BANK OF CANADA
BANQUE DU CANADA

Operational risk and incident response: At a glance

This supplementary material is intended to provide an overview of the Operational risk and incident response guideline (guideline) and summarizes a payment service provider's (PSP) requirements for operational risk and incident response. It also includes scope considerations and a list of questions to help PSPs assess and achieve these requirements.

This supplementary material does not substitute or modify the guideline. It should be read together with the:

- Operational risk and incident response guideline
- *Retail Payment Activities Act* (RPAA)
- Retail Payment Activities Regulations (RPAR)

This material is intended to help PSPs comply with the operational risk and incident response requirements in the RPAA and RPAR. While this material is primarily directed to PSPs in the early stages of establishing and implementing their operational risk and incident response framework (framework), other PSPs may also find it useful to review.

The considerations outlined in this material are not exhaustive, nor do they cover all regulatory requirements under the RPAA and the RPAR. All PSPs should read and adhere to the RPAA, the RPAR and the guideline.

Understanding operational risk and incident response expectations

This section explains operational risk and your operational risk and incident response requirements in the context of the RPAA.

Operational risk

RPAA defines operational risk as "a risk that any of the following will result in the reduction, deterioration or breakdown of retail payment activities that are performed by a payment service provider: a deficiency in the PSP's information system or internal process; a human error; a management failure; or a disruption caused by an external event."

Incident

RPAA defines an incident as "an event or series of related events that is unplanned by a payment service provider and that results in or could reasonably be expected to result in reduction, deterioration or breakdown of any retail payment activity that is performed by the payment service provider."

Scope

All PSPs subject to the RPAA must meet the operational risk management and incident response requirements. These requirements apply to all your retail payment activities, including any related services provided by a third party.

Proportionality and risk-based approach

The Bank recognizes that the PSP population is highly diverse. You are expected to tailor your risk management and incident response framework to reflect:

- the type of operational risks you face
- the nature and complexity of your operations
- your organization's size and structure
- your technology
- any other relevant factors

Operational risk management and incident response requirements

You must establish, implement and maintain an operational risk management and incident response framework. The framework must be designed to preserve the integrity, confidentiality and availability of your retail payments activities.

To accomplish this, you must:

- identify the operational risks you may face when providing retail payment activities
- protect your retail payment activities from those operational risks
- detect incidents, anomalous events and lapses in the implementation of the framework
- respond to and recover from incidents
- review and test your framework
- manage risks associated with the use of third parties

As part of response to and recovery from incidents, you must meet the incident notification obligations under the RPAA and RPAR. If an incident has a material impact on certain parties, you must notify all materially affected parties and the Bank within 48 hours. For details about these obligations, refer to the Incident notification guideline.

Establishing a framework

This section highlights your operational risk and incident response requirements and lists key questions and considerations to help you meet those requirements.

For more details about each topic, refer to the Operational risk and incident response guideline.

Framework

Your framework must be documented and available. Your framework should also be tailored to your own circumstances and risks. Refer to the **Introduction** and **Section 1. Documentation and availability of the framework** in the guideline for more information.

Key questions and considerations

- Is your framework in writing?
- Do you keep all records related to your compliance with regulatory requirements?
- How do you ensure that your framework is available to the persons who play a role in its implementation and maintenance?
- Has your framework been tailored to your circumstances, including the type and materiality of the risks you face?

- As part of establishing your framework, have you considered the potential impacts of reduction, deterioration or breakdown of your retail payment activities?

Objectives

You must set objectives to preserve the integrity, confidentiality and availability of your retail payment activities and monitor your achievement of those objectives using reliability targets and indicators. Refer to **Section 2. Objectives** in the guideline for more information.

Key questions and considerations

- What are your integrity, confidentiality and availability objectives?
- How do these objectives ensure the integrity, confidentiality and availability of your retail payment activities?
- How do you monitor and evaluate your performance against your objectives?
- Have you set reliability targets and indicators to assess if your objectives are met?

Roles and responsibilities

You must allocate and maintain roles and responsibilities for all aspects of your framework including those outsourced to third parties. Refer to **Section 3. Roles and responsibilities** in the guideline for more information.

