SEPTEMBER 2020

DEVELOPING FINANCIAL SECTOR RESILIENCE IN A DIGITAL WORLD:

SELECTED THEMES IN TECHNOLOGY AND RELATED RISKS

DISCUSSION PAPER

Office of the Superintendent of Financial Institutions Canada
OSFI BSIF

CONTENTS

DEVELOPING FINANCIAL SECTOR RESILIENCE IN A DIGITAL WORLD: SELECTED THEMES IN TECHNOLOGY AND RELATED RISKS

CONTENTS

DEVELOPING FINANCIAL SECTOR RESILIENCE IN A DIGITAL WORLD: SELECTED THEMES IN TECHNOLOGY AND RELATED RISKS

CONTENTS

DEVELOPING FINANCIAL SECTOR RESILIENCE IN A DIGITAL WORLD: SELECTED THEMES IN TECHNOLOGY AND RELATED RISKS

EXECUTIVE SUMMARY

OSFI continues to develop its regulatory and supervisory approaches to technology and related non-financial risks.

The Office of the Superintendent of Financial Institutions (OSFI) Canada supervises federally-regulated financial institutions (FRFIs) and pension plans to determine whether they are in sound financial condition and meeting their requirements. 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. With this objective, OSFI continues to develop its regulatory and supervisory approaches to technology and related non-financial risks. In doing so, OSFI recognizes the imperative for innovation in the Canadian financial sector while protecting the interests of depositors, policyholders, creditors, and pension plan members. Meanwhile, the COVID-19 pandemic has highlighted the need for resilient technology infrastructures and will provide important lessons for industry and regulators alike.

Through this paper OSFI shares some of its thinking and recent work, and invites stakeholder feedback on a range of issues surrounding technology and related risks, including:

- Operational risk and resilience, and the need for a holistic assessment of the overarching regulatory 'architecture' for technology and other non-financial risks;
- Understanding technology risk and the role of prudential regulators with respect to technology and data risk management; and
- Core principles to guide future regulatory guidance development in relation to three priority areas: cyber security, advanced analytics, and the technology third party ecosystem. These are summarized in the graphic below.

CORE PRINCIPLES OF TECHNOLOGY-RELATED RISK BY PRIORITY AREA

CYBER SECURITY
- Confidentiality
- Integrity
- Availability

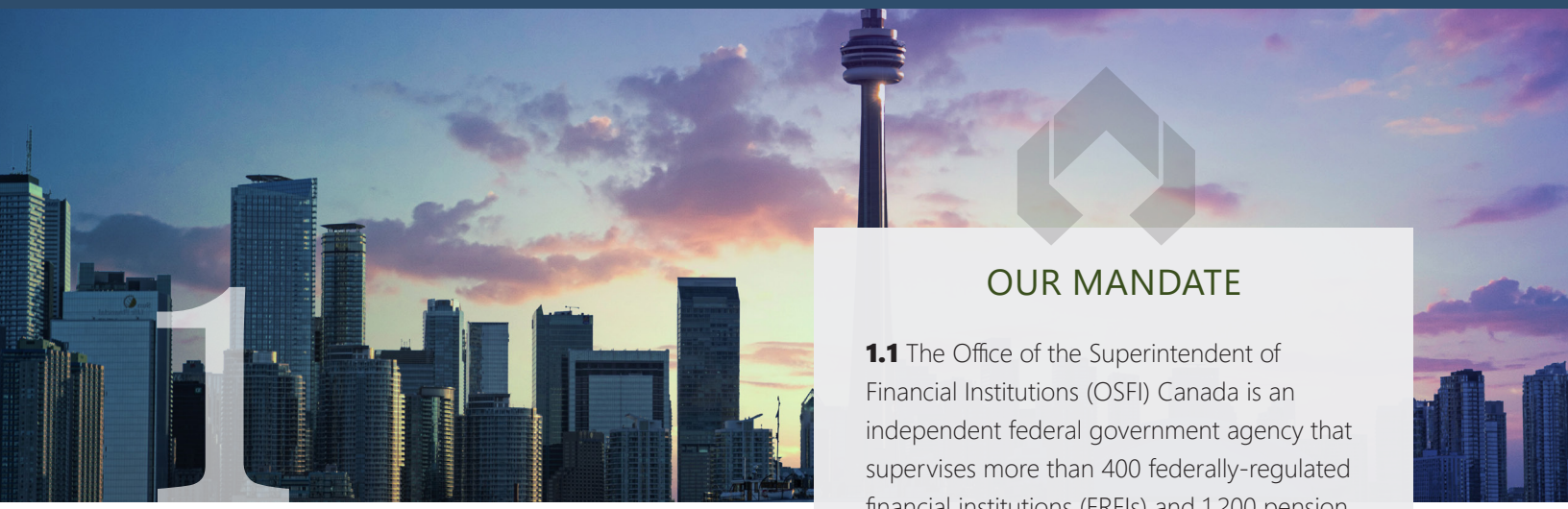
ADVANCED ANALYTICS
- Soundness
- Explainability
- Accountability

THIRD PARTY ECOSYSTEM
- Transparency
- Reliability
- Substitutability

This paper is an opportunity to engage stakeholders in an ongoing discussion on how OSFI can best position its regulatory framework in a complex, rapidly changing digital world. At this time, OSFI is not advancing any firm proposals and intends to follow this consultation process with one or more consultative documents.

All consultation questions are summarized in Annex I, and stakeholders are asked to submit feedback no later than December 15, 2020 to Tech.Paper@osfi-bsif.gc.ca.

> **Meanwhile, the COVID-19 pandemic has highlighted the need for resilient technology infrastructures and will provide important lessons for industry and regulators alike.**



1 INTRODUCTION

1.2 OSFI is a prudential regulator focused on controlling risks that can threaten a financial institution or pension plan's solvency. In short, it is about ensuring the "safety and soundness" of regulated entities.

OUR CONSULTATIVE APPROACH

1.3 In line with strategic goals, OSFI's consultative processes for regulatory guidance are evolving to promote greater transparency and early engagement from stakeholders. This paper is an opportunity for OSFI to share its thinking and invite feedback from interested stakeholders on a range of issues. In turn, this feedback will guide OSFI in developing more concrete proposals to be presented in subsequent consultative document(s) or revised guidance.

OUR MOTIVATION FOR EXPLORING TECHNOLOGY AND RELATED RISKS

KEEPING PACE IN A FAST EVOLVING AND COMPLEX REGULATORY ENVIRONMENT

1.4 Rapid technological advancement and digitalization[1] continue to shape both the global and Canadian financial sector. The COVID-19 pandemic has further accelerated digital transformation and automation within financial institutions, enabled by technology and data.

OUR MANDATE

1.1 The Office of the Superintendent of Financial Institutions (OSFI) Canada is an independent federal government agency that supervises more than 400 federally-regulated financial institutions (FRFIs) and 1,200 pension plans to determine whether they are in sound financial condition and meeting their regulatory requirements. OSFI's mandate is to protect depositors, policyholders, creditors and pension plan beneficiaries by:

- **DEVELOPING A REGULATORY FRAMEWORK TO MANAGE AND MITIGATE RISK;**
- **ASSESSING THE SAFETY AND SOUNDNESS OF FRFIs AND PENSION PLANS; AND**
- **INTERVENING PROMPTLY WHEN CORRECTIVE ACTIONS ARE NEEDED.**

Financial institutions, markets, and infrastructures are more tightly-linked than ever and depend critically on the resilience of different players and processes within the broader financial system. Entities operating within this ecosystem[2] are also changing in nature, increasing in number and concentration, and frequently operate beyond the traditional perimeter of prudential regulation.

