BANK OF CANADA
BANQUE DU CANADA

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, is intended to improve the Bank of Canada's understanding and should not be construed as indicative of any potential legislative or regulatory options.

Retail Payments Advisory Committee

Operational Risk

August 26 – August 27, 2020

This note is to assist participants in preparing for the August 2020 Retail Payments Advisory Committee (RPAC) meeting. In July, RPAC discussed the objectives and scope of what may be expected of PSPs on operational risk management, and, at a high level, the concepts that could be covered within such expectations. As mentioned during the July RPAC sessions, August RPAC sessions will build on the "Attachment 1" of the July RPAC discussion material; this has been re-attached for reference.

The purpose of this meeting is to help the Bank:

- better understand RPAC members' practices with respect to operational risk management; and
- Identify areas that would require additional interpretation in guidance.

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.

As mentioned in July, risk management standards can be considered from functional perspective. At the broadest level, it is expected that PSPs will be required to establish an **operational risk management framework** such that PSPs can: **identify** operational risks; **protect** their payment activities from those risks; **detect** operational incidents; and **respond and recover** from those incidents. PSPs could also be expected to **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. The structure of this paper follows that functional approach.

Questions for Discussion

Framework

1) The July paper noted that operational risk requirements for PSPs 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.

    a) Following the functional approach of the RPOF, the Bank's supervision with respect to these objectives would apply to a PSP's retail payment activities (and would not apply to other parts of a PSP's business), and in particular to data and systems that are relevant to the provision of those activities. Does this provide sufficient clarity regarding the scope of application for these objectives? If not, what additional information would be of use?
    b) How does your organization determine what is a 'reasonable' level of service availability?

c) Do external factors (such as requirements of other regulators, business contracts with other PSPs, or participation in other systems) drive your organization's targets / ability to achieve objectives in these areas?

Identify

2) The Bank has heard that the (high level) operational risks/events that are of greatest concern to PSPs are:

   - Operational failures, including software and hardware issues, that impact service availability; and
   - Data security and cyber incidents that can impact the integrity and confidentiality of systems and data.

   a) Is this list complete?
   b) What sources through which these risks could materialize are of most concern? (e.g. external vs internal threats; failures associated with third parties?)

3) Common information and cyber security standards recommend the identification of critical assets that must be protected. What methodology does your organization use to identify the assets that are critical to your operations?

Protect

4) The Bank recognizes that resources available to mitigate operational risk are finite. How do PSPs go about prioritising investment in protective controls for the risks they have identified?
   a) How does this factor into choices between protective, detective, and responsive controls?
   b) Does prioritisation of investment in protective controls require your organization to prioritize between achieving confidentiality, integrity and availability? If so, how would your organization go about prioritising the achievement of a particular objective over another?

5) The July paper discussed that confidentiality and integrity of data should be protected in transit, in use, and at rest; this is in line with common standards on information and cyber security.
   a) What are the challenges your organization faces with respect to maintaining confidentiality and integrity when 'in transit'?
   b) How are responsibilities for protection of data in transit established and coordinated across the multiple parties in a payments chain?

Respond and Recover

6) What is your organization's approach to business continuity planning? What types of scenarios does your business continuity plan contemplate?

7) How would your organization manage a return to operations in the event of an incident that involves the compromise of data or systems?

8) Financial and Human Resources: As part of your organization's business continuity planning, do you estimate the amount of financial and human resources that might be required to implement the business continuity plan under various scenarios?
   a) If so, how does your organization go about making those estimates?
   b) Does your organization have arrangements to access financial resources to respond to a significant event that impacts your operations?
   c) How does your organization ensure that those financial and human resources can be accessed reliably in times of crisis, in particular where a third-party is relied upon for their provision?

Questions for written response

During the RPAC sessions, the Bank would like to focus material discussion on the questions set out above. In addition, to further the Bank's understanding of RPAC members' practices with respect to operational risk management, the Bank requests that members provide written responses on the following set of questions that seek more detailed information, including information on the specific practices of individual members.

