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 Management Expectations

October 28 – October 29, 2020

This note is provided to assist participants in preparing for the October Interim Retail Payments Advisory Committee (RPAC) meeting, part of which will focus on possible expectations for retail payment service providers (PSPs) in relation to operational risk management. Based on what the Bank of Canada (the Bank) heard from RPAC in July and August, and on other regulators' practices, the following expectations may be appropriate to ensure the policy objectives of operational risk management for PSPs are met.[1]

RPAC members are asked to provide feedback on any part of the possible expectations outlined in this note, particularly as they relate to:

(i) structural or practical barriers that may hamper a PSP's ability to meet these expectations; and

(ii) how the listed expectations may not be sufficient to meet the policy objectives.

Feedback with respect to (i) could include, but would not be limited to, any areas where the possible expectations materially diverge from accepted international standards.

Where possible, members are asked to provide views on the application of the expectations across the industry, as well as feedback from the perspective of their own organisation.

Please note, these expectations have been drafted by the Bank and are still in development. Specific details are provided solely to make the expectations clearer and to facilitate discussion. **These expectations are subject to change based on future consultation and policy considerations. Ultimately, the Government is responsible for proposing legislation and regulations to implement the new oversight framework.**

Unlike previous RPAC meetings, no specific discussion questions are outlined in this note, as the intent of this session will be to walk through the possible expectations and identify concerns participants may have.

[1] Expectations regarding PSPs' management of operational risk are expected to focus on three objectives: integrity; confidentiality; and availability. The oversight framework for PSPs is intended to contain measures that are proportionate to the risks that PSPs pose to the economy and, consequently, the expectations are intended to place a greater emphasis on protecting end users, relative to the oversight of systemically important and prominent institutions.

POSSIBLE EXPECTATIONS

Framework

PSPs could be expected to have an operational risk management and incident response framework (Framework),[2] to enable it to: identify operational risks; protect its retail payment activities from those risks; detect incidents and control breakdowns; and respond to and recover from incidents. This Framework could be expected to be:

- approved by a senior person in the organisation,[3] and by the Board, where the PSP has one;
- documented; and
- communicated to staff and other stakeholders responsible for implementing it.

The PSP's Framework could be expected to support a PSP's achievement of certain operational reliability objectives, in particular, the preservation of: integrity; confidentiality; and appropriate availability of the PSP's retail payment activities and of the systems, and data or information that provide or facilitate the provision of those activities.

- To determine what is 'appropriate' availability, a PSP could be expected to take into account the impact of its non-availability on its end users and on interconnected entities (including other PSPs).
- A PSP could be expected to adopt measurable targets related to its availability objectives, including: recovery time objective; system availability target; and recovery point objective.

A PSP could be expected to establish roles and responsibilities for all aspects of its Framework, including for business as usual, as well as in detection of and response to incidents. The PSP's allocation of roles and responsibilities could be expected to provide for challenge and oversight within the PSP with respect to the management of operational risk, as appropriate for the size, business activities and complexity of the PSP.

A PSP could be expected to demonstrate that it would have access to sufficient financial and human resources to implement its Framework, including its incident response arrangements/plan. Human resources would need to be sufficiently skilled and provided with training.

A PSP could be expected to review its Framework at least annually, following any significant changes to operations or operational risk controls, and following material operational incidents.

Identify

A PSP could be expected to identify and document all plausible operational risks and all plausible sources of those operational risks. The processes a PSP adopts to meet this expectation would need to be appropriate for the size, business activities, and complexity of the PSP.

Plausible sources of operational risk that PSPs could be expected to consider could include, but might not be limited to: internal threats; external threats; employment practices; clients, products, and business practice; damage to physical assets; business disruption and systems failures; execution, delivery, and process

---

[2] The term 'framework' could cover: objectives, roles and responsibilities, systems, policies, procedures, and controls that comprise part of the PSP's management of operational risk.

[3] That is, a person who has accountability for the operation of the PSP and is responsible for decision making within the PSP.

management; third parties – including end users, FMIs, other PSPs, agents and mandataries, and third-party service providers; other parts of the PSP's business; change and change management; human error; and natural disaster and other emergencies.