1.5 Innovative financial technologies (FinTech), globalization, and other external factors have been influencing firms' business models and risk profiles since the adoption of computing and the Internet in commerce. Although these forces are known, they are generating new (non-financial) risks today and are amplifying risk in traditional (financial risk) areas of prudential oversight.

[1] "Digitalization" generally refers to the use of digital technologies and data by organizations to transform their business models.

[2] This refers to the system of interactions and dependencies between traditional (regulated) financial sector entities and other (non-regulated) entities they do business with.

ENHANCING FRFIs' PREPAREDNESS AND RESILIENCE TO NON-FINANCIAL RISKS

1.6 OSFI's *Strategic Plan 2019-2022* aims to ensure that FRFIs[3] are better prepared to identify and develop resilience to so-called "non-financial risks[4]" before these risks negatively affect their financial condition. With this goal, OSFI is continuing to develop its regulatory and supervisory approaches to technology and related risks.

1.7 Information and communications technology (ICT) underlies virtually all aspects of the financial sector. While technology is a key enabler for financial institutions, its widespread use also poses risks in many different areas of the business. In addition to considering technology risk itself, this paper touches on a number of technology-related themes, including three priority risk areas:

- CYBER SECURITY;
- ADVANCED ANALYTICS (I.E., ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) MODELS); AND
- THE THIRD PARTY ECOSYSTEM.

1.8 These three items are areas in which OSFI has observed an increasing number of incidents (e.g., data breaches, technology outages), shifts in the severity of risk, and emerging risks that both FRFIs and regulators should better understand (e.g., artificial intelligence and quantum computing). Across all technology risks, OSFI has identified sound data management and data governance as critical considerations.

1.9 Consistent with its principles-based regulatory approach[5], OSFI is advancing core principles for each priority risk area, on which more detailed expectations for sound risk management can be developed.

STRUCTURE OF THE DISCUSSION PAPER

1.10 This paper is organized in eight sections. Section 2 focuses on understanding technology risk and its relationship to operational risk and resilience, and relating the role of prudential regulators to existing ICT risk frameworks. Section 3 provides an overview of preliminary core principles, which are expanded on in subsequent sections.

1.11 Sections 4 through 7 address, respectively: cyber security, advanced analytics, the third party ecosystem, and data. Data is foundational to each theme of this paper, and so this paper concludes with a separate discussion on data risk management. Each thematic section presents OSFI's perspective in the area and, where applicable, OSFI's existing regulatory guidance and supervisory work. In turn, OSFI is interested in receiving stakeholder feedback based on questions posed in each section.

1.12 Section 8 invites stakeholders to participate in this consultation, provides instructions and the timeline for making submissions, and shares information on next steps in the consultation process.

3 While this paper refers to financial institutions (e.g., banks and insurance companies) throughout, federally-regulated pension plans often face similar risks and therefore the themes raised in this paper may apply to pension plans as well.

4 These include risks that are not considered to be traditional financial risks (e.g., operational risk, technology risk, culture and conduct risk).

5 By emphasizing principles over prescription, OSFI focuses on achieving positive risk outcomes at FRFIs rather than formal compliance with detailed rules.

UNDERSTANDING TECHNOLOGY RISK

ALIGNMENT WITH OPERATIONAL RISK MANAGEMENT

2.1 Many financial institutions and regulators assess technology risk within a broader operational risk management (ORM) framework. This reflects established guidance from international standard-setters[6] and OSFI's supervisory experience, and also takes advantage of existing structures, processes, policies and procedures within FRFIs.

2.2 OSFI Guideline E-21 (Operational Risk Management) addresses key expectations and principles, such as the three lines of defense, and many of the tools and processes that FRFIs employ in managing technology and other operational risks, including: risk taxonomies, business process mapping, and scenario analysis.

RELATION TO OPERATIONAL RESILIENCE

2.3 Recent global discussions have identified operational resilience as an area of focus in relation to established ORM and technology risk frameworks. Whereas ORM tends to be process-oriented, operational resilience takes a more outcomes-based approach to a given adverse event. It assumes that operational disruptions *will* occur and encourages financial institutions to consider ways in which the impact of these events might be reduced.

2.4 Authorities, including OSFI, are beginning to assess the merits of an operational resilience perspective, and reassess the adequacy of existing ORM frameworks in relation to operational resilience. OSFI is aware that some FRFIs have already adopted operational resilience programs that are aligned with existing operational risk or technology risk management programs.

2.5 International standard-setting bodies, such as the Basel Committee on Banking Supervision (BCBS), and some national authorities are in the process of articulating operational resilience principles and expectations.

6 For example, the International Association of Insurance Supervisors (IAIS) and the Basel Committee on Banking Supervision (BCBS).

INTERNATIONAL POLICY DEVELOPMENT ON OPERATIONAL RESILIENCE

On August 6, 2020, the Basel Committee on Banking Supervision's Operational Resilience Group (ORG) released a consultative document on Principles for operational resilience for banks. The ORG defines *operational resilience* as "the ability of a bank to deliver critical operations through disruption.[7]" The Committee also released Revisions to the principles for the sound management of operational risk for consultation. As a member of the BCBS, OSFI participates in this work and will be informed by the results of the consultative process.

2.6 Operational resilience is not a "new" concept for FRFIs or supervisors. OSFI's ORM supervisory assessments typically include an expectation that FRFIs be able to withstand, recover, and maintain continuity of critical operations through disruption. At the same time, traditional business continuity risk management (another sub-category of operational risk) does not sufficiently capture the breadth of dependencies across the business; nor does it go far enough in creating a culture in which organizations assume that disruption will occur, and prepare and adapt accordingly.

2.7 A healthy organizational culture is a precondition for developing operational resilience. A resilience perspective draws upon capabilities across ORM, including technology risk management, as well as organizational culture to ensure institutions are able to withstand significant operational disruption.

OPERATIONAL RESILIENCE OF CANADIAN FINANCIAL INSTITUTIONS DURING THE COVID-19 PANDEMIC

Since the outbreak of the COVID-19 pandemic in early 2020, FRFIs have implemented and updated business continuity plans to ensure they are able to maintain their critical operations.
Some key operational adaptations by FRFIs to date include:

- **Requiring a large proportion of their staff to work from home who previously had few or no existing remote working arrangements;**
- **Identifying critical staff and their access requirements (e.g., Remote or on-site), and developing contingency plans if critical staff are unable to work;**
- **Temporarily closing retail branches, with digital or telephone services available as alternatives;**
- **Monitoring and, in some cases, identifying alternatives to third party service providers (including offshore providers) in the event that they are not able to perform key services to the agreed standard;**
- **Developing and implementing tailored communication plans; and**
- **Developing "return to office" plans that prioritize the safety and well-being of staff.**

While most FRFIs have not experienced significant disruptions to their critical operations to date, there are many lessons to be learned from the pandemic across the various dimensions of operational resilience. These relate to governance, technology systems and infrastructure, third party risk management, people, change management, business continuity management, incident management and communications, among other domains.

