FINAL
December 14, 2020

OSFI Discussion Paper: Developing Financial Sector Resilience in a Digital World Submission of TECHNATION

TECHNATION welcomes the opportunity to provide its comments on OSFI's discussion paper regarding financial sector resilience in a digital world.

TECHNATION is the authoritative national voice for Canada's $170 billion information and communications technology (ICT) industry. Canada's 36,000 ICT firms generate over 1.1 million jobs directly and indirectly. The ICT industry in Canada also creates and supplies goods and services that contribute to a more productive, competitive and innovative economy and society.

Introduction

OSFI's discussion paper represents a timely and thoughtful overview of the technology and data issues that are fundamental to the resilience of financial institutions in a digital world. As the importance of technology and data continues to grow, it is critical that OSFI, financial institutions and suppliers share a deep understanding of the related risks and how they can be managed.

OSFI has indicated there is need for a holistic assessment of the overarching regulatory 'architecture' for technology. In addition, OSFI is looking to identify core principles that will guide future development of regulatory guidance. We agree with both of these objectives.

It is also clear that a balanced approach is critical. To maintain a healthy and strong financial system, innovation is essential. Financial institutions must innovate if they are to meet the needs of consumers, while remaining competitive in a sector that is increasingly being disrupted by non-traditional businesses.

The importance of innovation is not limited to leveraging technology and data. Financial institutions need flexibility in managing risks. This means freedom to innovate in how risks are mitigated, with a focus on the effectiveness of risk mitigation activities, rather than formal compliance with detailed rules.

Fortunately, OSFI's general approach to regulation – which emphasizes principles over prescription – is consistent with the framework that is needed to keep pace with rapid technological advancement and digital transformation.

As OSFI evaluates what technology and data risk management advice it should provide to financial institutions, we recommend that its approach reflect the following five overarching principles:

1. Technology neutrality. Any regulatory guidance issued by OSFI should be developed so that they are independent of any particular technology. By neither favouring nor discriminating against specific technologies, OSFI will (as much as possible) future-proof its approach – even at a time of rapid technological advancements and digital transformation.

2. Outcome-based guidance. Any guidance issued by OSFI should be developed by identifying the desired outcome, rather than how the outcome is to be achieved. For example, if the exercise of audit rights creates risk in a cloud environment (e.g., confidentiality, security, data availability), financial institutions should have latitude to deploy alternative strategies for achieving an appropriate level of oversight and assurance of the providers' operations (e.g., certification against an industry standards with verification by an independent auditor).

3. Interoperability. Any regulatory guidance issued by OSFI should be interoperable with guidance and regulatory models adopted by financial sector regulators in other jurisdictions, including the United States, the United Kingdom and the European Union. Interoperability does not require that the same exact obligations be adopted (for example, by copying regulatory guidance). Rather, it can be achieved through a regulatory framework with compatible outcomes and in the context of cloud computing can be achieved through adherence to globally accepted, industry recognized frameworks and standards.

4. Proportionality. Any regulatory guidance from OSFI should impose a burden on a financial institution only to the extent that it is proportionate and appropriate in the circumstances of the specific institution. In addition, any regulatory guidance should be applied flexibly so that a financial institution has latitude to take into account its own circumstances, including (i) its size, internal organization and risk profile, (ii) the nature, scope and complexity of its activities, and (iii) the nature of the outsourced services or cloud implementation.

5. Shared responsibility. Any regulatory guidance issued by OSFI should take into account that outsourced service delivery and cloud implementations are built upon a shared responsibility model, with responsibility for the implementation of controls and safeguards allocated between the financial institution and the service provider, and with the allocation of responsibilities varying depending upon the nature of the services being delivered and how these services are used by the financial institution.

In addition to these guiding principles, we believe the following four factors are critical to effective regulatory oversight from OSFI in respect of digital resilience:

1. Internationally-recognized standards. Any regulatory guidance from OSFI should encourage, without prescribing, the adoption of internationally-recognized standards for managing technology and data risks. For example, when developing and implementing security and organization controls in a cloud computing environment a financial institution should have the option, in connection with meeting OSFI's expectations, of adopting adopt controls reflected in the ISO/IEC 270001 family of standards published by the International Organization for Standardization (ISO), the Service Organization Control 2 reports (SOC 2) developed by the American Institute of Certified Professional Accountants (AICPA), or both.