Responding to these questions is voluntary, but the information will help the Bank and the Department of Finance better understand various business practices in the retail payments ecosystem and reflect them as appropriate in the design of the supervisory framework. Your participation is therefore greatly appreciated. **Please provide any responses to these questions by Friday 4 September.**

The confidentiality of information received will be maintained in accordance with the terms outlined in the RPAC Terms of Reference.[1]

Framework

1) Does your organization use quantitative measures to define operational reliability and performance objectives for your business (e.g., recovery time objective, recovery point objective, availability rate)? If so:
   a) Which measures are used?
   b) Have members adopted quantitative measures regarding preservation of integrity or confidentiality? If so, what are these measures?
   c) What targets are set for each measure used?
   d) What factors are taken into account when setting these targets?
      i) What external factors drive the targets, e.g., other regulation, system membership requirements, objectives of other third-parties?
   e) Are these targets disclosed to customers and/or other third parties?

Identify

2) Processes to identify and assess sources of operational risk can include:

   - Risk self-assessment;
   - Control effectiveness analysis;
   - Internal and external risk event analysis;
   - Scenario analysis;
   - Exposure quantification modelling;
   - Horizon scanning

   a) Does your organization use any of these processes? Are some not relevant? Does your organisation use other practices?
   b) How frequently does your organization conduct its processes?

Protect

3) Physical and information (including cyber) security controls include, at a high level, controls relating to: access to systems and data (including, least privilege, separation of duties, account monitoring and control, access logs); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; reconciliation; media protection; personnel security and screening;

[1] That is, the Bank will maintain the confidentiality of all information it receives from all members, except to the extent that the information may be public knowledge or in the event that the Bank is required by law (including the Access to Information Act) to release the information. The *Access to Information Act* outlines the grounds upon which the Bank can refuse to disclose third-party information. In the event that the Bank receives a request for information supplied by a member, the Bank will consult the third party to ensure that the Bank has a full understanding of the sensitivity of the information, and the member will be provided the opportunity to explain why the information requested is confidential.

automated system and communications protection (including, network port control, boundary defenses, encryption); system and information integrity (including, malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; physical access and monitoring; controls against human error (including four-eyes principle); power, telecommunication, and environmental controls; fire protection; change management processes; and vendor management and access controls.

   a) Are any of the controls listed not relevant to your organization? If so, please explain why.
   b) Are certain protective controls considered to be necessities, and thus your organization would always have them?

Detect

4) What are the key processes or controls that your organization uses to detect if the integrity of data, information, or systems have been compromised?
   a) What controls does your organization use to detect that data, information, or systems have been compromised due to physical operational risk?
5) Does your organization monitor and log unsuccessful cyber attacks?
   a) If so, how is this information used?
   b) If not, what is your reasoning for not doing so?
6) Does your organization participate in cyber threat intelligence sharing groups or networks? Are there such groups that exist or are widely used within the retail payments sector?

Respond and Recover

7) In the event of an operational incident, what would prompt your organization to conduct a detailed investigation, e.g., have pre-determined thresholds or triggers been established? If so, what are these thresholds or triggers?
   a) What does the investigation cover?
   b) Does your organization ever utilize external expertise in your investigations?
8) Does your organization have defined triggers for escalating an incident?
   a) How are these triggers determined?
   b) What is this escalation process?

Assess and Test

9) What kind of tests does your organization conduct of its operational risk controls?
   a) What factors does your organization take into consideration to determine the scope and depth of these tests?
   b) What is the frequency of this testing?
   c) Who conducts these tests?
10) How does your organization test its business continuity plan(s)?
   a) Does this testing consider specific scenarios?
   b) Which stakeholders (internal and external) are involved in this testing?
   c) What is the frequency of this testing?
11) Does your organization audit its operational risk framework? If so:
   a) How is the scope of these audits determined?
   b) What is the frequency of these audits?
   c) Who are the audits conducted by (i.e., internal or external auditors)?

Agents and Mandataries

12) Does your organisation use agents and mandataries to provide payment services? If so, please answer the questions below.
13) What are the main operational risks that your organization faces with respect to agents and mandataries?
14) How does your organization ensure that these risks are managed by the agents and mandataries, where relevant? E.g.,
    a) Does your organization establish policies, standards, or minimum service levels that agents and mandataries must meet?
    b) How are these standards communicated to those parties?
    c) How does your organization monitor fulfilment of these obligations by agents and mandataries?
15) How does your organization ensure that agents and mandataries (where relevant) are able to detect and report operational issues?
16) Do your agents and mandataries need to meet different operational risk management standards depending on which jurisdiction they are in?
    a) If so, how does this affect how your organization manages operational risk associated with the use of agents and mandataries?

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 mandataries. 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 Center 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.[2]	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

[2] 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.	