The Bank of Canada is gathering information from industry and stakeholders to enhance its understanding of the retail payment services ecosystem. This document, including any scenarios, diagrams, and questions, are posed to improve the Bank of Canada's understanding and should not be construed as indicative of any potential legislative or regulatory options.

BANK OF CANADA
BANQUE DU CANADA

Retail Payments Advisory Committee

Operational Risk

July 29 – July 30, 2020

This note is to assist participants in preparing for the July 2020 Retail Payments Advisory Committee (RPAC) meeting. The purpose of this meeting will be to:

1. Build upon the operational risk model outlined in the 2017 consultation paper (see below) and lay out the Bank of Canada's (Bank's) intended approach for operational risk management;
2. Develop a common understanding of the high-level principles of a proposed approach, which will enable more detailed conversation on specific topics at subsequent RPAC meetings;
3. Develop the Bank's understanding of current risk-management practices for risks posed by third-parties, for management of operational risk in cases in which PSPs serve end users in different geographic locations, and for risks related to information and cyber security; and
4. Identify topics for discussion in future consultation (see below).

Questions are provided to help guide preparation for the meeting. Questions should not be viewed as mandatory, nor as exhaustive. They are a starting point for discussion to assist the Bank in gathering information on PSPs' management of operational risk.

The results of this meeting will help shape and guide future engagement with RPAC, and the industry more broadly, on operational risk management.

Objectives and Scope

Operational risk relates to inadequate or failed internal processes, system failures, human errors, or external events that may disrupt or compromise payment services. It can affect the availability, reliability, and security of payment services, and the data and funds they process.

The Department of Finance Canada's 2017 Consultation Paper, *A New Retail Payments Oversight Framework* (the 2017 Consultation), proposed that an oversight framework for retail payment service providers (PSPs) should contain measures that are proportionate to the risks that PSPs pose to the economy and, consequently, that the framework would place an emphasis on protecting end users.

Requirements regarding PSPs' management of operational risk are expected to focus on three objectives:

- **Integrity**: ensuring accuracy of data and integrity of systems;
- **Confidentiality**: protection of data in use, in transit, and at rest; and
- **Availability**: supporting a reasonable level of service reliability.

PSPs will be expected to identify and mitigate all operational risks that may affect their retail payment activities, in particular focussing on these objectives.

Similar to other supervisory frameworks, it is intended for proposed retail payments oversight framework to include the activities of **agents and mandataries, and third-party service providers**,[1] where PSPs will be responsible for managing operational risks arising from and associated with these relationships as if they offered the service or provided the function themselves.

However, the scope of the framework is **not intended to cover**:

- Regulation of **other business activities** that a PSP might perform. In accordance with the functional approach of the framework, operational risk requirements are expected to focus on operational risks that may affect a PSP's payment activities. However, while the PSPs' other business lines are not in scope of the framework, such PSPs will be expected to ensure that their payment activities are appropriately protected from operational risk arising from those other business lines.
- Mitigation by PSPs of **money laundering and terrorism financing risks**. This is within the purview of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), and PSPs that are money service businesses are expected to be registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and to be in compliance with the PCMLTFA.
- **Fraud liability and compensation arrangements**. More broadly, however, fraud is a source of operational risk for PSPs. Notwithstanding that the scope of the framework is not intended to establish liability or compensation arrangements in the event that fraud does arise, it is anticipated that the operational risk requirements would cover the establishment by PSPs of controls to mitigate the occurrence of fraud, including through requirements that IT systems are secure.

The **geographic scope** of application of the proposed framework was not specifically covered in the 2017 Consultation.

- One option, discussed with Finance Canada's Payments Consultative Committee (FINPAY), would be to take a similar approach to that established through recent amendments to the PCMLTFA.
- Under the retail payments oversight framework, an equivalent approach would imply that PSPs would be subject to the requirements of the framework even if they are not physically present in Canada and perform payment functions outside Canada, but are directing and providing payment services to end users in Canada. PSPs with a physical presence in Canada would be subject to the framework's requirements with respect to their clients both inside and outside Canada. If a similar geographical scope of application as described above for the PCMLTFA were applied for the proposed retail payments oversight framework, this would result in a geographical scope of application as outlined in the following table.

Location of PSP	Location of end user	Would the PSP be subject to the framework?
In Canada	In Canada	Yes
In Canada	Outside Canada	Yes

[1] An agent is a person or company who represents and acts for a PSP (the principal) under the contract or relation of agency. An agent is not an employee of the PSP, but rather, a person or company acting with authority to execute specific tasks (e.g. performing payment functions on behalf of a PSP) on behalf of its principal. A mandatary is a person or company to whom a PSP has mandated, charged, or commanded specific tasks to be completed under a contractual relationship. "Mandatary" is a civil law term which is similar to a common law "agent". Third party service provider means a person or entity that, under a contract, provides a payment service provider with a service related to a payment function, e.g., PSPs could outsource elements of their operations to third-party service providers.

