BANK OF CANADA
BANQUE DU CANADA

Draft Guideline - Context

The *Retail Payment Activities Act* (RPAA) and the *Retail Payment Activities Regulations* (RPAR) require payment service providers to meet specific risk management and notification requirements. The RPAA also provides the Bank of Canada with the authority to issue guidelines that set out the manner in which the Bank expects the Act to be applied.

The Bank's guidelines outline the standards and practices that payment service providers are expected to incorporate into their business operations to support their compliance with the RPAA and RPAR.

From February 2024, we consulted industry and stakeholders over a 90-day period to receive their feedback on this guideline.

The consultation is now closed. The Bank thanks those who participated. The feedback received will inform the final supervisory guidelines.

The final guidelines will be published in the second half of 2024, alongside an anonymized summary of the comments received during this consultation.

PSPs can continue to refer to this version of the guideline to anticipate future compliance requirements.

To access all our supervisory policies and guidelines visit https://www.bankofcanada.ca/rps/#resources.

BANK OF CANADA
BANQUE DU CANADA

Operational risk and incident response

Type of publication: Draft supervisory guideline for consultation

Contents

Introduction

This supervisory guideline is intended to help payment service providers (PSPs) that are subject to the *Retail Payment Activities Act* (RPAA) meet their obligations related to operational risk management and incident response.

Outcomes

- A PSP establishes, implements and maintains a risk management and incident response framework to identify and mitigate operational risks and respond to incidents.
- A PSP tailors its framework to its own circumstances and ensures that the framework is commensurate to the materiality of the risks it faces. As part of this, the framework is proportionate to the impact that a reduction, deterioration or breakdown of a PSP's retail payment activities could have on end users and on other PSPs.

Guidance

Operational risk management and incident response requirements

Subsection 17(1) of the RPAA requires that "For the purposes of identifying and mitigating operational risks and responding to incidents, a payment service provider that performs retail payment activities must, in accordance with the regulations, establish, implement and maintain a risk management and incident response framework that meets prescribed requirements."

A risk management and incident response framework (framework) comprises all elements of a PSP's operational risk management and incident response arrangements. This includes but is not limited to systems, policies, procedures, processes, plans, controls, objectives, resources and the roles and responsibilities relevant to operational risk identification, mitigation and incident response.

The framework must be designed to preserve the integrity, confidentiality and availability of the PSP's retail payment activities and of the systems, data and information associated with the performance of those activities. To achieve this, PSPs must:

- identify operational risks that they may face when providing retail payment activities;
- protect against those operational risks;
- detect incidents, anomalous events and lapses in the implementation of the framework;
- respond to and recover from incidents (regardless of their materiality); and
- review and test their framework.

If a PSP uses third-party service providers, agents or mandataries, it must also conduct regular due-diligence assessments of those parties. Using third-party services can offer a PSP efficiencies and other advantages in the provision of its retail payment activities and its management of operational risk. However, it can also create added risks. Consequently, additional operational risk management requirements are associated with managing these relationships.

As outlined in subsection 17(1) of the RPAA, PSPs must establish, implement and maintain all elements described, identified or required in their framework. The Bank expects PSPs to broadly interpret the terms "establish," "implement" and "maintain." For example, "establish" should be interpreted to include the design and development of the framework and its elements; "implement" should be interpreted to include putting the framework into effect; and "maintain" should be interpreted to include ongoing monitoring and updating of the framework.

PSPs must be able to demonstrate their compliance with the RPAA requirements on an ongoing basis, including by retaining documentation in support of their compliance.

Scope of application of the operational risk expectations

All PSPs that are subject to the RPAA must meet the operational risk and incident response requirements established in the RPAA and the *Retail Payment Activities Regulations* (RPAR) and discussed in this guideline. This is regardless of where their systems, data, information or assets are located or where their operations are performed.

According to the RPAA, the Bank's supervision of a PSP's operational risk management and incident response arrangements applies to all of the PSP's retail payment activities. This includes the assets (e.g., systems, data, information and any other assets) and business processes that are associated with or involved in the PSP's performance of those activities. Section 5 (Identify) of this guideline provides further details on the scope of assets and processes that the framework should cover.

Compliance with operational risk management and incident response requirements also applies to any retail payment activities, or related processes or operations, that an employee, third-party service provider, agent or mandatary provides for the PSP. As outlined in section 87 of the RPAA, a PSP or other individual or entity that is subject to a requirement under the RPAA remains liable for a violation that is committed by any of its employees, third-party service providers, agents or mandataries.

If a PSP is part of a group, including international groups, it still must comply with the requirements of the RPAA and demonstrate that compliance to the Bank. A PSP may rely on elements of a related entity's operational risk management and incident response arrangements (including its resources, systems, policies, procedures, processes or controls). For example, a PSP may adopt a framework, or part of a framework, established by a parent entity. However, if doing so results in the PSP being non-compliant with the requirements of the RPAA, the PSP must make changes to the framework or develop supplementary arrangements to ensure compliance.

Risk-based approach and proportionality

The Bank recognizes that PSPs have different operational risk practices, depending on the nature and complexity of their operations, organizational structure, technology and other relevant factors. PSPs should tailor their framework to their circumstances, accounting for these factors and the nature of the risks they face. Subsection 5(2) of the RPAR requires a PSP to ensure that "all aspects of its risk management and incident response framework—including all objectives, targets, systems, policies, procedures, processes and controls—are proportionate to the impact that a reduction, deterioration or breakdown of the payment service provider's retail payment activities could have on end users and on other payment service providers." Subsection 5(2) also requires a PSP to consider factors including ubiquity and interconnectedness when determining the impact of a reduction, breakdown or deterioration of its retail payment activities.[1]

This means that a more ubiquitous and interconnected PSP should adopt a more stringent approach to operational risk management and incident response (referred to throughout this guideline as "proportionality"). This guideline includes examples of when a more stringent approach is expected by the Bank, although these examples should not be considered exhaustive.

---

1 Information the Bank would use to establish a PSP's ubiquity and interconnectedness includes:
- the number of end-users to which the PSP provides retail payment activities;
- the value of end-user funds held by the PSP;
- the value of electronic funds transfers in relation to which the PSP performed a retail payment activity;
- the number of electronic funds transfers in relation to which the PSP performed a retail payment activity; and
- the number of PSPs to which the PSP provides retail payment activities.

1. Documentation and availability of the framework

This section provides guidance on subsection 5(1) and section 6 of the RPAR.

Outcome

- A PSP's risk management and incident response framework is documented and available to everyone who plays a role in implementing or maintaining it.

Guidance

Documentation

1.1 Subsection 5(1) of the RPAR stipulates that PSP frameworks must be in writing.

1.2 However, there is no one-size-fits-all structure for the framework or how it should be documented. PSPs should document their framework in a way that supports the mitigation of their operational risk and their response to and recovery from incidents. Documentation should be:

- sufficiently comprehensive to convey all necessary information to meet its intended purpose (e.g., a documented procedure should cover all steps in the process);
- easily understandable and in a format that is accessible to the stakeholders who will use the documentation (e.g., the PSP's employees or other human resources or, as relevant, agents and mandataries); and
- kept up to date and accurate.