OSFI will continue to assess technology and cyber risks associated with sustained remote work environments at FRFIs, and to incorporate lessons learned from the pandemic in its regulatory and supervisory frameworks. Respondents are encouraged to reflect on pandemic-related insights in their submissions.

7 Although the ORG's work is focused on deposit-taking institutions, such a definition could apply equally to other regulated entities.

RECASTING THE REGULATORY 'ARCHITECTURE' OF OPERATIONAL RISK AND RESILIENCE

2.8 In line with international discussions, OSFI is assessing the merits of a focus on operational resilience objectives with respect to technology and related risks and believes that a holistic view of ORM and operational resilience is warranted. Preliminary work has begun to explore how operational resilience can be incorporated into OSFI's regulatory and supervisory frameworks.

2.9 The growing importance of technology and other non-financial risks requires an overarching policy framework that clarifies OSFI's expectations across a number of related risk areas. This architecture should also inform decisions as to whether different regulatory approaches should be adopted for different sub-categories of operational risk.

2.10 For example, the rapid pace of technological change calls for more adaptive and agile approaches to communicating risk trends and sound practice in technology and cyber risk. In response, OSFI has developed new supervisory tools to complement regulatory guidance in this area. These are discussed in section 4.

DEFINING TECHNOLOGY RISK

2.11 Broadly speaking, technology plays two important roles. First, technology *enables* business. It allows financial institutions to generate business value, to realize efficiencies in operations, and to effectively manage risk. As such, opportunity costs arise when institutions do not take full advantage of technology. Failure to maintain and invest in technology can also lead to operational disruption (e.g., prolonged slowdown or outage of key systems or business services). Mismanaging technology can even result in failure to achieve strategic organizational goals, at significant financial cost.

2.12 Second, technology *protects* an institution's systems and assets. Specifically, it ensures the confidentiality, integrity and availability of systems and the data contained therein. When technologies and related controls fail, systems and assets are vulnerable to damage or loss.

2.13 Many definitions exist for ICT, or technology risk, both within and outside the financial sector. OSFI is aware that FRFIs may have their own definitions and may capture this risk in different ways in their enterprise-wide risk management function. Regardless of definitions and approach, it is important to consider how technology risk can negatively impact operations and affect related risk areas.

2.14 For its purposes, OSFI has developed a working definition for technology risk that draws upon existing practice and guidance, and which is aligned with operational risk frameworks in the financial sector.

Technology risk is the risk arising from the inadequacy, misuse, disruption or failure of information technology systems, infrastructure or data to meet business needs.

SCOPE AND PRINCIPLES GOVERNING TECHNOLOGY RISK

2.15 Technology risk comprises different sub-risks. These include cyber risk, in regard to system and asset protection, but also an array of sub-risks that relate to technology's enabling role (e.g., risks arising from configuration, outages, and project management). As such, a technology risk taxonomy may encompass such domains as:

- SERVICE MANAGEMENT
- INFRASTRUCTURE MANAGEMENT
- APPLICATION MANAGEMENT
- SECURITY AND ACCESS MANAGEMENT
- PERFORMANCE AND CAPACITY MANAGEMENT
- ASSET CURRENCY AND CONFIGURATION MANAGEMENT
- RELEASE MANAGEMENT
- INCIDENT MANAGEMENT
- PROJECT AND CHANGE MANAGEMENT
- HR AND FINANCIAL MANAGEMENT FOR ICT
- AVAILABILITY, RECOVERY AND CONTINUITY MANAGEMENT

2.16 Technology risk management is also guided by a similarly broad set of principles that respond to different sub-risks. As expanded on in section 4 of this paper, the well known principles of *confidentiality*, *integrity* and *availability* (the "CIA triad") are foundational both to technology risk in general, and cyber security in particular. In addition to the CIA principles, common technology risk principles may include:

- LEAST PRIVILEGE
- RELIABILITY
- MAINTAINABILITY
- SERVICEABILITY
- SCALABILITY
- TRACEABILITY
- AUDITABILITY
- AUTHENTICATION
- AUTHORIZATION
- NON-REPUDIATION

Some of these principles can be applied differently in other contexts, such as *reliability* in third party risk management (section 6). Emerging technologies, such as artificial intelligence (section 5), are also causing industry and regulators to rethink and expand on traditional principles to include *explainability*, among others.

TECHNOLOGY RISK INTERSECTS MANY OTHER RISK AREAS

2.17 The dependence on technology throughout financial institutions' business lines means that technology risk can trigger or amplify other operational and financial risks. For example, a major data breach exposing millions of financial consumer records has the potential to damage a FRFI's reputation and cause financial loss from lost business. Similarly, poorly-executed ICT transformation projects can result in significant financial loss.

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?

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?

QUESTION 3
What factors influence the degree of financial loss exposure that may be generated by technology-related risks?

QUESTION 4
What are your views on OSFI's proposed definition and scope for technology risk?

FRAMEWORKS FOR MANAGING TECHNOLOGY AND RELATED RISKS

EXISTING ENTERPRISE ICT RISK MANAGEMENT FRAMEWORKS

2.18 Internationally-recognized technology standard-setters[8] have established frameworks and guidance for firms to use in managing their ICT systems and assets and have adapted these frameworks over time in response to changes in technology and the external environment.

2.19 OSFI does not endorse any particular framework, and FRFIs are encouraged to use frameworks that are best suited to their business context. At the same time, it is important that chosen frameworks adequately capture the inherent risks FRFIs face, and that robust risk management and controls exist to mitigate these risks.

2.20 To date, OSFI has not developed comprehensive regulatory guidance on technology risk management. International practice varies with respect to the scope and nature of technology risk management expectations. Some jurisdictions have developed comprehensive ICT or technology risk guidelines whereas others have focused on important sub-elements (e.g., cyber security). In contrast, other authorities capture technology and other risks within higher-level frameworks (e.g., operational risk). OSFI is considering the extent to which additional regulatory guidance could be helpful in building FRFIs' resilience to technology and related risks.

TECHNOLOGY RISK SUPERVISION

2.21 OSFI's *Supervisory Framework* addresses technology in two respects. First, it *indicates* that OSFI supervisors take technology into account when scanning a FRFI's external and internal operating environments in order to assess changes in risk profile. Second, it recognizes data/information security and ICT systems as a potential source of inherent operational risk.

8 These standard-setters include, for example: ISO, ISACA, and NIST.

2.22 In recent years, OSFI has conducted technology-related supervisory work in the following areas, across insurance and deposit-taking institutions:

- ICT GOVERNANCE AND RISK MANAGEMENT;
- PATCH MANAGEMENT;
- VULNERABILITY ASSESSMENT AND MANAGEMENT;
- ACCESS MANAGEMENT;
- INCIDENT MANAGEMENT AND RESPONSE;
- ICT ASSET MANAGEMENT, INCLUDING LEGACY SYSTEMS AND DATA;
- CYBER SECURITY AND RESILIENCE;
- ICT PROJECT AND CHANGE MANAGEMENT; AND
- BUSINESS CONTINUITY AND DISASTER RECOVERY.

