model development, implementation, validation, and use processes are operating as intended.*
>
> *Ultimately, the board is responsible for oversight of the MRM framework. However, the development and detailed execution is delegated to senior management.*

Organizations should formally document policies and procedures related to the MRM process. These policies and procedures are typically drafted by senior management and approved by the board, and they should meet the following criteria:

- *Cover the entire MRM process.*
- *Be written in a detailed manner to reduce the need for interpretation and increase uniform execution throughout the organization.*
- *Establish documentation standards for all key activities in the three model risk management areas of activity.*
- *Define MRM roles and responsibilities across the organization.*
- *Define the model risk assessment framework and process.*
- *Establish control standards for models.*
- *Require the creation and maintenance of an organizationwide model inventory.*

QUESTION 12

What is needed to minimize (or manage) reputational risks stemming from the use of AI/ML?

A: In our experience, sound governance over AI/ML is required to ensure its use is appropriate and aligned with the entity's business objectives and risk appetite.

THIRD PARTY ECOSYSTEM

QUESTION 13

Do the proposed principles for technology third party risk management adequately capture both current and emerging risks? What additional principles would you propose?

A: According to The IIA's supplemental guidance, "Auditing Third-party Risk Management," risk appetite is a key factor in adequately managing the risk associated with third-party arrangements and should be included in any risk assessment as follows:

> *When an organization agrees to pursue a strategy that involves engaging a third party, management should clearly communicate the minimum standards required regarding the capabilities of the candidate(s) in terms of governance, risk management, and internal control for the third party to stay within the limits of the organization's risk appetite. If an organization struggles with imposing their "minimum standards" of internal control and risk management on third parties they wish to engage, this can affect the risk exposure at the organizational level. If the organization uses a third-party risk management framework, internal auditors can assess whether each third party it audits complies with the organization's stated or implied risk appetite and whether minimum standards are enforced.*

QUESTION 14

How can OSFI's existing third party risk management guidance (Guideline B-10) be strengthened in view of current trends in technology-related third party arrangements? Do technology-related third party arrangements warrant separate treatment from traditional outsourcing requirements? If so, why? How should OSFI approach developing these separate expectations?

A: For simplicity and efficiency, the additional risk and control considerations associated with technology-related third party arrangements could be satisfied through an annex or revisions to the existing guideline (B-10). Language in B-10 could be strengthened to make it explicit that, in evaluating the performance of outsourced service providers, the outsourcer should apply the same standards that OSFI would expect of in-house technology operations.

QUESTION 15

Do you believe that additional, specific regulatory guidance on cloud risk management is warranted? If so, what elements should it address?

A: According to The IIA's supplemental guidance, "Auditing Third-party Risk Management," organizations should consider their "right to audit" their data, especially when data are contained in a public or private cloud. The supplemental guidance states:

> *An organization's standard contract should include a robust right-to-audit clause. If a significant vendor proposes changes to this content within the contract, management should consult the internal audit activity and/or any other auditor it relies on to perform third-party audits, prior to acceptance if feasible. Management and internal audit may choose to waive their right to audit; however, it is a leading practice to have such language included in the contract in the event of an occurrence suggesting an audit may be in order. The right-to-audit clause should be clear on who is able to exercise that right and to what extent.*

QUESTION 16

What risk factors should OSFI take into account when assessing relationships between FRFIs and FinTech firms?

A: OSFI should consider the governance and ongoing monitoring in place at the FRFIs to ensure that the objectives of the relationship and work practices (in particular, data sharing and management practices as outlined later in the document) between the FRFI and the FinTech firm are (and continue to be) appropriate and aligned with any privacy or contractual requirements.

DATA

QUESTION 17

What data risks should OSFI take into account as it contemplates changes to its regulatory framework?

A: According to The IIA's recently released "OnRisk 2021: A Guide to Understanding, Aligning, and Optimizing Risk,", Data Governance is an area of increasing risk for organizations. The IIA would like to see the idea of "data privacy" more thoroughly addressed in this document, especially in regard to data covered by the GDPR. We would recommend OSFI consider including more specific language regarding the GDPR Principle 2: Purpose limitation. This principle requires that "Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose. Processing that's done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom." Source: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

For further reference, The IIA addressed increasing data collection, use, storage, security, and disposition in the recently released OnRisk 2021 Risk Audit Tool, "Data Governance."

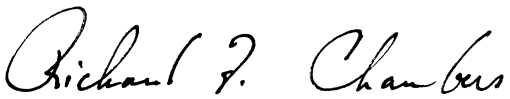
QUESTION 18

In addition to the elements of sound data management described in this paper, what other elements of data management should regulatory guidance consider? Which criteria should be used to determine data risk materiality and how should this inform the level of governance applied in managing these risks?

A: None

Thank you again for the opportunity to provide input on this Discussion Paper. We look forward to further opportunities to assist OSFI in providing guidance to assist federally-regulated financial institutions in identifying and developing resilience to non-financial risks before these risks negatively affect their financial condition. Should you have any questions regarding the comments provided, please do not hesitate to contact Paul Forgues, The IIA Canada's Executive Director, at paul.forgues@theiia.org.

Sincerely,



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President and Chief Executive Officer
The Institute of Internal Auditors

cc: Richard Arthurs, Chair of the Board, The IIA Canada
Tony Malfara, Advocacy Chair, The IIA Canada – Toronto Chapter
Kathy Anderson, Managing Director, Government & Stakeholder Relations
Jeanette York, Director, Financial Services Standards & Guidance