2. Independent certifications or audits. Any regulatory guidance from OSFI should acknowledge that effective due diligence and oversight of a service provider can be satisfied through certifications and audits against industry-recognized standards, such as ISO/IEC 27001 and SOC 2.

3. Risk mitigation advantages of cloud computing services. Any regulatory guidance from OSFI should take into account that cloud computing services often help to reduce risks that are inherent in a customer's operations. The Bank of England's Financial Policy Committee has acknowledged this: "*If configured correctly, cloud services could significantly improve operational resilience of individual institutions, because the scale and expertise of cloud service providers allowed them to build resilience in a way that exceeded the capability of individual firms.*"[1] Advantages of cloud computing services typically include, for example, enhanced business continuity (due to mirrored data storage across servers and data centres, allowing for near instantaneous continuity of service if the event of a failure), enhanced cybersecurity (due to large investments, including in artificial intelligence, to anticipate and prevent attacks) and enhanced maintenance (due to 24x7 monitoring and software updating).

4. Standardization of cloud computing services. Any regulatory guidance from OSFI should take into account that as a general rule cloud computing services cannot be customized to meet the needs of an individual customer or group of customers. By definition, cloud computing services make available to users globally a common, shared solution that relies on the economies of scale achieved through standardization. If OSFI were to mandate that financial institutions use only cloud computing services that satisfy prescriptive requirements, OSFI could be limiting significantly the cloud services that financial institutions can use and the benefits of technology made available through those services.

Frameworks for Managing Technology and Related Risks

QUESTION 5

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

The discussion paper acknowledges that internationally-recognized technology standard-setters have established frameworks for firms to use in managing their ICT systems and assets. The paper also references that these frameworks have been adapted over time in response to changes in technology and the external environment.

The internationally-recognized standard-setters identified in the discussion paper include ISO, AICPA and the National Institute of Standards and Technology (NIST). Rather than endorse any particular framework, OSFI has indicated that it encourages financial institutions to use frameworks that are best suited to their business context. We are supportive of this approach and believe that it will continue to be appropriate in the future. Internationally-recognized technology standards provide a technology-neutral, interoperable framework for managing technology risks that are developed and updated by leading thinkers on managing risks.

[1] https://www.bankofengland.co.uk/-/media/boe/files/record/2018/financial-policy-committee-meeting-november-2018.pdf

Although the existence of international standards makes comprehensive guidance from OSFI unnecessary, OSFI has demonstrated through its self-assessment tools and information bulletins that it has an important role to play in helping financial institutions to manage sub-elements of technology risk.

OSFI's Cyber Security Guidance sets out a self-assessment template that serves as both a checklist of risk mitigation factors and a road map for developing an action plan to remediate deficiencies. It assists financial institutions in determining cyber security maturity, and cyber posture and resiliency, without imposing prescriptive rules. OSFI could enhance its approach to self-assessments by educating and encouraging financial institutions to explore the Canadian Cyber Security Tool, a virtual self-assessment tool[2] developed by Public Safety Canada, Communications Security Establishment and its Canadian Centre for Cyber Security. The tool will launch in January 2021 and is specifically designed for Canadian critical infrastructure owners and operators to take part in a voluntary and easy to use self-assessment that provides the participant with an overview of their organization's operational resilience and cyber security posture, as well as comparative results across their sector.

OSFI's Intelligence Bulletins and Technology Risk Bulletins are also effective at helping financial institutions manage technology and data risks. OSFI uses them to disseminate information and observations on identified risks in a timely and impactful way, again without imposing prescriptive rules.

Principles as a Foundation for Regulatory Guidance

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.)?

OSFI's approach of principles-based regulation continues to be fit for tackling technology and data risks. A principles-based approach is critical to keep pace with rapid technological advancement and digital transformation, while also ensuring that guidance does not unnecessarily (and potentially unintentionally) constrain innovation or the deployment of technology or data by financial institutions.