2.23 In addition to cyber security and resilience, which is covered in section 4, OSFI's supervisory work has identified some common areas where FRFIs can enhance their existing capabilities and practices:

- ICT ASSET MANAGEMENT AND TECHNOLOGY RISK TAXONOMIES;
- ALIGNMENT OF THE ENTERPRISE RISK MANAGEMENT FRAMEWORK WITH THE TECHNOLOGY RISK MANAGEMENT FRAMEWORK;
- IDENTIFICATION OF ROLES AND ACCOUNTABILITIES FOR THE FIRST AND SECOND LINES OF DEFENSE, INCLUDING INDEPENDENT REVIEW AND OBJECTIVE ASSESSMENT; AND
- TECHNOLOGY RISK ASSESSMENTS, MONITORING, AND REPORTING.

QUESTION 5

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

> **The growing importance of technology and other non-financial risks requires an overarching policy framework that clarifies OSFI's expectations across a number of related risk areas.**

3 PRINCIPLES

PRINCIPLES AS A FOUNDATION FOR REGULATORY GUIDANCE

3.1 OSFI favours principles over rules, and makes deliberate choices about where and when to apply rules versus principles in its regulatory framework. Given the rapid pace of technological change, regulators are increasingly challenged to establish lasting, relevant guidance in this area. On one hand, principles are more likely to remain current and retain the features of sound business practice, regardless of prevailing technology trends. On the other hand, regulation must always support robust supervision, and the approach to guidance should be appropriate for the nature of the risks. In some cases, this may call for more prescriptive or rules-oriented expectations.

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.)?

ADVANCING PRINCIPLES IN THREE PRIORITY RISK AREAS

3.2 Based on research, consultations, and supervisory work to date, OSFI has identified three sets of core principles for cyber security, advanced analytics, and the third party ecosystem. OSFI's intent is to use these principles as a basis for building more specific regulatory expectations in these three areas going forward. These principles are expanded on in later sections of this paper.

3.3 The graphic below summarizes the core principles for priority areas, situated between technology and data to illustrate their relative importance and interconnectedness. Sections 2 and 7 on technology risk and data, respectively, discuss these interconnected relationships.

3.4 Focusing regulatory and supervisory efforts on inherent and residual risks (after compensating controls are applied) posed by a technology, versus the technology itself, is OSFI's starting point. It is aligned with OSFI's balanced mandate, its *Supervisory Framework*, and with a principles-based regulatory approach that strives to remain relevant through time.

CORE PRINCIPLES OF TECHNOLOGY-RELATED RISK BY PRIORITY AREA

TECHNOLOGY

Cyber Security Principles

- Confidentiality
- Availability
- Integrity

Advanced Analytics Principles

- Soundness
- Explainability
- Accountability

Third Party Ecosystem Principles

- Transparency
- Reliability
- Substitutability

DATA

OSFI focuses on the inherent and residual risks associated with technology and will neither favour nor discriminate against the use of a particular technology.

CYBER SECURITY

4.1 The pervasive use of technology to collect, store and use data in financial services has been accompanied by ever more sophisticated and frequent cyber-attacks against financial institutions, and third party entities with whom they have business relationships. In addition to malicious attacks, FRFIs are confronted with a host of other cyber events that could jeopardize their information security, undermine public confidence, or otherwise violate internal policies and procedures.

OSFI's EVOLVING ROLE IN CYBER SECURITY

4.2 In 2013, OSFI issued Cyber Security Self-Assessment Guidance that sets out desirable properties and characteristics of cyber security practices. OSFI continues to encourage FRFIs to use this guidance to assess their level of preparedness, and to develop and maintain effective cyber security practices. This guidance can also be used to determine cyber security maturity, and cyber posture and resiliency.

4.3 Although this tool has been in use for a number of years, OSFI still observes gaps in many FRFIs' cyber security policies, procedures and capabilities. More opportunities exist for FRFIs to advance the maturity of their overall cyber security programs. For example, FRFI self-assessments that were valid even a few months ago can become quickly outdated in today's threat environment.

CYBER SECURITY PRINCIPLES

Confidentiality, *integrity* and *availability* are core principles for managing technology and cyber risk that are commonly accepted and provide the foundation for a number of internationally-recognized definitions of cyber security.[9]

Confidentiality: Information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems. This includes means for protecting personal privacy and proprietary information.

Integrity: Information is not improperly modified, or destroyed. Integrity also provides for the authenticity and non-repudiation of information.

Availability: Information is accessible and usable in a reliable and timely manner.

9 For example, the FSB Cyber Lexicon defines *cyber security* as the "preservation of *confidentiality, integrity* and *availability* of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."

4.4 In 2017-18, OSFI conducted a cross-sector supervisory review of cyber resilience. Selected FRFIs were required to respond to a severe but plausible cyber scenario. This work resulted in a number of recommendations communicated to FRFIs to enhance cyber resilience[10] in areas such as cyber risk identification, prevention, detection, response, and recovery capabilities.

4.5 Going forward, OSFI will continue enhancing its approach for assessing technology and cyber risks at FRFIs. This will include cross-sector reviews, intelligence-led penetration testing, as well as more responsive means of sharing information with FRFIs.

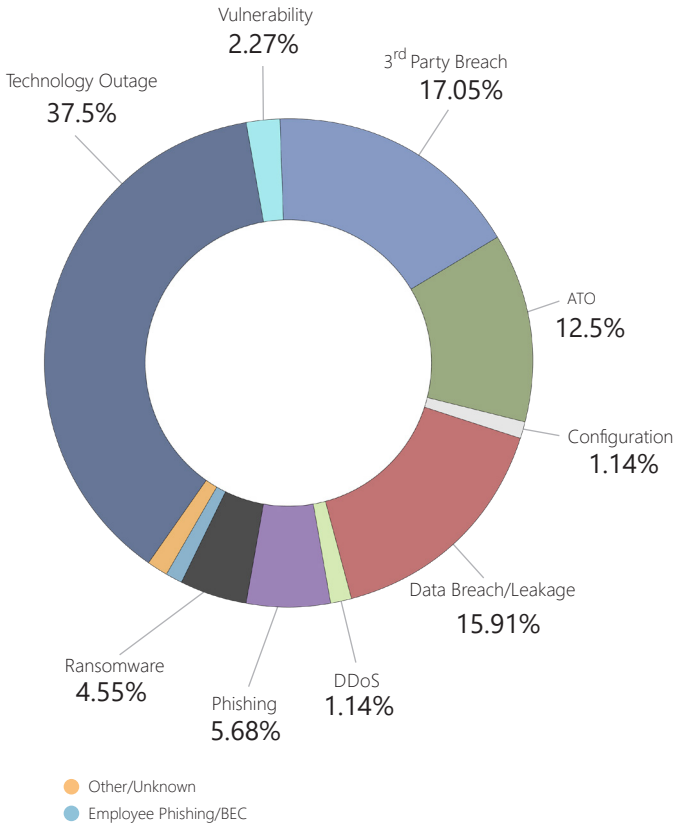
ADVANCING OSFI's ROLE IN TECHNOLOGY AND CYBER SECURITY INCIDENT REPORTING

4.6 In January 2019, OSFI issued an Advisory on Technology and Cyber Security Incident Reporting that sets out OSFI's expectations with respect to FRFI's reporting of technology and cyber security incidents affecting their operations.