1.3 Appendix B describes examples of the types of documentation that PSPs should consider when establishing, implementing and maintaining their framework.

1.4 Under section 40 of the RPAR, framework documentation must also support PSPs' broader compliance with the record-keeping requirements established in the RPAA. PSPs must retain records to demonstrate and justify their compliance with the RPAA, including how they established, implemented and maintain their framework.

Availability

1.5 A PSP "must ensure that its risk management and incident response framework remains available to all persons who have a role in implementing or maintaining it and must take all reasonable precautions to prevent its unauthorized deletion, destruction or amendment," as outlined in section 6 of the RPAR.

1.5.1 The framework and documentation must be available to relevant staff and other stakeholders when required. For example, PSPs should ensure that incident response and recovery plans and procedures are accessible if an incident occurs.

1.5.2 PSPs should establish, implement and maintain procedures and other means to ensure availability and to prevent unauthorized deletion, destruction or amendment of their documentation. This could include, among other things, access controls, version controls and document storage and retention arrangements.

2. Roles and responsibilities

This section provides guidance on paragraph 5(1)(d) and subsections 5(5) and 5(6) of the RPAR.

Outcomes

- A PSP establishes, implements and maintains roles and responsibilities for all aspects of operational risk management and incident response and recovery, including providing oversight and challenge.
- A PSP monitors the roles and responsibilities outsourced to third parties.

Guidance

2.1 Paragraph 5(1)(d) of the RPAR states that a risk management and incident response framework must "allocate specific roles and responsibilities in respect of the implementation and maintenance of the framework—both in the normal course of business and when detecting, responding to and recovering from incidents." Defining roles and responsibilities establishes accountability and responsibility for operational risk management and incident response within PSPs.

2.2 PSPs should tailor the roles and responsibilities necessary to establish, implement and maintain the framework to their circumstances, including the nature and complexity of their operations. This includes ownership, organizational structures, technology and other relevant factors.

2.2.1 A PSP that is part of a broader group (including an international group) may allocate roles and responsibilities related to the framework outside the regulated entity. Regardless, the PSP remains responsible for ensuring its compliance with the RPAA.

2.3 Unless the PSP is an individual, the allocation of roles and responsibilities should:

- cover all parties who are responsible for establishing, implementing and maintaining the framework. The parties covered will depend on the nature and specific arrangements of the PSP, but should include the senior officer, the board of directors (if any), management, staff and, where relevant, third-party service providers, agents, mandataries, affiliated entities or other third parties;
- allocate responsibility and accountability for each step of establishing, implementing and maintaining the framework;
- be assigned to specific roles (this could include specific teams or business units as well as roles allocated to individuals);
- define responsibility for challenging and overseeing the exercise of each of the allocated roles and responsibilities, as required by subparagraph 5(1)(d)(i) of the RPAR. For example, senior officers, management, or an independent function can provide challenge and oversight;
- respect separation of duties, when necessary, to ensure that an individual does not have control of a process from start to end; and
- include clearly defined reporting lines and, when necessary, escalation paths for issues.

2.4 PSPs should ensure that they have adequate resources to fulfill each role and responsibility (see Human and financial resources).

2.5 According to the principle of proportionality, the Bank expects that more ubiquitous and interconnected PSPs will implement a three-lines-of-defence model.

The senior officer, board of directors and framework approval

2.6 Subparagraph 5(1)(d)(ii) of the RPAR states that unless the PSP is an individual, its framework must allocate responsibility to a senior officer for overseeing:

- compliance with subsection 17(1), section 18 and subsection 19(3) of the RPAA as well as sections 6 to 10 of the RPAR; and
- material decisions that relate to the PSP's identification and mitigation of, and response to, operational risks and incidents.

2.7 Regardless of where they are located, the senior officer should be an employee of the PSP, occupy a specific position within the PSP or report directly to certain persons within the PSP (see section 1 of the RPAR).

2.8 According to subsection 5(6) of the RPAR, the framework must be approved:

- by the senior officer and PSP's board of directors (if any) at least once a year; and
- by the senior officer following each material change.

2.9 PSPs have discretion for determining whether a change is material; however, all significant changes (see supervisory guideline Notice of Significant change or new activity) should be included as material changes. Any major, non-administrative changes in the way that the PSP manages operational risk should also be considered as a material change.

2.10 PSPs must also provide the senior officer with:

- the findings of reviews of the framework for approval (subsection 8(4) of the RPAR);
- the findings of testing (subsection 9(3) of the RPAR);
- independent reviews of the framework (subsection10(3) of the RPAR); and
- information about incidents (subparagraph 5(1)(i)(vi) of the RPAR).

Oversight of third parties

2.11 As outlined in subsection 5(5) of the RPAR, if the framework allocates any roles or responsibilities to a third-party, including any third-party service provider, agent or mandatary of the PSP, the framework must set out systems, policies, procedures, processes, controls or other means for overseeing the third-party's fulfillment of those roles and responsibilities. This should include allocation of responsibility for:

- conducting due diligence assessments; and
- monitoring the delivery of services and the performance of the roles and responsibilities.

3. Human and financial resources

This section provides guidance on paragraph 5(1)(c), section 7 and paragraph 8(2)(c) of the RPAR.

Outcome

- A PSP has timely and reliable access to financial and human resources to establish, implement and maintain its risk management and incident response framework, including responding to incidents.
- Human resources have the skills, information and training necessary to carry out their roles.

Guidance

3.1 Paragraph 5(1)(c) of the RPAR states that a PSP's framework must "identify the human and financial resources that are required to implement and maintain the framework, including, with respect to human resources, their skills and training, as well as the measures that the payment service provider must take to ensure timely and reliable access to those resources, whether from internal or external sources."

Quantity, timeliness and availability

3.2 PSPs should tailor to their circumstances the amount of human and financial resources necessary to implement and maintain their framework. This includes considering the nature and complexity of operations, ownership, organizational structures, technology and other relevant factors.

3.2.1 Human resources include personnel employed directly by the PSP and those provided by a third-party, such as agents and mandataries, third-party service providers or affiliated entities.

3.2.2 Financial resources include the budget that the PSP allocates to establish, implement and maintain its framework. This includes hiring, engaging and training human resources and investments in systems, controls, technology, property and other assets.

3.2.3 A PSP should also consider any additional human or financial resources that it may need to access to implement its incident response and recovery plan or to cover one-off or unexpected expenditures. Such resources could include resources accessed from a third party (including a parent or other affiliated entity), insurance, funding from a parent entity or investors or use of specialized external expertise.

3.3 PSPs must be able to access their human and financial resources in a timely and reliable manner during business-as-usual operations, as well as in the event of incidents, to ensure the ongoing achievement of their operational risk management objectives and targets.

3.4 If a PSP relies on a third-party for access to resources to establish, implement or maintain its framework during business-as-usual operations, the arrangements should be set out in a written contract.