Location of PSP	Location of end user	Would the PSP be subject to the framework?
Outside Canada	In Canada	Yes
Outside Canada	Outside Canada	No

- This approach would imply that PSPs outside Canada would only be required to meet the obligations established under the proposed framework (including the operational risk management requirements) for payment services that they provide to end users in Canada, while services provided to end-users outside Canada would be outside scope. PSPs in Canada would be expected to meet the obligations for their whole payments operations.

1. **What are your current practices to manage and mitigate Integrity, Confidentiality, and Availability risks when services are provided by:**
    a. **agents and mandataries; and**
    b. **third-party service providers (i.e. outsourcing).**
2. **What challenges are you aware of, or do you think could arise, with respect to meeting operational risk requirements when payment services are provided to end-users in multiple jurisdictions?**
    a. **How are PSPs dealing with these challenges currently?**

Expectations

This section discusses **concepts** that could be covered within the proposed operational risk expectations for PSPs. **It is not intended to convey the expected drafting or structure of legislation, regulations, or guidance.**

The 2017 Consultation indicated that the operational risk expectations for retail payments would be based on Principle 17 (Operational Risk) of the CPMI-IOSCO *Principles for Financial Market Infrastructures* (PFMI). The consultation also acknowledged that the PFMI, which are international standards, are intended to apply to systemically important institutions, and proposed modifying the requirements to ensure their relevance for PSPs. It was proposed that PSPs would be required to comply with the following standards:

- A PSP should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.
- A PSP's management should clearly define the roles and responsibilities for addressing operational risk and should endorse the PSP's operational risk-management framework. Systems, operational policies, procedures and controls should be reviewed, audited, and tested periodically and after significant changes.
- A PSP should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.
- A PSP should have comprehensive physical and information security policies that address all major potential vulnerabilities and threats.
- A PSP should have a business continuity plan that addresses events posing a significant risk of disrupting operations. The plan should be designed to protect end users' information and payments data

and to enable recovery of accurate data following an incident. The plan should also seek to mitigate the impact on end users following a disruption by having a plan to return to normal operations.

- A PSP should identify, monitor, and manage the risks that end users, participants, other PSPs, and service and utility providers might pose to its operations. In addition, a PSP should identify, monitor, and manage the risks that its operations might pose to others.

The standards proposed in the 2017 Consultation can also be considered from a **functional perspective**. At the broadest level, it is expected that PSPs will be required to:

- Establish an operational risk management framework with the objectives of:
  - Identifying operational risks;
  - Protecting their payment activities from those risks, i.e. establishing protective controls;
  - Detecting operational incidents, i.e., establishing detective controls; and
  - Responding to and recovering from those incidents, i.e., establishing responsive controls.
- Assess and test the framework, and any supporting policies, procedures and controls, and to adopt lessons learnt from those tests to enhance their operational risk management capabilities.

For added clarity, operational risk would capture sub-categories such as cyber security, information security, IT security, etc. Further detail about the concepts that could be covered (in legislation, regulations or guidance) is presented in Attachment 1.

The alignment of operational risk expectations for PSPs with the PFMI (adapted for the retail payment context) provides for a **consistent approach with other regulatory regimes**, in particular the international standards for systemically important payment systems, and the Canadian regulatory requirements for prominent payment systems.[2]

It is also recognized that PSPs may be guided by other standards, including public or industry standards, or requirements in other jurisdictions. In order to minimize conflicting regulatory requirements, it is intended that the operational risk requirements for PSPs will – where appropriate, and taking into account the nature of risks posed by PSPs – align with these. The Bank, working with the Department of Finance, intends to take into consideration, in particular, the following standards:

- European Banking Authority (EBA) Guidelines on ICT and Security Risk Management[3]
- Office of the Superintendent of Financial Institutions Canada (OSFI) Guideline E21 on Operational Risk Management
- National Institute of Standards and Technology (NIST) – Cybersecurity Framework
- Payment Card Industry (PCI) Data Security Standards (DSS)
- COBIT 5 by ISACA
- Critical Security Controls for Effective Cyber Defense by Center for Internet Security
- ISO/IEC 27001 – Information Security Management

[2] Further details of the definitions of prominent payment systems and systemically important payment systems, and the relevant regulatory requirements (which are based on the PFMI), are available on the Bank of Canada website.