4.7 OSFI began tracking technology and cyber incidents prior to publishing the Advisory. The graphic below summarizes the share of major reported incidents that occurred from end-October 2018 to end-June 2020, based on incident type (root cause).

4.8 Apart from data breaches and attacks, technology outages account for a large portion of all incidents. The breadth of incidents emphasizes the importance of an enterprise-wide incident management capability, that is both documented and repeatable, to effectively respond to ICT and cyber incidents.

CYBER AND TECHNOLOGY INCIDENTS REPORTED TO OSFI (OCTOBER 2018 – JUNE 2020)



NEW TOOLS FOR TECHNOLOGY AND CYBER SUPERVISION

4.9 As cyber and technology risks rapidly evolve, OSFI needs to ensure its guidance to FRFIs is responsive to the emerging risks. With this objective, OSFI has developed two types of Bulletins as additions to its supervisory toolkit.

4.10 *Intelligence Bulletins* are a new supervisory tool that OSFI is using to help institutions enhance their readiness for dealing with cyber events, and to better protect the financial sector as a whole. OSFI issued its first Intelligence Bulletin to all FRFIs in August 2019 following a major data breach impacting the Canadian financial sector. It contained a high-level description of the tactics, techniques and procedures used in the data breach, as well as applicable detection and prevention defences for FRFIs to consider.

10 The FSB Cyber Lexicon defines *cyber resilience* as "the ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents." As such, it is related to, but distinct from the concept of *operational resilience* discussed above.

4.11 In addition, OSFI has begun circulating *Technology Risk Bulletins* to FRFIs, which share observations on current *cyber* and technology issues. OSFI uses these bulletins to disseminate sound industry practice in an agile way. OSFI's first bulletin focused on multi-factor authentication. Other topics identified for future bulletins include: Open API; blockchain; and quantum computing. Topics will be informed by incident reporting data from FRFIs, emerging trends in technology and cyber risk, and ongoing supervisory risk surveillance. OSFI expects to circulate these bulletins to FRFIs on a periodic (e.g., quarterly) basis.

4.12 The new bulletins are a form of supervisory communication and are intended to complement OSFI's regulatory guidance (e.g., Guidelines, Advisories). Bulletins are circulated privately with FRFIs, consistent with other supervisory communication.

INTELLIGENCE BULLETINS	TECHNOLOGY RISK BULLETINS
▪ HIGHLIGHT CURRENT CYBER THREATS AND VULNERABILITIES ▪ PROVIDE INSIGHT ON APPLICABLE DEFENCES	▪ SHARE OBSERVATIONS AND SOUND PRACTICE ON KEY CYBER AND TECHNOLOGY ISSUES

Timely supervisory communication that complement regulatory guidance

ENHANCING CYBER RESILIENCE AND COOPERATION

4.13 OSFI's efforts to enhance its capabilities and expectations for technology and cyber risk occur in the broader context of the Government of Canada's National Cyber Security Strategy and in close cooperation with other authorities. This includes the work of the Canadian Financial Sector Resiliency Group (CFRG), which is responsible for coordinating a sector-wide response to systemic-level operational incidents and supporting ongoing resiliency initiatives, such as regular crisis simulation and benchmarking exercises. OSFI also engages regularly with the Canadian Centre for Cyber Security (CCCS). The CCCS shares knowledge about systemic threats, risks and vulnerabilities, and provides situational awareness, technical advice, and guidance.

4.14 OSFI continues to build strong partnerships and evaluate its role and contribution as the Government's legislative framework for cyber security evolves. This includes OSFI's current role in incident reporting, and ensuring timely dissemination of threat intelligence among responsible authorities.

QUANTUM READINESS

4.15 Quantum computing is a new technology that uses principles of quantum mechanics to process information with greater efficiency and power. The application of quantum computing in the financial sector could bring many advantages relative to conventional computing. Use cases range from AI/ML applications to fraud detection and portfolio allocation. Adoption of this technology is expected to yield greater efficiencies in time, effort, and cost.

4.16 The emergence of quantum computing also introduces new risks. From a cyber security perspective, the main threat posed by this technology is the risk that traditional public-key cryptography, on which many information systems rely, can be broken by its speed and computational power. There remains considerable debate regarding the timeframe in which quantum-related threats may materialize, but experts agree that systems should be updated to quantum-safe cryptography sooner, especially those holding high-value, long-life information.

4.17 A sufficiently powerful quantum computer could proliferate traditional attack vectors, such as denial of service (DoS), ransomware, and infiltration into a network to steal private and/or commercially-sensitive information. Malicious actors already conduct harvest-and-decrypt attacks in which encrypted data is accessed, copied, and stored for decryption in anticipation of using a powerful quantum computer.

4.18 Efforts have focused on developing quantum-safe cryptography designed to be resilient against quantum computers. Cutting-edge research on communications techniques using quantum technologies, such as Quantum Key Distribution (QKD), may provide potential solutions to the challenges posed by this technology in the future. To date, sound industry practice has focused on quantum readiness (e.g., developing quantum risk assessment capacity, planning for investment required to transition to quantum-safe cryptography).

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?

QUESTION 8

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

> **OSFI continues to encourage FRFIs to use this guidance to assess their level of preparedness, and to develop and maintain effective cyber security practices.**

ADVANCED ANALYTICS

5.1 The growth of computing power is transforming the ability to analyze more and increasingly diverse sources of data. Advanced analytics, including artificial intelligence (AI) and machine learning (ML), have gone well beyond traditional business intelligence tools to gain deeper insights into customer behaviour to make predictions or to generate recommendations for decision-making. These technological advancements are enabling new products and services, improved efficiencies and reduced costs for financial institutions.

5.2 For the purposes of this paper, OSFI has adopted definitions of AI and ML.

- **ARTIFICIAL INTELLIGENCE** IS THE APPLICATION OF COMPUTATIONAL TOOLS TO ADDRESS TASKS TRADITIONALLY REQUIRING HUMAN SOPHISTICATION (E.G., RECOGNIZING IMAGES AND PROCESSING NATURAL LANGUAGES BY LEARNING FROM EXPERIENCE).[11]
- **MACHINE LEARNING** IS A SUBSET OF AI THAT REFERS TO TECHNOLOGY THAT IS SELF-LEARNING / IMPROVING AND CAN BUILD PREDICTIVE MODELS FROM EXAMPLES, DATA, AND EXPERIENCE, RATHER THAN FOLLOWING PRE-PROGRAMMED RULES.[12]

ADVANCED ANALYTICS PRINCIPLES

OSFI's research, analysis and consultations with FRFIs have identified soundness, explainability and accountability as core principles to manage heightened risks associated with advanced analytics including AI and ML.

Soundness: An AI/ML model is accurate, reliable, auditable and fair by design.

Explainability: The ability to understand and describe the mechanics of the AI/ML model, tool or system and meaningfully explain the results to pertinent parties.