3.4.1 A PSP may require third-party human or financial resources (such as external experts or contingency funds) before a contract is established. In this situation, the PSP should realistically assess how it would access those resources in a timely manner and, if relevant, cover the costs incurred.

3.4.2 Regardless, the PSP should take steps to ensure the timeliness and reliability of its access to those resources.

3.5 If PSPs expect to rely on insurance to access financial resources (e.g., to implement their incident response and recovery plan), they should be able to demonstrate that they have considered how they will be able to access these resources, at the expected value, when required.

3.6 When PSPs use their own financial resources or funding from a parent entity, they should consider how these resources are invested to ensure they are available, at the expected value, when required.

3.7 The RPAA does not impose a capital requirement on PSPs or require them to have resolution arrangements in place. Nonetheless, it is important that PSPs consider and plan for the costs and resource requirements associated with establishing, implementing and maintaining their framework according to the RPAA. This includes any buffer to cover foreseen additional costs and resource needs that might arise from an incident.

Skills, training and provision of information

3.8 As stated in paragraph 5(1)(c) of the RPAR, the framework must identify the human resource skills and training required to implement and maintain the framework.

3.9 Under section 7 of the RPAR, PSPs must ensure that all employees and other persons who have a role in establishing, implementing or maintaining the framework, are provided with the information and training they need to carry out that role.

3.10 Training should support the following outcomes:

- awareness and understanding of the framework; and
- development and maintenance of the skills required to establish, implement and maintain the framework, as needed. Human resources can obtain the necessary skills from a combination of education, experience and training.

3.11 PSPs should ensure the training for their employees and other persons:

- is provided on a regular basis so human resources maintain skills and awareness to fulfill their responsibilities;
- is updated on a regular basis, including to reflect changes to the framework or operations;
- is tailored, where needed, to the roles and responsibilities of the individual, including specific skills or process-related training that they need to perform their roles and responsibilities; and
- allows for cross-training as needed, to continue operations and avoid potential gaps resulting from staff turnover or absences, both in business-as-usual operations and in response to and recovery from incidents.

3.12 A PSP's structure and the specifics of its framework will determine which human resources should receive training and be informed about the framework. Relevant human resources could include any parties internal or external to the PSP who play a role in establishing, implementing or maintaining the framework, including agents, mandataries and third-party service providers (including, if relevant, affiliated entities).

3.13 Communication about the framework should ensure that staff and other stakeholders have the information they need to fulfill their allocated roles and responsibilities in establishing, implementing or maintaining the framework (or particular elements of it). PSPs should also inform human resources about any relevant changes to the framework, as necessary.

3.14 The Bank encourages PSPs to evaluate the effectiveness of their training to ensure that human resources understand their roles and responsibilities and how to fulfill them.

Internal review

3.15 Subsection 8(1) of the RPAR requires PSPs to review their framework at least once a year and before making any material changes to their operations or systems, policies, procedures, processes, controls or other means of managing operational risk.

3.16 As part of the review, PSPs must evaluate the adequacy of their human and financial resources for ensuring the framework is implemented, as per paragraph 8(2)(c) of the RPAR (see also Internal review). PSPs should be able to demonstrate:

- that the necessary financial and human resources are or will be available, in a timely and reliable manner, to implement, establish and maintain the framework during business-as-usual operations and in the event of incidents, so that PSPs can achieve their operational risk management objectives; and
- the sufficiency of their human resources, including the adequacy of their skills and training.

4. Objectives

This section provides guidance on paragraphs 5(1)(a), 5(1)(b) and 8(2)(b) of the RPAR.

Outcomes

- A PSP sets objectives that ensure the integrity, confidentiality and availability of its retail payment activities and of the systems, data and information involved in the performance of those retail payment activities.
- A PSP develops reliability targets and indicators to assess the achievement of its integrity, confidentiality and availability objectives.
- A senior officer oversees the achievement of the PSP's objectives.

Guidance

Objectives

4.1 Under paragraph 5(1)(a) of the RPAR, the risk management and incident response framework must set out the following among its objectives:

- "ensuring that the payment service provider can perform retail payment activities without reduction, deterioration or breakdown, including by ensuring the availability of the systems, data and information involved in the performance of those retail payment activities, and
- preserving the integrity and confidentiality of those activities, systems, data and information."

4.2 The remainder of this guideline refers to these objectives as the PSP's "integrity, confidentiality and availability objectives."

4.3 The integrity, confidentiality and availability objectives should apply to the PSP's retail payment activities as a whole and to the systems, data and information that provide or facilitate the provision of those activities. The requirements to set integrity, confidentiality and availability objectives, reliability targets and indicators apply even in cases where a PSP's services are provided using a third-party service provider, or on the PSP's behalf by an agent, or mandatary.

4.3.1 For example, PSPs are required to set objective(s) related to the overall availability of the retail payment activities they provide. Additionally, PSPs should set more granular level, objectives about the availability of specific systems, data and information involved in the performance of those retail payment activities in a way that will support the overall availability objective.

4.4 Availability objectives should be proportional, as outlined in subsection 5(2) of the RPAR. This means that more ubiquitous or interconnected PSPs will set more stringent availability objectives. However, regardless of proportionality, PSPs should set objectives to preserve integrity and confidentiality.

4.5 PSPs should establish, implement and maintain their framework so they can achieve their integrity, confidentiality and availability objectives.

Reliability targets and indicators

4.6 Under paragraph 5(1)(b) of the RPAR, the framework must set out clearly defined and measurable reliability targets for the performance of PSPs' retail payment activities and for the availability of their systems, data and information.

4.7 PSPs should consider a variety of reliability targets to specify the performance standards they intend to meet related to their availability objective. The Bank recommends that more highly ubiquitous or interconnected PSPs should, at a minimum, establish the following types of reliability targets:

- system availability target(s);
- recovery time objective(s);
- maximum tolerable downtime(s); and
- recovery point objective(s).

4.8 Paragraph 5(1)(b) of the RPAR also requires that the framework set out indicators for assessing whether each integrity, confidentiality and availability objective is met.

4.9 Reliability targets and indicators should clearly articulate the performance standards and underlying measurements that PSPs intend to monitor to ensure they are able to meet their integrity, confidentiality and availability objectives.

4.10 See Appendix C for further considerations on the establishment, implementation and maintenance of objectives, reliability targets and indicators.

Review of performance against objectives

4.11 According to subsection 8(1) and paragraph 8(2)(b) of the RPAR, PSPs must review their framework at least once a year and before making material changes. Among other things, the review must evaluate the PSP's effectiveness at meeting its integrity, confidentiality and availability objectives, having regard to its reliability targets and indicators.

4.12 When evaluating its effectiveness at meeting its objectives, a PSP should analyze information from several sources, which could include:

- data on incidents that resulted in breaches in integrity or confidentiality, or in system downtime, including how well the PSP was able to meet its reliability targets in responding to such incidents;
- observed measures of performance against objectives, reliability targets and indicators, such as system availability over the relevant period; and
- results of testing and independent reviews, which could also indicate how well the PSP may be able to meet its objectives and reliability targets in future. This could include tests of the PSP's incident response plan that indicate how well it might be able to meet certain objectives and reliability targets.