[3] These guidelines come into effect in June 2020, and will supersede the EBA *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*

- ISO 31000 – Risk Management

The 2017 Consultation also considered a **risk-based approach** to supervision. With respect to operational risks, policy objectives regarding operational risk management would be expected to be met by all PSPs, but the oversight framework would recognize that the way in which the PSPs meet these objectives would depend on the unique characteristics of the PSPs. As part of the risk-based approach, the Bank may also assess the compliance of certain PSPs with the requirements more closely or more frequently.

3. **Information and cyber security will be captured in the operational risk expectations for PSPs. Are information and cyber security risks covered as part of your operational risk management processes/policies, or do you think of them as standalone streams of work?**
4. **Do members have any concerns about the standards that could be taken into consideration in the development of the operational risk requirements? Are there other standards that should be considered?**

Topics for further discussion

In the next RPAC meeting, the Bank intends to seek RPAC members' views on more specific elements of the operational risk measures to be reflected in the retail payments oversight framework. The Bank and Department of Finance will also consult on the operational risk measures using a number of methods, including the Government of Canada's public consultation process for regulations (*Canada Gazette*), and the Bank's public consultation on guidance.

Specific items that the Bank intends to seek views from RPAC on in the next meeting are:

- Operational reliability objectives;
- Identification of operational risks, including operational risks from third parties (including third party service providers, agents and mandataries);
- Protection from operational risk (including information security and cyber risks) and detection of operational incidents;
- Incident response and business continuity planning;
- Assessment and testing;
- Roles and responsibilities; and
- Human and financial resources PSPs maintain to manage operational risk.

The discussion will build off certain elements reflected in Attachment 1.

5. **Are there additional topics regarding operational risk that the Bank should engage the industry about, or any specific issues related to the items listed above?**

Attachment 1: Operational Risk Concepts

This attachment provides further details about the concepts that could be covered in the operational risk requirements for PSPs, either in legislation or regulations, or in guidance. The attachment also lists a small number of examples of other standards that the Bank and the Department of Finance might take into consideration when developing these concepts. The concepts in this table are not intended to convey the expected drafting, level of detail, or structure of legislation, regulations, or guidance. Neither the concepts set out in this Attachment, or the examples of other standards that might be considered, are intended to be exhaustive.

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
1. A PSP should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.	What an operational risk-management framework should contain, such as the: • Necessary procedures and systems to identify, measure, monitor, and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed. These should include at minimum an incident response and business continuity plan, and policies to address physical, information, and cyber security; and • General principles used to manage operational risk throughout the organization. What the framework should achieve, for example: • Taking a broad view of potential risks (human error, cyber attacks, technical errors, natural disasters, etc.); and • Considering interdependencies (how different parts of the framework work together, whether they are internally consistent, e.g. how the PSP's preventative controls and responsive controls work together). Resources to implement and maintain the framework: • Access to sufficient financial and human resources to identify, monitor and manage operational risks, including to achieve reliability objectives and implement business continuity plans.	PFMI Principle 17.1 OSFI Guideline E21 Operational Risk Management ISO 31000 Risk Management

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
	Factors PSPs should consider when identifying risks: • Plausible threats and vulnerabilities (given their business, technology, physical presence, etc.); • Different potential sources such as human error, natural disaster, system deficiencies, cyber threats, risks from other parts of the PSP's business, etc.; and • Consideration of risks associated with provision of services by agents or mandataries, or third-party service providers. Practical requirements: • PSPs must have a process for reviewing and updating the framework, and the related risk policies, procedures, and systems. The Framework should be applied on an ongoing basis, including when changes are made to the PSP's operations.	
2. A PSP's management should clearly define the roles and responsibilities for addressing operational risk and should endorse the PSP's operational risk-management framework.	Different roles that should be established and the purposes of each. Including: • Roles and responsibilities will range from senior management providing strategic directions through to front-line staff knowing their roles and responsibilities with regards to operational risk (e.g. actions to control risk, responsibilities for reporting events, etc.) and the establishment of a challenge function (of some form) within the PSP; • Define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks, during business as usual as well as during the management of incidents; and • Roles and responsibilities related to third-party services providers, and agents and mandatories. The specific roles that should be assigned may vary based on a PSP's business model and risks.	PFMI Principle 17.2 EBA Guidelines on ICT and Security Risk Management