Accountability: Risk management frameworks integrate AI/ML and clear roles and responsibilities are assigned across the institution.

11 Financial Stability Board, "Artificial intelligence and machine learning in financial services," November 2017.

12 CIO Strategy Council, "Ethical design and use of automated decision systems," National Standard of Canada, CAN/CIOSC 101:2019, October 2019.

IMPACT OF ADVANCED ANALYTICS ON MODEL RISK

5.3 While there are numerous benefits and opportunities associated with advanced analytics, their application introduces some new risks and amplifies existing ones. OSFI is primarily interested in FRFIs' application of advanced analytics, including the risks associated with developing, deploying and using AI/ML models.

5.4 OSFI recognizes that what constitutes a "model" in the AI/ML context is not always clear, and so FRFIs may classify some AI/ML methods differently. The principles set forward in this paper, however, can also apply to any AI/ML method that is substantially similar to a model.[13] Regardless of internal classification, it is important that appropriate governance and controls surround the use of AI/ML.

5.5 There is currently no overarching guidance for model risk that applies across industries. OSFI's expectations for model risk management are contained in Guideline B-9 (Earthquake Exposure Sound Practices), Guideline E-23 (Enterprise-Wide Model Risk Management for Deposit-Taking Institutions), and Guideline E-25 (Internal Model Oversight Framework), which pertains to property and casualty insurers. Stakeholder feedback from this discussion paper will inform future work in this area, including whether and how overarching model risk guidance ought to be developed.

ARTIFICIAL INTELLIGENCE / MACHINE LEARNING (AI/ML) MODELS SURVEY AND RESEARCH

5.6 To gain a better understanding of AI/ML model risk, OSFI researched actions taken by prudential regulators and authorities in other jurisdictions to develop regulatory guidance for financial institutions' use of big data and advanced analytics.

5.7 In September 2019, OSFI surveyed a selection of FRFIs across banking and insurance to learn more about their use of AI/ML in modelling.

The survey results pointed to a range of risks, many of which can undermine confidence in an institution, including:

- **MODELS** – INCREASED MODEL RISK, TRANSPARENCY, EXPLAINABILITY, AND PERFORMANCE;
- **RELATED RISKS** – REPUTATION, OPERATIONAL, CYBER SECURITY, AND THIRD PARTY; AND
- **DATA** – GOVERNANCE, QUALITY, SECURITY, BIAS, AND PRIVACY.

PRINCIPLES FOR THE RESPONSIBLE USE OF AI/ML

5.8 OSFI believes that its existing model risk guidance remains relevant, but could be better aligned and strengthened to address increased use of advanced analytics. OSFI is considering whether and how to incorporate additional principles of soundness, explainability, and accountability in its regulatory and supervisory frameworks to address emerging risks resulting from AI and ML.

SOUNDNESS

5.9 Sound models are accurate, auditable, reliable and fair by design. This increases their trustworthiness. Subtle differences in model architecture or inputs can produce unexpected or biased results that may go undetected in systems that are not sound.

5.10 In view of new and heightened risks associated with AI/ML, OSFI has identified several potential areas where the current model risk management framework could evolve to enhance model soundness. These include:

13 For example, some FRFIs identified chatbots as "models" while others did not.

- **DATA MANAGEMENT AND GOVERNANCE** – WITH A FOCUS ON THE QUALITY OF DATA ON WHICH THE ACCURACY AND PERFORMANCE OF AI/ML MODELS RELY (SECTION 7, BELOW, DISCUSSES DATA IN MORE DETAIL).

- **MODEL DEVELOPMENT AND VALIDATION** – EXPLAINABILITY, SIMPLICITY AND RISK TOLERANCE INFORM SELECTION OF THE "RIGHT" MODEL. MODEL TRAINING AND RETRAINING NEED TO ADDRESS KEY TECHNICAL CHALLENGES[14], AND CONTINUOUS MONITORING AND ONGOING REVALIDATION IS IMPORTANT FOLLOWING INITIAL VALIDATION AND DEPLOYMENT.

- **AUDITABILITY** – THE ENTIRE PROCESS USED TO DESIGN, DEVELOP, VALIDATE, DEPLOY AND OPERATE THE AI/ML MODEL SHOULD PRODUCE A DETAILED AUDIT TRAIL TO UNDERSTAND WHAT LED TO THE COMPLEX AI/ML DECISIONS MADE.

- **FAIRNESS** – FAIRNESS SHOULD BE CONSIDERED THROUGHOUT THE AI/ML LIFECYCLE TO MITIGATE AGAINST UNDESIRED AND/OR UNLAWFUL DISCRIMINATION. WHILE PRIMARILY A CONDUCT RISK, A LACK OF REAL OR PERCEIVED FAIRNESS CAN RESULT IN HEIGHTENED REPUTATIONAL, LEGAL AND COMPLIANCE RISKS FOR FRFIs. EFFORTS TO UNDERSTAND, IDENTIFY AND ELIMINATE VARIOUS FORMS OF BIAS (E.G., SAMPLE, MEASUREMENT, ALGORITHM) ARE ALSO IMPORTANT.

EXPLAINABILITY

5.11 A robust approach to achieving model explainability, as identified by OSFI analysis and supervisory work, includes: quality data that are well managed; strong algorithmic interpretability (e.g., relationships between input variables and results are understood and documented); and, transparent processes at all stages of the model lifecycle (e.g., design, develop, validate, deploy and operate), and identification and adherence to model limitations.

5.12 The degree of explainability needed to appropriately manage model risk depends on a number of factors, including the materiality of consequences that could result from erroneous model outputs. Other factors generally considered in determining the level of explainability are: the model application and the regulatory environment within which it will be used; customer and client expectations; and, the extent to which decision-making logic could change[15].

5.13 In the insurance industry, for example, explainability is crucial for AI/ML pricing models in jurisdictions that require regulatory approval to increase premiums. Conversely, explainability is less crucial for an AI/ML model that helps a sales team identify policyholders with lower likelihood of renewing their policies.

ACCOUNTABILITY

5.14 AI/ML applications are complex and are often developed and deployed by multi-disciplinary teams. Absent clear lines of accountability, there are increased risks and potential for unintended negative outcomes (e.g., misuse of models, inadequate model governance and oversight).

5.15 OSFI analysis and supervisory work has identified the integration of an institution's AI/ML processes with its enterprise risk management framework as a key factor in effectively managing risks associated with AI/ML. This includes ensuring that the use of AI/ML applications is aligned with an institution's corporate values, ethical standards and risk appetite.

14 These include: model decay, feature stability, overfitting, input perturbations, interdependencies among models, and precision (exactness) vs. recall (completeness).

15 The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance," January 2020.

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?

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.

QUESTION 11
Can you describe what levels of explainability are appropriate across the range of AI/ML uses and/or underlying technique complexities?

QUESTION 12
What is needed to minimize (or manage) reputational risks stemming from the use of AI/ML?

> **OSFI believes that its existing model risk guidance remains relevant, but could be better aligned and strengthened to address increased use of advanced analytics.**

6

THE TECHNOLOGY THIRD PARTY ECOSYSTEM

6.1 Financial institutions rely on a wide range of third parties in order to conduct their business. Many of these relationships have taken the form of outsourcing arrangements, whereby a third party entity performs a business activity, function or process that is, or could be undertaken by the institution itself.