4.13 If an evaluation indicates that a PSP is not meeting its objectives, it should consider whether enhancements to its framework are required to achieve objectives, reliability targets and indicators.

4.14 The Bank encourages PSPs to monitor and evaluate their performance against their objectives, reliability targets and indicators on an ongoing basis. This may also support their compliance with the requirement to ensure continuous monitoring for the purpose of promptly detecting incidents, anomalous events and lapses in the implementation of the framework, as prescribed in paragraph 5(1)(h) of the RPAR.

Approvals and reporting

4.15 The senior officer responsible for operational risk and incident response and the board (if any) should approve a PSP's objectives, reliability targets and indicators. This is part of their obligation to approve the framework, as outlined in subsection 5(6) of the RPAR (additionally, see Roles and responsibilities).

4.16 The senior officer should be aware of a PSP's performance against its objectives. Results of a PSP's evaluation of its performance, including any consideration for improvements to the framework, should be reported to the senior officer for their approval as stated in section 8 of the RPAR.

5. Identify

This section provides guidance on paragraphs 5(1)(e) and 5(1)(f) of the RPAR.

Outcomes

- A PSP identifies and understands its operational risks.
- A PSP identifies the assets and business processes associated with its retail payment activities and classifies those assets and businesses processes based on criticality and sensitivity.

Guidance

Identification of operational risks

5.1 The 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."

5.2 Paragraph 5(1)(f) of the RPAR requires that a risk management and incident response framework identify a PSP's operational risks and describes their potential causes.

5.3 The Bank expects PSPs to establish, implement and maintain procedures to identify their operational risks and potential causes. PSPs should also identify inherent risks, which are defined as risks that are present before implementing controls or mitigation measures.

5.4 The risks that each PSP faces will depend on the nature and complexity of its operations, ownership, organizational structures, technology and other relevant factors. At a minimum, PSPs must identify operational risks that relate to each of the following areas (paragraph 5(1)(f) of the RPAR):

- business continuity and resilience—risk to a PSP's ability to perform retail payment activities due to the unavailability of people, processes, systems, premises or third parties;
- cybersecurity—risk of unauthorized access to, malicious and non-malicious use of, a failure of, or a disclosure, disruption, modification or destruction of a PSP's information system or data due to a cyber attack or a data breach;
- fraud—risk of intentional activities by internal (i.e., originating from an entity with authorized access to systems, data or information) or external (i.e., originating from an entity without authorized access to systems, data or information) threats to cause a loss of, or obtain benefit from, a PSP's assets, products or data;
- information and data management—risk related to a failure to manage information or data through its life cycle;
- information technology—risk related to inadequacy, disruption, failure, loss or malicious use of information technology systems, infrastructure, people or processes that enable and support a PSP's business needs;
- human resources—risk related to inadequate or insufficient human resources or skill requirements;

- process design and implementation—risk related to a failure to effectively design, implement, document or execute a process;
- product design and implementation—risk related to a failure to effectively design, implement or manage a product or service;
- change management—risk related to an inability to effectively implement changes, including through ineffective project design or delivery (includes but is not limited to changes to business structure, product design, services and information technology delivery);
- physical security of persons and assets—risk related to an inability to safeguard employees, clients, physical assets or facilities; and
- third parties—risk related to a failure to effectively manage third parties, including but not limited to third-party service providers, agents and mandataries, affiliated entities, other PSPs and financial market infrastructures. PSPs should consider the risk from all third parties, regardless of whether they have a contract with that party (see Third-party service providers and Agents and mandataries).

5.5 The above list is not exhaustive. PSPs should consider any other relevant operational risks that could result in the reduction, deterioration or breakdown of their retail payment activities.

5.5.1 This would include operational risks arising from activities not related to retail payments that PSPs perform that could affect their retail payment activities.

5.5.2 In the identification of risks, the Bank also encourages PSPs to consider their reliance on a particular third party, asset, system, human resource, role or any other factor (i.e., concentration risk) to determine if it may hinder the PSP's ability to achieve its objectives.

5.6 Paragraph 5(1)(f) of the RPAR stipulates that a framework must describe the potential causes of a PSP's operational risks. This includes causes of incidents that could result in the reduction, deterioration or breakdown of retail payment activities performed by a PSP. PSPs should consider the following potential causes:

- 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 (as established under section 2 of the RPAA).

5.7 As an outcome of their identification of operational risks and potential causes of those risks, PSPs should be able to:

- prioritize the identified operational risks by materiality; and
- use the prioritized operational risks to inform the systems, policies, procedures, processes and controls needed to mitigate those risks (see Protect).

5.8 PSPs should review and update their operational risks and the potential causes of those operational risks at least annually or as they identify new risks (including after an incident has occurred, as relevant). This should include assessing for emerging or evolving risks resulting from changes to both external and internal environments.

5.9 PSPs should identify the operational risks associated with material changes to their operations or systems, policies, procedures, processes, controls or other means of managing operational risk. Material changes could introduce new risks or change previously identified risks. PSPs should establish and implement any changes necessary to their framework to mitigate these risks before the change is made (see, for example, Protect and Detect).

Identification of assets and business processes

5.10 Paragraph 5(1)(e) of the RPAR states that a PSP's framework must "identify the assets—including systems, data and information—and business processes that are associated with the payment service provider's performance of retail payment activities."

5.11 The assets and business processes that a PSP should identify will depend on the nature and complexity of its operations, ownership, organizational structures, technology and other relevant factors.

5.12 Identification of assets and business processes should include, but is not limited to, any assets and business processes for which a reduction, deterioration or breakdown would adversely affect the PSP's provision of retail payment activities. Specific examples of assets related to a PSP's retail payment activities include but are not limited to:

- data or information that enables the PSP to provide retail payment activities (see the supervisory guideline Safeguarding end-user funds), including where data and information are in transit as well as where data and information are used and stored at rest;
- the physical or virtual systems, hardware or other physical assets that the PSP uses to facilitate retail payment activities;
- the software or applications that the PSP uses to facilitate retail payment activities; and
- the people and premises the PSP relies on to provide its retail payment activities.

5.13 PSPs should identify any asset or business process that is associated with their performance of retail payment activities, regardless of where it is located geographically or where the process is operationally performed. PSPs should also consider assets and businesses processes that are held or performed outside of the organization, such as by third parties (including affiliated entities), agents and mandataries and end users.

5.14 Assets or business processes that are not involved in the provision of retail payment activities may be considered outside the scope of the Bank's direct supervision (e.g., systems used solely for marketing or advertising activities).

5.15 Paragraph 5(1)(e) of the RPAR also requires that the framework classify those assets and business processes according to how sensitive and critical they are to the performance of the PSP's retail payment activities. Classification of individual assets and business processes informs the systems, policies, procedures, processes, controls and other means needed to achieve the PSP's integrity, confidentiality and availability objectives.