A PSP could also be expected to identify an inventory of assets that should be protected in order to meet its operational availability objectives (i.e., to preserve confidentiality, integrity, and appropriate availability). In identifying these assets, a PSP may be guided to consider the criticality of the asset to the provision of retail payment activities.

Protect

A PSP could be expected to establish protective controls that mitigate all plausible operational risks in a manner that achieves the objectives of preserving confidentiality, integrity, and appropriate availability.

The PSP's protective controls could be expected to:

- protect the assets that the PSP has identified as critical to the provision of retail payment activities;
- mitigate the likelihood of accidental or deliberate destruction, modification, or disruption to data/information and systems; and
- protect data and information in transit, in use, and at rest.

A PSP could be expected to assess how its protective controls are appropriate for the potential degree of impact that a compromise of confidentiality, integrity, or availability might have on its end users and interconnected entities (e.g., other PSPs) that it provides services to. This assessment could be expected to consider the number of end users and interconnected entities that might be affected.

Access Control

As part of its protective controls, a PSP could be expected to establish access controls that minimise the likelihood of access by unauthorised internal and external parties. The depth of a PSP's access controls (i.e., whether the controls are multi-layered)[4] should be appropriate for the potential degree of impact on retail payment activities due to an unauthorised access to data/information and systems that provide or facilitate the provision of retail payment activities.

A PSP's access control should enable it to:

- mitigate insider threat risks associated with changes in employment status;
- permit only authorised individuals to access data/information and systems;
- track, log, and review access and activity history; and
- log and review maintenance and repair.

Detect

A PSP could be expected to establish controls so that it can detect operational incidents and breakdowns in the effectiveness of operational risk controls. To support this, escalation and decision-making processes in relation to incidents and breakdowns in controls should be established in advance.

---

[4] The concept of "multi-layered" access control is to capture how a single layer of control may not be sufficient depending on the level of criticality of the asset (i.e., data, information and communication technology).

Response and Recovery

Responding to an Incident

PSPs could be expected, upon detection of an incident, to promptly perform an investigation. Such an investigation could be expected to cover: the nature and root cause(s) of the incident; and the impact of the incident on the PSP's retail payment activities, end users, and other PSPs or affected parties.

In the event of an incident, PSPs could be expected to take actions to:

- prevent and/or mitigate further damage to the confidentiality, integrity, or availability, while the incident is being investigated; and
- to remediate vulnerabilities or gaps identified during its response to, and investigation of, the incident.

These actions could be prioritised using a risk-based approach.

It could be expected that a PSP should only return to normal operations if it has verified that the integrity and confidentiality of the data/information and systems have been restored as necessary to safely resume operations.

Roles and Responsibilities for Responding to an Incident

A PSP could be expected to establish roles and responsibilities specifically for incident response. This could include specifying who in the organisation would be responsible for carrying out the tasks of reporting, coordinating, and treating an incident, as well as specifying escalation and decision-making processes. It might be expected that training and testing exercises would be undertaken to verify that these roles and responsibilities could be implemented as expected in the event of an incident.

Incident Response Framework and Business Continuity Plans

As part of its Framework, a PSP could be expected to establish a plan that addresses how it would respond to, and recover from, an incident. This plan would need to be designed to address all events that would be expected to pose a risk to preserving confidentiality, integrity, or availability, or a risk to providing or facilitating the provision of retail payment activities. This could include events that would be expected to make critical people, processes, or systems to be unavailable or impaired for significant periods of time.

It could be expected that the objectives of the plan would be to: identify how a PSP would return to meeting its operational reliability objectives; and facilitate the PSP's return to normal operations. As part of this, it is expected that the plan would need to identify the status of all transactions at the time of the disruption with certainty in a timely manner.

To achieve these objectives, it is expected that the plan might need to address a range of issues, including:

- how the PSP would expect to recover lost or corrupted data, correct data integrity issues, and continue or resume its provision of retail payment activities, following an incident – and how promptly this could be expected to be achieved;
- human and financial resources a PSP would have (or need to access) to enact the plan;
- manual processes or other alternate solutions that a PSP might plan to adopt if primary systems are unavailable; and

- how incident response frameworks or business continuity plans of its third-party service providers are taken into account.