6.2 While the third party ecosystem captures much more than just technology arrangements, many of the new opportunities and risks presented to FRFIs in this area are technology and data-driven.

MODERNIZING OSFI's APPROACH TO THIRD PARTY RISK MANAGEMENT

6.3 OSFI's expectations on the outsourcing of business activities, functions and processes (Guideline B-10) were first introduced in 2001, and last revised in 2009[17]. Many third party arrangements fall outside the definition of an "outsourcing arrangement" in Guideline B-10, including certain technology and data-related arrangements that are increasingly common today (e.g., data sharing and aggregation). In addition, shifting trends in technology-related third party arrangements merit a review of OSFI's existing expectations for FRFIs and consideration of additional principles.

TECHNOLOGY THIRD PARTY PRINCIPLES

Through analysis and consultations with FRFIs, OSFI has identified transparency, reliability and substitutability as core principles for managing technology-based third party risks.

Transparency: FRFIs are accountable for their business activities[16], functions and processes, including those provided by third parties and should have visibility into the operations of third party providers, and those of their subcontractors.

Reliability: Services provided by third party vendors should be continuously available and perform as expected, while FRFIs are able to sustain operations in the event of service disruption.

Substitutability: Third party technology services can be effectively ported to, and delivered by an alternative provider.

16 While Guideline B-10 generally refers to "activities," other terms (e.g., "services") are also applicable.

17 In 2012, OSFI released a memorandum on new technology-based outsourcing arrangements (e.g., cloud computing) which affirms that expectations in Guideline B-10 continued to apply in respect of these arrangements.

6.4 At the same time, existing principles contained in Guideline B-10 (e.g., FRFIs' accountability for outsourced services, due diligence of service providers) remain relevant.

6.5 OSFI will undertake a separate consultation process related to the expectations contained in Guideline B-10. This will be informed by findings from this consultation, policy discussions at the international level, and OSFI's supervisory work. Of note, OSFI undertook a study of third party risk with a subset of FRFIs in 2019, which included cloud risk management as a key focus area. The summary results of this study are available on OSFI's website.

CLOUD COMPUTING

6.6 Cloud computing usage in the Canadian financial sector continues to increase. As in other sectors, institutions seek to take advantage of the greater security and efficiency that is possible with moving ICT functions to the cloud. The scalability of cloud services also offers flexibility to meet varying business needs of different institutions.

6.7 As a prudential regulator, OSFI focuses on the inherent risks posed by the use of technology, no matter the type, and how institutions manage these risks. While cloud computing offers many advantages, there are certain features of the market for cloud service providers (CSPs) that raise important policy issues for regulators and institutions (e.g., market concentration), discussed below.

CLOUD ADOPTION AND RISK MANAGEMENT

6.8 Through its supervisory work, OSFI observes that cloud adoption at some FRFIs has moved well beyond the proof-of-concept stage and toward "cloud first" onboarding. Cloud-specific standards, governance and oversight mechanisms, however, are still nascent in many instances.

6.9 FRFIs' top challenges with cloud adoption to date include: effective management of cloud migration; adequacy of internal processes for cloud management; and portability of cloud-based services to another CSP. The need for more skillsets to use and support cloud, and resource-intensive legal contract development are also key challenges.

6.10 With respect to service models, software as a service (SaaS) is most common among FRFIs, followed by platform as a service (PaaS). Private cloud is the most common deployment model, followed by public and hybrid cloud. Regardless of the extent of cloud adoption, or the service and deployment models chosen, managing cloud services is a shared responsibility between institutions and CSPs. Under an SaaS model, for example, FRFIs still retain responsibility for data management, and identity and access management, among other things.

6.11 Based on industry developments and practices observed to date, the key risks associated with cloud computing can be summarized as follows:

- **LACK OF SUFFICIENT UNDERSTANDING OF RISKS AND THREATS, COMPLICATED BY THE INVOLVEMENT OF NUMEROUS PROVIDERS IN THE OVERALL SERVICE OFFERING;**
- **LACK OF ADEQUATE CONTROLS FOR DATA PROTECTION, ACCESS AND CONFIGURATION MANAGEMENT;**
- **LACK OF APPROPRIATE OVERSIGHT AND MONITORING DUE TO OVERRELIANCE ON THE CSP; AND,**
- **LACK OF EXIT STRATEGY AS IT PERTAINS TO BUSINESS OPERATIONS, CONTINGENCY PLANNING AND DATA RECOVERY.**

OSFI's supervisory work indicates that some FRFIs have already established, or plan to establish, cloud-specific practices with respect to: risk assessment, security controls, oversight and testing, and exit strategies.

BROADER POLICY ISSUES CONCERNING DOMINANT CSPs

6.12 The global market for CSPs is characterized by several "BigTech" firms[18]. While the scale and sophistication of these firms can be advantageous to FRFIs, they also pose unique challenges. For example, even the largest, systemically-important financial institutions may have less opportunity to customize their contractual arrangements with dominant CSPs. In turn, this may limit transparency and the ability of FRFIs to audit the CSP's practices and assess risk exposures. Moreover, even where contractual terms exist for access and audit rights, experience has shown that they can be difficult to enforce in practice.

6.13 A second issue relates to the concentration of the CSP market and the ability of FRFIs to ensure continuity of critical business functions in the event of a significant outage or failure at a dominant CSP. This scenario underscores the importance of sound business continuity management and operational resilience.

THE INTERACTION OF FRFIs AND FINTECH FIRMS

6.14 The prevalence of FRFI relationships with third party FinTech firms[19] is growing. These firms have a beneficial role to play in the Canadian financial system and either compete or collaborate with FRFIs in offering a range of innovative services to consumers and other businesses.

6.15 In 2018, the Government of Canada finalized amendments to the legislation governing FRFIs that will, once in force, provide FRFIs with greater flexibility to participate in offerings that blend financial and non-financial activities. This includes greater flexibility to network with, and acquire FinTech firms.

6.16 Given this and other developments, the number of FRFI interactions with FinTech entities is expected to increase over time. To date, OSFI has observed technology risk considerations related to cyber security and data management for FRFIs involved with FinTech entities. OSFI continues to monitor trends in this area and work closely with its federal partners as these developments progress.

6.17 OSFI aims to ensure that its regulatory guidance for FRFIs remains current and strikes the right balance between protecting the interests of depositors, policyholders and creditors, and allowing FRFIs to compete effectively and take reasonable risks.

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?

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?

QUESTION 15
Do you believe that additional, specific regulatory guidance on cloud risk management is warranted? If so, what elements should it address?

QUESTION 16
What risk factors should OSFI take into account when assessing relationships between FRFIs and FinTech firms?

18 BigTech firms are large technology companies.

19 FinTech firms have business models that focus on innovative financial technologies.

DATA

7.1 Vast amounts of digital data are produced and processed daily within the Canadian financial sector. In addition to technology, data is a key business enabler for FRFIs. Institutions are harnessing data to create new value, and to effectively manage enterprise-wide risks.