5.15.1 When rating the sensitivity of data, information or business process, a PSP should consider how important it is to the PSP's provision of retail payment activities, and achievement of its integrity, confidentiality and availability objectives, that:

- the data, information or process be available;
- the integrity of the data, information or process be maintained; and
- the data, information or process be kept confidential.

5.15.2 Similarly, when rating the criticality of assets other than data, information or business processes, a PSP should consider how important it is to the PSP's provision of retail payment activities, and achievement of its integrity, confidentiality and availability objectives, that:

- the asset or process be available (fully operational); and
- the integrity of the asset or process be maintained.

6. Protect

This section provides guidance on RPAR paragraph 5(1)(g).

Outcome

- A PSP preserves the integrity, confidentiality and availability of its retail payment activities by mitigating operational risks and protecting the assets and business processes used to conduct retail payment activities.

Guidance

Protection of assets and business processes

6.1 Paragraph 5(1)(g) of the RPAR requires that a PSP's risk management and incident response framework "describe the systems, policies, procedures, processes, controls and any other means that the payment service provider must have in place to mitigate its operational risks and protect the assets and business processes" that are associated with its performance of retail payment activities. This means that PSPs must establish, implement and maintain protective elements to mitigate their operational risks and protect the assets (including data) and business processes associated with their retail payment activities. They must also describe those protective elements in the framework, including the protection of data and information in transit, at rest and in use.

6.2 PSPs must establish, implement and maintain their protective elements in a manner that aligns with their individual circumstances. In the establishment, implementation and maintenance of protective elements, a PSP should consider:

- the inherent level of the risks it faces and the potential impact of those risks on its retail payment activities, assets and business processes;
- its ability to achieve its integrity, confidentiality and availability objectives; and
- its ubiquity and interconnectedness, as outlined in subsection 5(2) of the RPAR (i.e., relatively more ubiquitous and interconnected PSPs should adopt more stringent protective elements).

6.3 PSPs should take a risk-based approach to the protective elements of their framework. This means that when mitigating their operational risks, PSPs should ensure that the degree of protection is appropriate for the materiality of the risks they face.

6.4 PSPs should also take a multi-layered approach to their protective elements to provide redundancy in the event of a failure or circumvention of a single protective element (e.g., a single control).

6.5 Once PSPs have established the protective elements of their framework, they should consider the adequacy and effectiveness of those protective elements in mitigating operational risks and protecting their assets and business processes. That is, PSPs should consider whether their residual risks are aligned with objectives and, if there is a misalignment, take action to enhance the level of protection.

Information technology and cyber security protective elements

6.6 The Bank expects that all PSPs will face cyber security and information technology risks. PSPs are required to identify their operational risks related to cyber security and information technology, among other risks. They must also establish, implement and maintain protective elements to mitigate those risks and to protect their assets and business processes, as outlined in paragraphs 5(1)(f) and 5(1)(g) of the RPAR.

6.7 With respect to mitigating information technology and cyber security risks, the Bank recommends that PSPs establish, implement and maintain protective elements for the following outcomes and concepts:

- access management, including management of physical access;
- vulnerability management, remediation and patching;
- security software;
- securely configured devices;
- network security defences;
- secure cloud and outsourced information technology services;
- secure information system media;
- secure system development life cycle; and
- other protective elements.

6.8 These outcomes and concepts are expected to be relevant for all PSPs. How a PSP achieves each outcome or concept, including the nature of the protective elements that it adopts, will depend on its circumstances.

6.9 See Appendix D for further information on the recommended protective elements related to information technology and cyber security risks.

7. Detect

This section provides guidance on paragraphs 5(1)(h) and 5(1)(j) of the RPAR.

Outcomes

- A PSP establishes, implements and maintains continuous monitoring and detection capabilities.
- A PSP promptly detects incidents and anomalous events in its retail payment activities and lapses in the implementation of its risk management and incident response framework.
- A PSP escalates anomalous events and lapses in the implementation of its framework to the appropriate stakeholders (including decision-makers) in a timely manner to enable prompt response actions.

Guidance

Detection and continuous monitoring

7.1 According to paragraph 5(1)(h) of the RPAR, a framework must describe the systems, policies, procedures, processes, controls and any other means that PSPs must have in place to ensure continuous monitoring to promptly detect incidents, anomalous events that could indicate emerging operational risks and lapses in the implementation of the framework.

7.1.1 "Promptly" means that the detection must be done quickly, while taking specific circumstances into account. In other words, unless PSPs have reasonable justification for delaying, they must prioritize the detection.

7.1.2 In this context, "continuous" means that the PSP's systems, policies, procedures, controls and other means provide ongoing awareness and are analyzed at a frequency that supports risk-based decisions.

7.2 As outlined in subparagraphs 5(1)(h)(i), (ii) and (iii) of the RPAR, the scope of continuous monitoring should include:

- the PSP's retail payment activities;
- the systems, data and information involved in the performance of those activities; and
- the protective elements in place to mitigate operational risks and protect assets and business processes.

7.3 The detection of anomalous events and lapses in the implementation of the framework should support:

- the PSP's understanding of its risk environment, including identification of areas where risks are beyond appetite;
- identification of new or emerging risks that could adversely affect the integrity, confidentiality or availability of the PSP's retail payment activities or the systems, data or information that provide or facilitate the provision of those activities;
- identification of any problems in the functioning of the framework, particularly the protective elements of the framework; and
- the PSP's identification of incidents.

7.4 Examples of anomalous events and lapses in the implementation of the framework may include but are not limited to:

- unauthorized changes to systems or assets;
- misuses of access by employees, third-party service providers, agents or mandataries;
- breaches in internal policies (e.g., mandatory training, approval or record retention requirements);
- reduction or deterioration in systems or controls; and
- attempts by external entities to reduce, deteriorate or break down retail payment activities.

Continuous monitoring capabilities

7.5 PSPs should establish, implement and maintain systems, policies, procedures, processes, controls and other means that ensure continuous monitoring and detection to facilitate the prompt detection of incidents, anomalous events and lapses in the implementation of the framework.

7.6 Continuous monitoring and detection capabilities should:

- be designed to facilitate the PSP's incident response process and support information collection for the investigation of incidents, anomalous events and lapses in implementation of the framework (e.g., to determine the root cause of an incident);
- cover all types of incidents and anomalous events, along with all relevant elements of the framework (in particular, the protective elements, such as those related to cyber, information and physical security);
- allow for the detection of incidents related to, or anomalous events in, any services provided by third-party service providers and, if relevant, any lapses in the implementation of the framework by those parties; and
- allow for the detection of incidents, anomalous events and lapses in the implementation of the framework at agents or mandataries, if relevant.

7.7 See Appendix E for further information on the relationship between continuous monitoring, incident detection and response and recovery.

7.8 PSPs should take a risk-based approach to their continuous monitoring and detection capabilities. In other words, if an incident, an anomalous event or a lapse in implementation could have significant impact or is likely to occur, a PSP should increase the rigour of its continuous monitoring and detection capabilities.