As explained in our response to Question 5, we believe that the development by OSFI of comprehensive technology risk management guidance is unnecessary. If OSFI considers it to be important to issue additional guidance, the Basel Committee on Banking Supervision has provided an important example of how this can be accomplished using a principles-based approach. The Basel Committee's August 2020 consultative document[3] recognizes that many banks have well-established risk management processes that are appropriate for their individual risk profile, operational structure, corporate governance and culture, and conform to applicable risk management requirements. By building upon existing guidance and current practices, the Basel Committee has proposed "*a pragmatic, principles-based approach to operational resilience that will help to ensure proportional implementation across banks of various size, complexity and geographic location*."

[2] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-en.aspx?utm_source=linkedin&utm_medium=public+safety+canada+%7C+s%C3%A9curit%C3%A9+publique+canada&utm_term=3c4df2d4-a801-4703-9780-b63b281be836

[3] Basel Committee on Banking Supervision - Consultative Document Principles for operational resilience https://www.bis.org/bcbs/publ/d509.pdf

In addition, and as described in our response to Question 5, we recommend that OSFI explore providing value added guidance in the form of self-assessment tools and industry bulletins. Any such tool and bulletins can be developed taking into account the guiding principles that we identified in our introductory comments.

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?

OSFI's cyber security self-assessment tool provides an effective model for regulatory guidance that addresses both current and emerging cyber security risks. It reflects a technology-neutral approach that assists financial institutions in determining cyber security maturity, and cyber posture and resiliency, regardless of the underlying threat.

Opportunities exist for OSFI to enhance its cyber security self-assessment tool. Specifically, we believe that the tool can be used to promote the adoption by financial institutions of globally accepted, industry recognized security frameworks and standards.

There is a myriad of industry agnostic, globally accepted cyber risk management and maturity models that OSFI can recommend to financial institutions as reference points to identify, track, and manage cyber security risks. By adopting globally accepted and up-to-date frameworks and standards, OSFI and financial institutions can focus on their core mandate and competencies, while leveraging expertise from organizations such as the Canadian Centre for Cyber Security (CCCS) to give specific cybersecurity advice and guidance.

OSFI also has an important role to play in placing a spotlight on emerging cyber risks, such as risks arising from quantum computing. Through the continued issuance of information bulletins, OSFI can highlight specific risks and the globally accepted, industry recognized security frameworks and standards that have emerged to address them.

We recommend that OSFI undertake consultations with financial institutions and technology experts prior to issuing future guidance on technology or data risks. Consultations will ensure that there is a shared understanding of the risks and how they can be managed and ultimately improve the effectiveness of the guidance.

QUESTION 8

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

Quantum computing can be managed effectively in the same way that other technology risks are managed – through a technology neutral, principles-based approach that promotes the adoption by financial institutions of globally accepted, industry recognized security frameworks and standards. If appropriate, information bulletins that address quantum computing specifically can be issued.

The importance of globally accepted frameworks and standards is underscored by the current shortage of experts on quantum computing. Gaining access to experts through industry recognized fora will be critical to ensuring that risks associated with quantum computing are effectively managed.

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?

The principles proposed by OSFI – soundness, explainability and accountability – are appropriate for managing risks associated with deploying AI/ML techniques. They provide flexibility for innovation without compromising individual rights or placing unnecessary burdens on individuals, and without relieving financial institutions from needing to stand ready to demonstrate that the models they deploy are accurate, reliable and fair.

How these principles are implemented in practice will be of critical importance. Leveraging and ensuring interoperability with established approaches in other jurisdictions needs to be emphasized.

QUESTION 10

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

For the reasons set out in our answer to question 9, we believe that self-assessment against the principles of accountability, explainability and soundness is appropriate, with OSFI standing ready to consult with stakeholders and issue bulletins on specific areas of related risk.

Self-assessment tools should include a focus on the nature of impacts on individuals. For example, the degree of explainability of an AI model should be proportional to the use case and related impacts on the person concerned.