A PSP could also be expected to specify arrangements for implementation of the plan, such as: the trigger(s) for enacting the plan and for escalating the incident; arrangements for reporting and treatment of an incident until closure; and arrangements for coordination with internal and external stakeholders.

Testing and Audit

PSPs could be expected to establish a testing program to validate the adequacy and effectiveness the Framework, and to identify any gaps or vulnerabilities in the Framework. The testing program could be expected to:

- employ a variety of methodologies and practices so that each test is appropriate to validate the adequacy and effectiveness of particular component of the Framework that is the subject of the test; and
- cover all components of the PSP's Framework in a comprehensive manner no less frequently than every three years.

Testing should be based on scenarios of relevant and known potential threats, as well as an adequate set of severe but plausible scenarios. Each test could be expected to be designed to assess whether a PSP could meet its operational reliability objectives in response to these scenarios. Testing could be expected to cover manual workarounds if applicable to a PSP.

Each testing exercise could be expected to:

- involve relevant internal stakeholders and decision-makers;
- consider a PSP's dependencies on external stakeholders such as third-party service providers, agents, and mandataries, and involve those relevant external stakeholders where appropriate.

It could be expected that individual testing exercises should be conducted on a regular basis, at least once a year, as well as prior to significant changes to the PSP's operations.

Following a testing exercise, a PSP could be expected to distill lessons and determine whether additions or modifications to its Framework are needed.

Audits

A PSP could be expected to conduct an internal audit, external audit, or independent review of select components of its Framework (i.e., policies, systems, controls, procedures, and processes) on a regular basis, at least once every two years. These could be expected to be conducted so that so that all components of its Framework are audited or subject to independent review over a period of three years.

The objective of an audit, or independent review would be to assess:

- the degree to which a PSP's policies, systems, procedures, and processes comply with the operational risk requirements established under the RPOF.
- whether the policies and procedures for decision-making, and the PSP's roles and responsibilities are effective in enabling a PSP to meet the objectives of preserving the confidentiality, integrity, and appropriate availability.

For a PSP that has an internal auditor, an internal audit function, or an external auditor, it could be expected that the internal audit or external audit would be conducted by that function or auditor. If a PSP that does not have an internal auditor, internal audit function, or an external auditor, it could be expected

that an independent review would be conducted, by a person (or persons) within the PSP who was independent of the PSP's operational risk management function.

Third-party Service Providers

In cases in which a PSP relies on third-party service providers, a PSP could be expected to conduct due diligence of those providers, covering: the third-party service provider's operational risk practices; and operational risks that the PSP could face from relying on the service provider.

A PSP could be expected to establish operational risk management criteria to consider when selecting and managing third-party service providers. These criteria could include:

- how the third-party service provider informs and consults the PSP prior to making changes to the arrangements with the PSP (e.g. changes to connections with the PSP, products provided to the PSP, storage or use of data);
- arrangements for the third-party service provider to inform the PSP when of breaches to data or other operational incidents; and
- arrangements for the management of the security of external connections.

A PSP's arrangements with its third-party service providers could be expected to include:

- a clear allocation of responsibilities between the outsourcing provider and the PSP; and
- clear terms about ownership and confidentiality of data.

Agents and Mandataries

In cases in which a PSP relies on agents or mandataries, the PSP could be expected to assess whether retail payment activities provided on its behalf by those agents and mandataries comply with the operational risk management requirements established under the proposed Retail Payments Oversight Framework.

A PSP's arrangements with its agents and mandataries could be expected to include:

- a clear allocation of responsibilities between the agent/mandatary and the PSP; and
- clear terms about ownership and confidentiality of data.

Reporting to the Bank

To verify that a PSP is in compliance with expectations, the Bank could ask for documentation or other reports to be provided on a regular (e.g., annual) basis, or following a significant change. This could include, for example:

- the documented Framework, policies, procedures, controls, and roles and responsibilities (e.g., as referred to throughout this note);
- documentation of the PSP's reliability objectives, and reports on the PSP's performance against those objectives;
- documentation or reports concerning the PSP's identification of risks and critical assets;
- reports on the performance and outcomes of reviews and assessments;

- reports on use of third-party service providers, and agents and mandataries, and evidence about the arrangements with, and due diligence conducted on, these parties; and
- reports on the performance and outcomes of testing exercises and audits.