Information technology and cyber security controls

7.9 With respect to information technology and cyber security risks, the Bank recommends that PSPs establish, implement and maintain continuous monitoring and detection capabilities related to the following outcomes and concepts:

- key indicators and internal thresholds (which, if breached, would trigger an action or decision);
- logging and monitoring (e.g., through access logs or traffic logs);
- network defences;
- malware detection;
- intrusion detection and prevention;
- vulnerability detection;

- security monitoring;
- physical security (e.g., through access logs);
- threat intelligence; and
- other relevant controls.

7.10 These outcomes and concepts are expected to be relevant for all PSPs. How a PSP achieves each will depend on its circumstances.

7.11 See Appendix F for further information on the recommended information technology and cyber security controls related to continuous monitoring and detection capabilities.

Escalation of incidents, anomalous events and lapses in implementation

7.12 Under paragraph 5(1)(j) of the RPAR, a framework must set out a plan for responding to anomalous events or lapses in the implementation of the framework.

7.13 This plan should establish clearly defined policies and procedures for escalation and decision-making in response to anomalous events or lapses in the implementation of the framework. The plan should:

- establish internal thresholds and timelines so that the PSP can escalate anomalous events and lapses in the implementation of the framework in a methodical and timely manner. As part of this, the PSP could consider defining alert thresholds for its detection systems to trigger the escalation of anomalous activities or events.
- define roles and responsibilities, including who would be responsible for decision-making.
- establish processes to ensure that decision-makers are provided with timely and accurate information about the anomalous event or lapse in implementation of the framework.
- when relevant, establish internal thresholds and determine who is responsible for the decision(s) when an anomalous activity or event occurs at or is detected by agents and mandataries.
- when relevant, establish the actions to take when a third-party service provider informs the PSP of an anomalous activity or event that occurs at or is detected by that third-party service provider.

7.14 PSPs must also establish, implement and maintain clearly defined policies and procedures for reporting incidents and coordinating incident response. For more information, see Response and recovery.

8. Response and recovery

This section provides guidance on paragraph 5(1)(i) of the RPAR.

Outcomes

- A PSP has a plan to respond to and recover from incidents. The plan seeks to ensure that the PSP can continue to provide retail payment activities on an ongoing basis; contain the impact of any incidents; and continue to preserve the integrity, confidentiality and ongoing availability of retail payment data, information or systems.
- A PSP allocates roles and responsibilities and develops policies, processes and procedures for implementing the plan that allow for timely action in response to an incident.
- A PSP investigates the root cause of all incidents and takes actions to address any gaps and vulnerabilities identified in its risk management and incident response framework.
- A PSP meets its obligation to report incidents that have a material impact on an end user, a PSP or a clearing house without delay (see section 18 of the RPAA).

Guidance

Incident response plans

8.1 Under paragraph 5(1)(i) of the RPAR, a PSP's framework must "set out a plan for responding to—including recovering from—incidents, including those involving or detected by an agent or mandatary or a third-party service provider."

8.2 The incident response plan should address all plausible incidents that could be caused by a PSP's operational risks, including business-as-usual incidents and major or crisis events.

8.3 When designing and establishing its incident response plan, a PSP should identify and categorize plausible events that could affect its operations and the achievement of its objectives. For example, a PSP should address incidents that would be expected to:

- pose a risk to preserving the integrity and confidentiality of the data, information or systems that support the provision of retail payment activities; or
- limit the availability of the PSP's retail payments activities or the data, information or systems that support the provision of retail payment activities. This includes incidents that would cause critical or sensitive processes or assets to be unavailable or impaired for a significant period time, including loss of technology, data, people, premises or a third party.

8.4 Although the plan should address all plausible incidents, if an incident—or category of incidents—could have a material impact or is likely to occur, PSPs should increase the rigour of incident response plans for those incidents.

8.5 Subparagraphs 5(1)(i)(i) to (viii) of the RPAR state that the incident response plan must set out:

8.6 policies, processes and procedures for implementing the plan and for escalating the response to an incident. Where relevant, the PSP must also consider the incident response procedures of its third-party service providers and the need to coordinate its response to the incident with that of the third-party service provider.

- measures to be taken to mitigate the impact of an incident and indications of how quickly the PSP could implement those measures.
- a requirement that the PSP begin an investigation (including specific areas that must be investigated) immediately upon becoming aware of an incident.
- a requirement that, while an investigation is underway, the PSP take immediate measures to prevent or mitigate further damage, including to the integrity, confidentiality or availability of systems, data or information.
- a requirement that the PSP take measures as soon as feasible to address the identified root cause(s) of the incident.
- policies and procedures for reporting incidents to, and coordinating incident response with, relevant internal and external stakeholders.
- measures to promptly identify the status of all transactions at the time of the incident. The PSP must also recover or correct data lost or otherwise affected by the incident.
- policies and procedures to maintain appropriate records for each incident.

Roles and responsibilities, reporting and escalation

8.7 As outlined in paragraph 5(1)(d) of the RPAR, PSPs must allocate roles and responsibilities for the implementation of the framework, both in the normal course of business and with respect to incident response and recovery.

8.8 PSPs should predetermine and clearly define and document in advance the roles, responsibilities, policies and procedures for reporting and coordination. PSPs should enact these policies and procedures after an incident has been detected, allowing them to take timely actions in response.

8.9 With respect to incident response, the PSP's roles and responsibilities should specify who is responsible for:

- reporting an incident to necessary stakeholders, including internal escalation and notification to the Bank, as required;
- coordinating the PSP's response to an incident (e.g., system owner, incident response manager, incident response team, third parties, agents and mandataries, and backup staff to perform certain roles and responsibilities);
- resolving an incident;
- tracking the implementation of any corrective action plans through to completion; and
- owning, reviewing and updating the incident response plan to ensure its ongoing effectiveness.

8.10 As part of their incident response plan, PSPs should determine when it would be necessary to work with their agents and mandataries to support incident response actions. For example, this might be required when the incident occurs or impacts retail payment activities provided or supported by agents or mandataries.

8.11 As stated in subparagraph 5(1)(i)(vi), a PSP's policies and procedures for reporting and coordination of incident response with relevant internal and external stakeholders must address, among other things, the timing and information shared in reporting and coordination. Internal stakeholders include the senior officer and, as necessary, agents and mandataries.

8.12 Policies and procedures for reporting and coordination of incident response should:

- require PSPs to keep relevant internal and external stakeholders (including third parties, agents and mandataries) informed in a timely manner, including providing details on the incident, communications and action plans;
- provide clear guidance on and criteria for escalating incidents internally for awareness and involvement of applicable decision-makers; and
- facilitate the PSP's regulatory obligation to report certain incidents to the Bank and materially affected end users, PSPs and clearing houses of clearing and settlement systems, as per section 18 of the RPAA.

8.11 PSPs should communicate roles, responsibilities, policies and procedures for reporting and coordination to employees and stakeholders (internal or external) who have a role in incident response. Human resources responsible for incident response should have the necessary skills to fulfill their responsibilities, and PSPs should provide training to staff with roles and responsibilities for incident response. Details of these requirements are set out in Roles and responsibilities and Human and financial resources.

8.12 PSPs should test their incident response plan to verify that the plan can be implemented as intended, as discussed in Testing.