QUESTION 11

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

Some AI applications can be highly impactful on human life, while others can be trivial. Researchers and developers across the world are creating new applications of AI every day and cover a wide variety of use cases that can range from translation, transcription or text extraction. Understanding the full range of AI, from applications that connote science fiction to mundane examples that make our lives just a little easier, will demonstrate that trying to regulate all AI applications with the same approach is impractical and inefficient.

Policymakers concerned about the opacity of certain AI techniques (e.g., so called “black box” models) should clearly understand whether and how opacity might actually lead to harms, and consider how to address the harms directly, rather than restricting a useful AI technique. One method of addressing opacity might be to require human review and oversight in specific use cases before taking action based on AI output, rather than attempting to regulate technical requirements around opacity.

The inclusion of explainability as a key consideration in an AI governance framework is important. However, as algorithmic transparency remains a technical challenge in some cases, we recommend a more nuanced approach taking into consideration the context for the deployment, and the circumstances when explainability is desirable, versus when explainability is required.

The nature and scope of an explanation must be calibrated to individual circumstances, determined by reference to general principles, rather than prescriptive rules. For example, depending upon the nature of the impact on individuals, it may be sufficient to publish general information about the use of automated decision making, while in other cases a more detailed explanation may be appropriate. The degree of explainability should be proportional to the use case and impact on financial institutions and their customers. For example, a model on credit decisioning should require more transparency versus say a translation service given the impact on institutions and their customers. In addition, and again depending upon the impact on individuals, it may be sufficient to provide basic information about how the automated decision is made, rather than detailed information about the logic, which may be impractical to provide or lead to the disclosure of proprietary information.

The publication of impact assessments or algorithms should not be required by OSFI. The existence of such a requirement would create significant disincentives to innovate, including the loss of confidentiality in respect of proprietary information and trade secrets, and place financial institutions at a significant competitive disadvantage to non-traditional businesses operating in the financial services sector. Additionally, the publication of algorithms will rarely provide meaningful transparency. For many AI techniques, the algorithmic output will not provide insight into the subtle patterns the AI systems may find.

QUESTION 12

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

Reputational risks stemming from the use of AI/ML can be mitigated through strong ethics and strong governance. There needs to be an unwavering commitment to use ethical principles to guide the development and deployment of AI/ML systems. These principles should ensure that AI/ML systems are accurate, auditable, reliable, fair, transparent, secure and accountable.

Financial institutions should be encouraged to consider how any deployment of AI/ML systems is incorporated in their overall decision-making and whether human oversight is necessary in some cases. For example, human review could be incorporated into AI/ML systems if decisions will be made or actions taken that would impact a person’s civil liberties or equivalent human rights, or their safety, economic, or legal status.

Third Party Ecosystems

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?

When considering which principles should apply to third party ecosystems, it is important to acknowledge that some risks are inherent within the operations of a financial institution (or any business). For example, a financial institution's own technology will be unavailable at times – either due to scheduled downtime or an unforeseen interruption – or need to be replaced. OSFI's thinking about third party ecosystems should take into account these inherent risks and acknowledge how cloud computing services can help to reduce them.

The scale and expertise of cloud service providers often allows them to build resilience in a way that exceeds the capability of individual firms. Advantages of cloud computing services often include, for example, enhanced business continuity (due to mirrored data storage across servers and data centres, allowing for near instantaneous continuity of service in the event of a failure), enhanced cybersecurity (due to large investments, including in artificial intelligence, to anticipate and prevent attacks) and enhanced maintenance (due to 24x7 monitoring and software updating).

These observations help to inform our views on the principles identified in the discussion paper: Transparency, Reliability, and Substitutability. While each principle is important for managing technology-based third party risks, it will be important that they be applied in a pragmatic and flexible way.

In the case of the transparency principle, OSFI's expectation should not be that a financial institution will always have visibility into the operations of third party providers, and those of their subcontractors. Rather, the focus should be on the level of assurance the institution has from their providers that appropriate processes and controls are in place to meet their obligations to the institution. An appropriate level of assurance can be given through a broad range of mechanisms, including service dashboards, service level reports, and certifications and audits against industry-recognized standards. While direct audits may be appropriate in some circumstances, because they create operational challenges for service providers (particularly cloud service providers with thousands of customers), risks for the cloud service provider's clients (e.g., confidentiality, data availability and service levels) and significant financial and human resource burdens on financial institutions, they should be exercised only when the alternative mechanisms for providing assurance are inadequate or when reasonable concerns exist about a service provider's compliance with its obligations.