7.2 While managing data is not a new activity, digitalization is altering the scale, speed and impact of data risks that cut across many other risk areas, including cyber security, advanced analytics and the third party ecosystem. Large-scale theft of sensitive financial consumer data, for example, can harm a FRFI's reputation and increase its exposure to legal and compliance risks.

7.3 A key lesson from the 2007-08 Global Financial Crisis is that financial institutions were unable to quickly and accurately aggregate risk exposures and recognize risk concentrations across business lines and group entities. The crisis revealed how inadequate ICT and data infrastructures contributed to this failure and identified a need to enhance risk data aggregation and risk reporting within systemically-important institutions[20]. Maintaining sound data management and governance is an important, ongoing task for all financial institutions.

MANAGING RISK THROUGH THE DATA LIFECYCLE

7.4 Like technology risk, OSFI observes that many FRFIs capture data risks within existing enterprise risk frameworks. Risks are often considered with reference to the data lifecycle, which generally comprises: creation and capture, maintenance and processing, usage, publication, retention, and disposal.

7.5 Sound data risk management frameworks account for a range of important elements, such as:

- DEFINED ROLES AND RESPONSIBILITIES FOR DATA GOVERNANCE, INCLUDING A DATA ARCHITECTURE THAT OUTLINES DATA OWNERSHIP, USE, QUALITY ASSESSMENT, RISK AND ASSOCIATED CONTROLS;
- CONTROLS TO LIMIT ACCESS TO DATA TO AUTHORIZED PERSONS AND PURPOSES;
- ENSURING DATA QUALITY, INCLUDING THROUGH DATA VALIDATION AND CLEANSING;
- PROCEDURES FOR ONGOING COMPLIANCE MONITORING; AND,
- PERIODIC STAFF TRAINING AND AWARENESS INITIATIVES.

20 BCBS, "Principles for effective risk data aggregation and risk reporting," January 2013.

7.6 In 2006, OSFI published implementation notes on data maintenance for deposit-taking institutions using advanced approaches to calculating required capital against credit risk and operational risk exposures, pursuant to OSFI's Capital Adequacy Requirements (CAR) Guideline. Both documents set out principles for managing credit and operational risk data at each stage of the data lifecycle.

DEVELOPMENTS INFLUENCING DATA RISK MANAGEMENT

DATA SECURITY AND PRIVACY

7.7 In May 2019, the Government announced two important initiatives. It launched Canada's Digital Charter, which outlines ten principles to guide digital innovation and growth, including the security of personal information and data. It also announced proposals to modernize the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which focus on enhancing individuals' *control* over their personal information and privacy; enabling responsible innovation; and, strengthening enforcement and oversight, while maintaining a principles-based approach.

7.8 The collection and use of consumer data can lead to reputational, legal and compliance risks for FRFIs. In the insurance industry, for example, issues may arise around obtaining consent to collect and use non-insurance consumer data (e.g., from wearable devices)[21] and protecting the security of the collected data.

7.9 The potential impact of financial consumer data exposure or misuse highlights the importance of strong information security and privacy controls. Leading industry practice embeds Security and Privacy by Design principles within enterprise-wide technology architecture, and end-to-end through the data lifecycle.

OPEN API FRAMEWORKS

7.10 Many jurisdictions, including Canada, have either implemented or are contemplating Open API frameworks[22] whereby financial consumer-permissioned data can be leveraged by third party developers to build innovative applications and services. Following the appointment of an Advisory Committee on Open Banking in September 2018, the Government launched consultations and issued a paper on the merits of open banking in January 2019.

7.11 In January 2020, the Government announced that the Advisory Committee will undertake a second phase of work on open banking focused on data security in financial services. This will include working with stakeholders to examine issues such as governance, consumer control of personal data, privacy, and security. OSFI is closely monitoring developments with respect to the adoption of Open API, and associated implications for FRFIs.

QUESTION 17

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

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?

21 IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, February 2020.

22 Related terms include "open banking" and "consumer-directed finance."

8

BUILDING FINANCIAL SECTOR RESILIENCE IN A DIGITAL WORLD: AN ONGOING DISCUSSION

8.1 Stakeholder comments on the discussion paper and responses to the questions contained in the sections above are requested by December 15, 2020. Submissions and comments should be sent to Tech.Paper@osfi-bsif.gc.ca.

8.2 In making a submission to OSFI, stakeholders acknowledge that OSFI may incorporate their anonymized feedback in a published summary of consultation findings or similar documents.

8.3 OSFI requests that stakeholders clearly identify the questions they are responding to and to use paragraph references from this paper, where appropriate. Stakeholders are not required to respond to all questions in their submissions.

8.4 In the coming months, submissions will be analyzed against OSFI's aim that FRFIs are better prepared to identify and develop resilience to non-financial risks before these risks negatively affect their financial condition. OSFI may invite stakeholders to participate in further discussions, on a bilateral basis or in a multi-stakeholder forum.

ANNEX 1

LIST OF CONSULTATION 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?

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?

QUESTION 3

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

QUESTION 4

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

QUESTION 5

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

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.)?

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?

QUESTION 8

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

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?

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.

QUESTION 11

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

QUESTION 12

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

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?

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?

QUESTION 15

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

QUESTION 16

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

DATA

QUESTION 17

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

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?

ANNEX 2

GLOSSARY & ACRONYMS

OSFI draws on definitions from a variety of domestic and international sources. These include, for example, the Canadian Centre for Cyber Security and the U.S. National Institute of Standards and Technology (NIST). The FSB Cyber Lexicon is another common source and references other generally-accepted standards and glossaries of terms. OSFI recognizes that some terms may be defined and used differently in certain contexts.

Cryptography
The study of techniques used to make plain information unreadable, as well as to convert it back to a readable form. (*CCCS*)

Cyber event
Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. (*FSB*)

Cyber incident
A cyber event that: i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. (*FSB*)

Cyber resilience
The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. (*FSB*)

Cyber risk
Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a [...] system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the [...] system. (*NIST*)

Cyber security
Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (*FSB*)

Cyber threat
A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security. (*FSB*)

Data breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed. (*FSB*)

Denial-of-Service attack
Any activity that makes a service unavailable for use by legitimate users, or that delays system operations and functions. (*CCCS*)

Distributed-Denial-of-Service attack
An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users. (*CCCS*)

Information and Communications Technology
Encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information. (*NIST*)

KEY ACRONYMS REFERENCED IN THIS PAPER:

AI	Artificial Intelligence
API	Application Programming Interface
ATO	Account Takeover attack
BCBS	Basel Committee on Banking Supervision
BEC	Business Email Compromise
CCCS	Canadian Centre for Cyber Security
CFRG	Canadian Financial Sector Resiliency Group
CSP	Cloud Service Provider
DoS	Denial-of-Service attack
DDoS	Distributed Denial-of-Service attack
FRFI	Federally-Regulated Financial Institution
FSB	Financial Stability Board
IAIS	International Association of Insurance Supervisors
ICT	Information and Communications Technology
ML	Machine Learning
ORM	Operational Risk Management
OSFI	Office of the Superintendent of Financial Institutions
PIPEDA	*Personal Information Protection and Electronic Documents Act*
QKD	Quantum Key Distribution