Responding to an incident

8.13 Upon the detection of an incident, PSPs should implement their incident response plan, which requires immediate investigation and containment of the incident, regardless of the incident's materiality. As stated in subparagraph 5(1)(i)(i) of the RPAR, the incident response plan should include clearly defined policies, processes and procedures for implementing the plan.

8.14 According to subparagraph 5(1)(i)(iii) of the RPAR, as part of its investigation, the PSP must determine the incident's:

- root causes;
- possible or verified impact on retail payment activities (e.g., downtime, number of transactions affected);
- possible or verified impact on end users;
- possible or verified impact on other PSPs or on clearing houses of clearing and settlement systems that are designated under subsection 4(1) of *Payment Clearing and Settlement Act*; and
- possible or verified impact on systems, data or information involved in the performance of retail payment activities.

8.15 When incidents have a material impact on an end user, a PSP or a clearing house, PSPs must report them to materially affected individuals or entities and the Bank of Canada without delay, as established under section 18 of the RPAA. See the supervisory guideline Incident notification.

8.16 PSPs are responsible for determining whether an incident, anomalous event or lapse in implementation of the framework identified by a third-party service provider, agent or mandatary constitutes an incident for them. If it does, the PSP must investigate that incident.

8.17 As outlined in its incident response plan, when responding to an incident, the PSP should:

- enact the predetermined mitigation measures, such as manual processes or alternative solutions, as necessary, to reduce the impact of the incident (subparagraph 5(1)(i)(ii) of the RPAR).
- take immediate measures to prevent or reduce any further damage while an investigation is underway, including to the integrity, confidentiality or availability of systems, data or information (subparagraph 5(1)(i)(iv) of the RPAR).
    - For example, depending on the nature of the incident, the PSP may need to pause retail payment activities or revoke certain privileges or user access to certain systems or data.
    - If the PSP experiences a compromise in data availability, integrity or confidentiality and continues to provide its retail payment activities while investigating and resolving the incident, the PSP should confirm that it is able to contain the issue (e.g., quarantine compromised data) so that no further damage occurs.
- identify the status of all transactions at the time of any service disruption, recover lost or corrupted data and correct any integrity issues (subparagraph 5(1)(i)(vii) of the RPAR).
- consider the need to coordinate its response with that of a third-party service provider, if relevant (subparagraph 5(1)(i)(i) of the RPAR).
- implement measures as soon as feasible to address the identified root causes of the incident (subparagraph 5(1)(i)(v) of the RPAR).
    - This includes implementing, in a timely manner, any measures necessary to be able to return to preserving the integrity, confidentiality and availability of its retail payment activities and of the systems, data or information that provide or facilitate the provision of those activities.

8.18 In addition to addressing the identified root cause of the incident, the PSP is expected to consider any lessons learned from its response following the resolution of the incident. This would include addressing any vulnerabilities or gaps identified in the investigation, including but not limited to gaps and vulnerabilities in the PSP's incident response plan or its implementation. The PSP should prioritize the remediation of those vulnerabilities or gaps that would prevent it from meeting its objectives, reliability targets or regulatory requirements.

Records

8.19 As stated in subparagraph 5(1)(i)(viii) of the RPAR, the plan must require a PSP to keep, for each incident, a record of the:

- information about the incident's root cause and its possible or verified impact, as determined by the investigation;
- measures taken to mitigate the impact of the incident, to prevent or mitigate any further damage while an investigation is underway and to address the identified root causes of the incident;
- manner in which the PSP reported the incident and coordinated the incident response; and
- status of all transactions identified, the manner in which that status was identified and the manner in which it recovered any lost or corrupted data and corrected any data integrity issues.

8.20 PSPs must document all aspects of the investigation, actions, planned actions and outcomes for each incident.

9. Internal review

This section provides guidance on section 8 of the RPAR.

Outcomes

- A PSP reviews its risk management and incident response framework at least once a year and before making any material changes to its operations or its management of operational risks.
- A PSP reports the findings of each review to the senior officer and takes actions to address gaps or vulnerabilities identified in a review.

Guidance

9.1 As outlined in subsection 8(1) of the RPAR, PSPs must review their framework:

- at least once a year; and
- before making any material change to their operations or systems, policies, procedures, processes, controls or other means of managing operational risk.

9.2 Subsection 8(2) of the RPAR states that the review must evaluate:

- the framework's conformity with the requirements in section 5 of the RPAR;
- the PSP's effectiveness at meeting its integrity, confidentiality and availability objectives, considering its targets and indicators; and
- the adequacy of the PSP's human and financial resources for ensuring implementation of the framework.

9.3 Annual internal reviews should take a broad perspective to assess the overall compliance of the framework to ensure that it meets the standards required by the RPAA and RPAR. Notably, the review should evaluate the completeness, appropriateness and performance of the framework at identifying and mitigating operational risks and responding to incidents, given the PSP's circumstances. As part of this, the scope of the review should include, at minimum:

- the PSP's ability to meet its integrity, confidentiality and availability objectives;
- the overall adequacy and performance of the framework to identify, protect, detect, respond to and recover from operational risk and incidents;
- the sufficiency of the allocated roles and responsibilities and adequacy of human and financial resources; and
- the PSP's arrangements for assessing and mitigating risks from third-party service providers, agents and mandataries.

9.4 Internal reviews conducted before making material changes (including those to the PSP's operations or operating environment) should ensure that the changes will not negatively impact the PSP's ability to mitigate risks or respond to incidents. Reviews of the framework before material changes may be more targeted, focusing on the elements of the framework relevant to, or affected by, the change.

9.5 As per subsection 8(3) of the RPAR, a payment service provider must, in respect of each review, keep a record of:

- the date on which it is conducted;
- its scope,
- methodology; and
- findings

9.5.1 With respect to the methodology of the internal review, a record should include the factors and sources of information considered. See Appendix G for further information on the sources of information and factors that PSPs could consider in their review.

9.5.2 With respect to the findings of the review, a record should include any findings, such as gaps or vulnerabilities, identified in the review.

9.6 If a review identifies any gaps, vulnerabilities or areas for improvement, a PSP should, in a timely manner, update its framework as necessary to ensure that the PSP can continue to meet the operational risk and incident response requirements established in the RPAA and the RPAR.

9.6.1 As per subsection 8(4) of the RPAR, a PSP must report the findings of each review to the senior officer, if any, for their approval.

9.6.2 The Bank encourages PSPs to take a risk-based approach to prioritizing actions needed to address vulnerabilities, gaps or areas of improvement, considering the materiality of the risks arising from them.

10. Testing

This section provides guidance on section 9 of the RPAR.

Outcomes

- A PSP implements a testing program to identify deficiencies in its risk management and incident response framework.
- Relevant stakeholders actively participate in testing exercises.
- A PSP takes actions to address gaps and vulnerabilities in the framework that are identified in testing exercises.