In the case of the reliability principle, OSFI's expectation should not be that a third party vendor's services be "*continuously available and perform as expected*". More appropriate expectations are that a vendor: (i) make commitments to service levels and report on its performance (such as through dashboards), (ii) develop and test business continuity and disaster recovery plans, and (iii) when appropriate, make available to customers opportunities for reducing service interruption (such as through optional service redundancy). As well, OSFI should recognize that managing reliability is a shared responsibility. In the case of many technology services, availability will be directly impacted by the security safeguards and controls implemented by the customer, as well as a customer's decision on whether to purchase redundant processing capacity or other optional services.

In the case of the substitutability principle, differences in the service offerings of third party providers makes it is unrealistic for OSFI to expect that a solution must always be portable to another provider. Rather, OSFI should expect that financial institutions will have the ability to retrieve their data and remotely hosted software programs so that they can implement a contingency plan for migrating to another platform (or repatriating service delivery to their own information technology infrastructure). It is important for OSFI to recognize that the management of this technology risk is not new or unique to cloud computing. The deployment of any third party technology – including within a financial institution's own infrastructure – will entail some risk of service interruption if a technology provider were to stop meeting its obligations. Financial institutions have a long track record of managing this and similar risks.

We recommend the following revisions to OSFI's descriptions of the principles:

- Transparency: Remove reference to "visibility" which implies the need for a direct audit of the third party technology vendor and replace with a need for "assurance" of the vendor's control environment.
- Reliability: Remove reference to "continuously available" (which implies 100% uptime) and replace with the need for a vendor to be able to meet a financial institution's requirements for availability and recovery (typically referred to as "resiliency" in other jurisdictions).
- Substitutability: Remove reference to "portability" and replace with a need for financial institutions to define contingency plans for material applications in the event they can no longer be provided by the third party technology vendor. (This is to avoid an expectation for applications to be designed using a "lowest common denominator" approach wherein they can operate on any service provider's platform without any need for rearchitecting.)

In addition, we recommend OSFI consider adding the principle of "modernization" in the context of managing third party technology risk. This would incent financial institutions to evaluate legacy practices and standards and seek modern solutions that may help them improve their security posture and effectively govern the use of technology across the organization.

We also recommend OSFI consider adding a principle for "shared responsibility" between financial institutions and their third party technology vendors. Unlike a traditional business process outsourcing arrangement where a service provider retains most responsibility for the design and operation of effective controls, third party technology arrangements (such as cloud computing) require both parties (and in some cases, multiple parties) to implement and operate effective controls for security, compliance, and resiliency. Financial institutions remain ultimately accountable, but they can gain the assurance they require on the effectiveness of their third party technology vendors' controls through independent certifications and attestations (e.g., SOC 2).

Finally, although likely encompassed with the "reliability" principle, consideration could be given to specifically calling out the importance of safeguarding information and respecting the rights of individuals.

QUESTION 14

How can 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?

Guideline B-10 sets out a general framework for managing risk, essentially by serving as a checklist of risk mitigation factors. It generally works well for technology-related third party arrangements, including arrangements that are not traditional outsourcings. There are elements of Guideline B-10, however, that lack compatibility with the service delivery models of cloud service providers. This disconnect typically arises where Guideline B-10 sets out prescriptive requirements. By way of example:

1. Guideline B-10 provides that: "*The contract or outsourcing agreement is expected to detail the physical location where the service provider will provide the service.*" In the context of cloud computing, identification of the street addresses from which multi-tenant cloud services are delivered is meaningless, as the location of the data centre at which data is processed does not enhance the ability of a customer or OSFI to maintain access to its data. These access rights, including the right to retrieve customer data, are exercised remotely. Disclosing the physical location of data centres also creates security and operational risks for the customer and service provider – making physical attacks on the service provider's data centres more likely.