Key questions and considerations

- What roles and responsibilities are necessary to ensure that you can effectively mitigate operational risks and respond to incidents?
- Have you defined roles and responsibilities for both the normal course of business and when responding to incidents?
- How do you ensure that there is sufficient oversight and challenge to ensure these roles and responsibilities are performed effectively?
- Have you appointed a senior officer? Your senior officer should:
    - oversee the PSP's compliance with regulatory requirements regarding operational risk, incident response and incident notification
    - make material decisions related to the PSP's management of and response to operational risks and incidents
    - approve the framework, at least annually and following any material change
- If you have a board of directors, is your board also responsible for approving the framework at least annually?

Human and financial resources

You should have timely and reliable access to financial and human resources to establish, implement and maintain your framework. Refer to **Section 4. Human and financial resources** in the guideline for more information.

Key questions and considerations

- What human resources are needed to fulfill the defined roles and responsibilities?
- How do you ensure you have timely and reliable access to those resources, during both the normal course of business and when responding to incidents?
- What skills, training and information are required for human resources (internal or external) to perform their assigned responsibilities?
    - How do you ensure that your human resources receive the necessary information and training?
- What financial resources are needed to establish, implement and maintain the framework, during both the normal course of business and when responding to incidents?

Identify

You need to identify and understand your operational risks, assets and business processes. Refer to **Section 5. Identify** in the guideline for more information.

Key questions and considerations

- What are the operational risks that could cause a reduction, deterioration or breakdown in your retail payment activities?
- What are the potential causes of these operational risks?
- What assets (systems, data and information) and business processes are associated with your retail payment activities?
    - Which assets and business processes need to be available and operating as intended to ensure you can effectively perform your retail payment activities?
- What is the sensitivity and criticality of each identified asset and business process?
    - How important are they to the provision of retail payment activities and achievement of the confidentiality, integrity and accountability of your objectives?

Protect

You are responsible for preserving the integrity, confidentiality and availability of your retail payment activities by mitigating operational risk and protecting the assets and business processes. Refer to **Section 6. Protect** in the guideline for more information.

Key questions and considerations

- What protective elements (systems, policies, procedures, processes, controls or other means) are necessary to mitigate your operational risks and protect your assets and business processes?
- How do you ensure that the protective elements are effective in mitigating operational risks, protecting assets and business processes, and supporting your objectives?

Detect

You must promptly detect and escalate incidents, anomalous events and lapses in the implementation of the framework. Refer to **Section 7. Detect** in the guideline for more information.

Key questions and considerations

- What types of incidents and anomalous events could occur in your retail payment activities?
- What types of lapses could occur in the implementation of your framework?
- How do you continuously monitor to promptly detect these incidents, anomalous events and lapses?
- How do you respond to a detected anomalous event or lapse in the implementation of the framework?
    - What are your escalation and decision-making processes?

Response and recovery

You are expected to use your defined incident response plan to respond and recover from incidents. Refer to **Section 8. Response and recovery** in the guideline for more information.

Key questions and considerations

- What is your plan to respond and recover from incidents?
- Does the response and recovery plan address all plausible incidents, including those involving or detected by a third party?
- Does the response and recovery plan set out how you will:
    - investigate and mitigate the impact of an incident immediately
    - respond and restore retail payment activities, while preserving their confidentiality and integrity
    - escalate, report and coordinate incident response with internal and external stakeholders

    - investigate and address each incident's root cause
    - keep a record of each incident and associated action plans?
- How do you ensure that the Bank and materially impacted end users, other PSPs and clearing houses are notified within 48 hours of incidents with material impact?

Third-party service providers, agents and mandataries

As part of your third-party risk management, you manage the risks associated with the use of third-party service providers, agents or mandataries. Refer to **Section 12. Third-party service providers** and **Section 13. Agents and mandataries** in the guideline for more information.

Key questions and considerations

If you receive services in relation to a payment function from **third-party service providers**:

- What risks do you face from using third-party service providers? How do you manage those risks?
- What would be the impact on your retail payment activities if the service provided by the third-party service provider was impaired?
- What due diligence do you conduct to adequately mitigate the risks associated with outsourcing service(s) to a third-party service provider?
    - At a minimum, is due diligence performed annually and also prior to entering into, renewing, extending or substantially amending a contract?
    - What is assessed as part of due diligence of a third-party service provider?
    - What compensating controls are needed to mitigate risks arising from third-party service providers?
- What roles and responsibilities are necessary to oversee and monitor the performance of third-party service providers?