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
	• For example, larger/more complex PSPs may consider establishing formal separation of responsibilities and a three lines of defence structure. Less complex PSPs may not need as many roles defined.	
3. A PSP should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.	Reliability objectives should include the preservation of, confidentiality, integrity, and appropriate levels of availability. At a more detailed level, specific objectives could include: • Recovery Time Objective (RTO) which is a measure of availability loss; • Recovery Point Objective (RPO) which is a measure of data loss; and • Availability rate (percentage of time the operations are available). Factors to be taken into consideration to determine reliability objectives that are appropriate for the PSP's business needs and risks, such as the PSP's impact on end-users and third parties (e.g. other PSPs, FMIs). Policies and procedures (e.g. mitigation, business continuity, etc.) should be designed to achieve these objectives. PSPs should also consider their reliance on third-party service providers, and agents and mandataries in achieving these objectives.	PFMI Principle 17.3 EBA Guidelines on ICT and Security Risk Management
4. A PSP should identify, monitor, and manage the risks that end users, participants, other PSPs, and service and utility providers might pose to its operations. In addition, a PSP should identify, monitor, and manage the risks that its operations might pose to others.	As part of identifying operational risks (discussed in the first row of this Table), PSPs should consider the risks they might experience from others, and, as necessary, appropriately mitigate those risks. Description of what type of interdependencies a PSP should consider: • End-users; • Other PSPs (e.g. that the PSP provides services to or receives services from); • FMIs (e.g. that the PSP participates in, or provides services to); • Third-party service providers; and • Agents and mandataries.	PFMI Principle 17.7 Elements of OSFI Guideline E21 Operational Risk Management, Principle 4

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
	PSPs should consider the risks that they might pose to others, and take this into account in determining their reliability objectives and incident response and business continuity plans.	
5. A PSP should have comprehensive physical and information security policies that address all major potential vulnerabilities and threats.	Data should be protected from loss and leakage, unauthorized access, and other processing risks, such as inadequate record keeping. PSPs should identify protective (i.e., preventative), detective and responsive controls that address each risk identified. Discussion of how that can be achieved: • Establishing standards for confidentiality, integrity, authentication, authorisation, non-repudiation, availability, and auditability (accountability). • Having sound and robust information security policies, standards, practices, and controls to ensure an appropriate level of confidence and trust in the PSP by all stakeholders. • Having policies effective in assessing and mitigating vulnerabilities in its physical sites from attacks, intrusions, and natural disasters. Cyber and information security risk considerations will also be reflected, including: • Approaches to identifying what type of IT assets, data, and information should be protected from cyber attacks; • Assessment of the risk of and impact from cyber attacks on end users and other interconnected entities; • Ability to detect attempted as well as successful cyber attacks/breaches; and • Procedures and policies on responding to and recovering from cyber attacks/breaches in a manner that achieves the reliability objectives while continuing to provide safe and reliable payment services.	PFMI Principle 17.5 NIST – Cybersecurity Framework PCI DSS COBIT 5 by ISACA Critical Security Controls for Effective Cyber Defense by Centre for Internet Security ISO/IEC 27001 – Information Security Management
6. Systems, operational policies, procedures and controls should be reviewed, audited,	Information on when a review, audit or test is appropriate, as well as what each of those might involve.	PFMI Principle 17.2

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
and tested periodically and after significant changes.[4]	Information about adopting lessons learnt from tests or audits and remediating identified gaps or vulnerabilities. What parts of the operational risk management should be assessed and tested (e.g. the BCP plan, cyber controls, other policies, testing and assessment of protective, detective and responsive controls, etc.). Information on how to develop and conduct tests. The frequency for testing, audit, and review: • Some processes should be tested annually (e.g., BCP, although the parts of the plan that are tested may vary year to year); others might be tested less frequently. • All components of the risk management framework might be audited over a fixed period. • The risk management framework should be reviewed annually. Whether the review, audit or test should be conducted by the PSP or by a third party.	EBA Guidelines on ICT and Security Risk Management
7. A PSP should have a business continuity plan that addresses events posing a significant risk of disrupting operations. The plan should be designed to protect end users' information and payments data and to enable recovery of accurate data following an incident. The plan should also seek to mitigate	PSPs should monitor for and detect operational incidents. The purpose of a business continuity plan: • To have a structured defined plan for responding to incidents if they occur, including incidents that materially disrupt the confidentiality, integrity and availability of the PSP's retail payment activities and of the IT systems and data or information that facilitate its payment functions. Governance of a business continuity plan: • A PSP should explicitly assign responsibility for business continuity planning and management of incidents and devote adequate resources to this planning.	PFMI Principle 17.6 EBA Guidelines on ICT and Security Risk Management

[4] In the 2017 Consultation this Principle was included as part of the expectation that PSPs should define roles and responsibilities for addressing operational risk.

Principles	Concepts that might be covered in legislation, regulations, or guidance	Examples of other relevant standards
the impact on end users following a disruption by having a plan to return to normal operations.	The contents of a business continuity plan: • Business continuity plan should have clearly stated steps to achieve the PSP's objectives regarding its response to and recovery from an incident, in a safe and reliable manner; • Plan should identify and address events that pose a significant risk of disrupting operations and should focus on the impact on the operation of critical infrastructures and services; and • A PSP's BCP should seek to ensure that the PSP can continue to meet service levels in such events, while continuing to provide safe and reliable payment services.	