2. Guideline B-10 provides that: "*The contract or outsourcing agreement is expected to clearly stipulate the audit requirements and rights of both the service provider and the FRE. At a minimum, it should give the FRE the right to evaluate the service provided or, alternatively to cause an independent auditor to evaluate, on its behalf, the service provided. This includes a review of the service provider's internal control environment as it relates to the service being provided*." As a practical matter, an onsite audit of a data centre does not provide meaningful insight to a financial institution and has the potential to compromise the security of the data of other customers of the cloud services provider. Alternative mechanisms for effectively evaluating service delivery exist, including service dashboards, service level reports, and certifications and audits against industry-recognized standards.

3. Guideline B-10 provides that: "*The service provider should be required to notify the FRE about significant changes in insurance coverage and disclose general terms and conditions of the insurance coverage*." As a practical matter, providing notice about changes in insurance coverage and disclosing related terms and conditions is not a meaningful way to assess risk of large cloud providers, most if not all of whom have material financial resources.

If OSFI decides to revise Guideline B-10, we recommend that these and other prescriptive elements of the guideline be replaced with outcome-based principles. In addition, we recommend that Guideline B-10: (i) clarify the meaning of "material outsourcing" in the context of cloud computing, and (ii) place more emphasis on a financial institution's overall third party risk management framework vendor management practices.

QUESTION 15

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

Consistent with our endorsement of a technology-neutral approach, we do not recommend that OSFI issue specific regulatory guidance on cloud risk management. Technology-neutral guidance through Guideline B-10 continues to be appropriate.

If OSFI nonetheless decides to issue cloud-specific guidance, we recommend that OSFI collaborate with financial institutions and cloud service providers to develop a self-assessment tool that will help financial institutions to evaluate their approach to managing cloud-related third party risk, rather than prescribe what they must do. This tool should be calibrated to align with the five overarching principles for effective guidance that we identified in our introductory comments above:

1. Technology neutrality;
2. Outcome-based guidance;
3. Interoperability;
4. Proportionality; and
5. Shared responsibility.

In addition, the approach to self-assessment should be informed by the four additional factors identified in our introductory comments:

1. Internationally-recognized standards;
2. Independent certifications or audits;
3. Risk mitigation advantages of cloud computing services; and
4. Standardization of cloud computing services.

More broadly, a financial institution should be given the latitude to evaluate its use of cloud computing by looking at all relevant factors, including how a cloud service provider addresses the core risk management principles identified by OSFI and the internal frameworks and processes that the institution has in place to manage cloud-related risk.

The practices of cloud service providers in respect of transparency, reliability and substitutability have strengthened over time:

- Cloud service providers have increased **transparency** by improving their customers' insight into the controls deployed in their environments. In addition to independent verification of compliance with these controls, many cloud service providers also have enhanced their customer-accessible dashboards and provide customers with direct sight into access logs.

- **Reliability** has been enhanced through service level commitments and related performance dashboards, the development and testing of business continuity and disaster recovery plans, and redundant computing capacity and storage, both as an inherent benefit of cloud computing and as an optional service.

- **Substitutability** has been strengthened through providing customers with the flexibility to bring their activities back in-house or move to another provider. This flexibility is enabled by allowing customers to retrieve their data at any time and for any reason and through transition assistance services.

The capacity to manage cloud-related risk within financial institutions has also strengthened. Many, if not most, financial institutions now have internal risk frameworks and processes for assessing and overseeing the consumption of cloud services.

The strengthening of risk management practices – both by cloud service providers and financial institutions – helps to reinforce the importance of non-prescriptive regulatory guidance. We encourage OSFI to focus on the desired outcome of any guidance that it provides on cloud computing, rather than prescribing how risks are to be managed or what provisions need to be in a contract for cloud services. Guidance that reflects this approach has many advantages, as it will keep pace with technological changes and emerging best practices and standards, and avoid creating unnecessary obstacles to innovation or inappropriate red tape or costs for financial institutions.

To discuss this submission please contact: Nevin French, Vice-President, Policy, TECHNATION
nfrench@technationcanada.ca