If an **agent or mandatary** performs retail payment activities on your behalf:

- What risks do you face from using agents or mandataries? How do you manage those risks?
- What due diligence do you conduct to adequately mitigate the risks associated with using an agent or mandatary?
    - What are the minimum criteria that you require a potential agent or mandatary to meet before entering into an agreement with them?
    - Do you assess agents or mandataries annually, at a minimum?
    - What compensating controls are needed to mitigate the risks arising from agents or mandataries?
- What roles and responsibilities are necessary to oversee and monitor the performance of agents or mandataries?

Reviewing and testing the framework

Internal review

You must review your framework at least once a year and before making any material changes, and you should address any gaps or vulnerabilities identified in a review. Refer to **Section 9. Internal review** in the guideline for more information.

Key questions and considerations

- Do you conduct an internal review of your framework at least annually and before any material changes are made?
- Does the internal review assess:
    - the framework's compliance with regulatory requirements

    - its effectiveness at meeting confidentiality, integrity and availability objectives
    - the adequacy of human and financial resources?
- How do you address findings from internal reviews?

Testing

You must test all elements of your framework to identify and address deficiencies. Refer to **Section 10. Testing** in the guideline for more information.

Key questions and considerations

- Do you test your framework?
    - What type of testing do you perform to effectively identify gaps in the framework's effectiveness and vulnerabilities?
    - What is the scope of testing?
    - How often do you perform these tests?
- How do you address findings from testing?

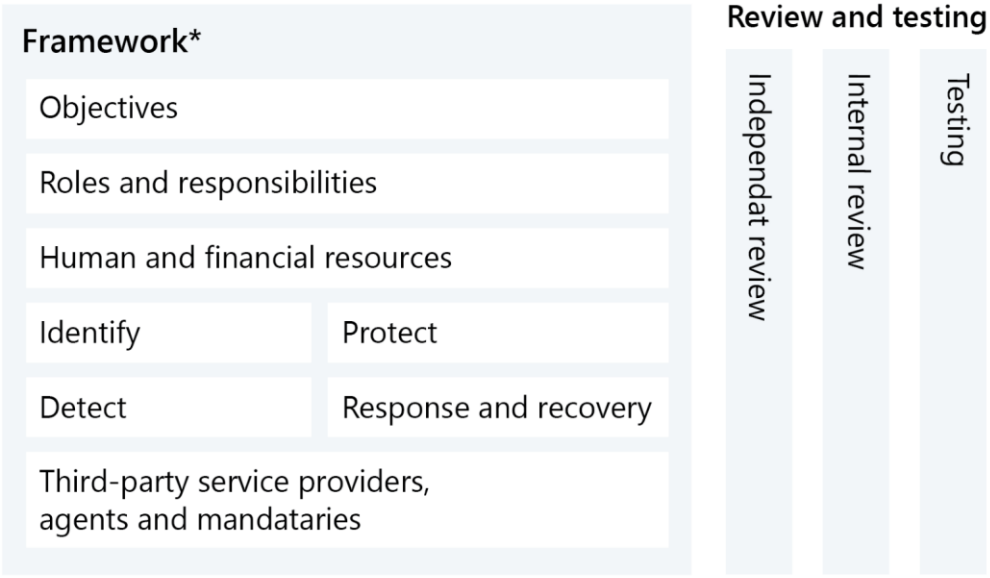
Independent review

If you have an internal or external auditor, an independent review of the framework must be conducted at least once every three years, and you should address identified gaps and vulnerabilities. Refer to **Section 11. Independent review** in the guideline for more information.

Key questions and considerations

- If you have an internal or external auditor, do you ensure an independent review is conducted at least once every three years?
    - Is the independent review conducted by an independent and sufficiently skilled individual?
- Does the independent review assess compliance with section 5 and section 6 to section 9 of the RPAR?
- How do you address findings from independent reviews?

Figure 1: **Risk management and incident response requirements**



*A PSP's framework must be approved and available.