Guidance

Objectives

10.1 As outlined in subsection 9(1) of the RPAR, PSPs must establish and implement a testing methodology to identify gaps in the effectiveness of, and vulnerabilities in, the systems, policies, procedures, processes, controls and other means provided for in their risk management and incident response framework. PSPs must ensure that their testing methodology:

- is proportionate to the impact that a reduction, deterioration or breakdown of the PSP's retail payment activities could have on end users and other PSPs, considering factors such as the PSP's ubiquity and connectedness;
- is designed to consider both high-likelihood and high-impact operational risks;
- provides for the use of tests that involve relevant internal stakeholders, including agents or mandataries, decision-makers and individuals responsible for the PSP's operational risk management;
- considers the PSP's reliance on external stakeholders, including third-party service providers;
- sets out the frequency and the scope of testing; and
- provides for testing before the adoption of any material change to the systems, policies, procedures, processes, controls or other means—or to any of the PSP's operations that will affect them—for the purpose of evaluating the effects of the change.

Testing methodology, scope, frequency and proportionality

10.2 PSPs should document their testing methodology and ensure that it provides a structured approach that guides:

- the scope of the testing;
- the testing methodology, including the reasoning for the choice of methodology for each testing exercise;
- the frequency of testing;
- the principles for involving particular stakeholders in a test(s);
- the processes for internally reporting the results of each testing exercise; and
- the principles for responding to the results of testing exercises, including determining whether, how and when the PSP will remediate identified gaps or vulnerabilities.

10.3 The scope of testing (e.g., the systems, policies, procedures, processes, controls and other means subject to testing) should be comprehensive enough to identify deficiencies in the PSP's risk management and incident response framework.

10.4 PSPs should take a risk-based approach to the scope and frequency of testing. They should test more important systems, policies, procedures, processes, controls or other means more frequently and in more depth. PSPs should also prioritize testing for elements of their framework with high inherent risk. This includes, in particular situations, where the potential impact of failure of the systems, policies, procedures, processes, controls or other means would be a reduction, deterioration or breakdown in the PSP's retail payment activities.

10.5 According to the principle of proportionality, the overall approach to the testing methodology should be appropriate for the PSP's level of ubiquity and interconnectedness. In other words, PSPs that are relatively more ubiquitous or interconnected should conduct additional and more in-depth testing.

Types of tests

10.6 The Bank expects that the testing methodology will cover three broad categories of tests to meet regulatory requirements.

10.6.1 Verifying and validating controls: These tests focus particularly on assessing the effectiveness and identifying deficiencies in the individual elements that make up the framework (such as systems, policies, procedures, processes and controls). This includes deficiencies in how those elements have been established, implemented or maintained.

10.6.2 Scenario-based testing: These tests should be designed to assess whether a PSP's framework (including incident management planning) will preserve the integrity, confidentiality and availability of:

- a PSP's retail payment activities and
- the systems and data or information that provide or facilitate the provision of those activities,
  - PSPs should design their testing program to cover a range of scenarios over time to assess the functioning of key framework elements.
  - For this category of testing, it is particularly important to consider high-likelihood and high-impact operational risks.

10.6.3 Testing of changes: Testing is a fundamental component of change management. This testing ensures that the framework will continue to be adequate and effective after a material change to the PSP's operations or its systems, policies, procedures, processes, controls or other means. The scope of this testing should cover elements of the framework and operations that will be affected by the change.

10.7 Within each category of testing, PSPs should use a variety of testing practices so each test can identify gaps in the effectiveness of or vulnerabilities in the relevant system, policy, procedure, process or control. PSPs should tailor their choice of testing practices to their operations and retail payment activities.

10.8 See Appendix H for further information on types of testing.

Stakeholders

10.9 Under subparagraphs 9(1)(c)(i) and (ii) of the RPAR, a PSP must use tests that:

- "involve relevant internal stakeholders, including agents or mandataries, decision-makers and individuals responsible for the payment service provider's operational risk management, and
- take into account the payment service provider's reliance on external stakeholders, including third-party service providers."

10.10 To determine which internal stakeholders, decision-makers and individuals responsible for operational risk management to involve in a test and the degree of involvement of each stakeholder, a PSP should consider:

- the nature and purpose of the test being conducted; and
- its allocation of roles and responsibilities for the establishment, implementation and maintenance of its framework, or for the specific system, policy, procedure, process or control being tested.

10.11 PSPs that use agents or mandataries are expected to include those agents and mandataries in the scope of their testing. This includes situations when agents and mandataries establish, implement or maintain the framework elements being tested (such as systems, policies, procedures, processes or controls).

10.12 When conducting testing exercises, PSPs must also consider their reliance on external stakeholders, including third-party service providers or other third parties.

10.13 For example, an objective for testing a PSP's incident response plan may be to verify organizational preparedness, including how well stakeholders understand and will be able to implement the plan if required. In this example, to be most effective, the test exercise should involve all stakeholders who play a role in implementing the incident response plan. Considerations for testing may include:

- agents and mandataries if they have roles and responsibilities related to the incident response plan; and
- assumptions made about the availability of services or resources when relying on a third-party service provider or other external parties.

Outcomes of testing

10.14 Following a testing exercise, PSPs should identify lessons and determine whether they need to add to or modify their framework, systems, policies, procedures, processes and controls.

10.15 PSPs must take timely actions to remedy gaps and vulnerabilities as needed to ensure they can continue to meet the operational risk and incident response requirements established in section 17 of the RPAA and section 9 of the RPAR. The Bank expects that PSPs will take a risk-based approach to prioritizing and implementing actions needed to address such gaps and vulnerabilities.

10.16 PSPs should also consider whether they need to assess the possibility that the gap or vulnerability was exploited before it was identified and remedied.

10.17 When testing conducted before a material change identifies gaps or vulnerabilities, the Bank expects PSPs to assess whether these need to be remediated before implementing the material change and to document the outcomes as necessary.

Records

10.18 Under subsection 9(2) of the RPAR, PSPs must keep a record of:

- the date each test is carried out;
- the methodology of each test, including a summary of how the test satisfies the requirements to involve relevant internal stakeholders and consider the PSP's reliance on external stakeholders;
- the results; and
- any measures taken or to be taken to address those results.

10.19 With respect to the methodology of the test, a record should include the scope of the test, such as the systems and the retail payment activities on which the testing was performed, as well as the factors and sources of information considered. With respect to the results of a test, a record should include the PSP's analysis of gaps and vulnerabilities identified and the rationale for not remediating certain gaps or vulnerabilities, if applicable.

10.20 Subsection 9(3) of the RPAR states that PSPs must ensure that the record referred to above is provided to the senior officer, if any.

11. Independent review

This section provides guidance on section 10 of the RPAR.

Outcomes

- If a PSP has an internal or external auditor, an independent and sufficiently skilled resource must conduct the independent review.
- A PSP takes action to address gaps and vulnerabilities in the risk management and incident response framework that are identified in the independent reviews.

Guidance

Objectives, methodology and scope

11.1 According to subsection 10(1) of the RPAR, PSPs that have an internal or external auditor must ensure that, at least once every three years, a sufficiently skilled individual who has had no role in establishing, implementing or maintaining the PSP's risk management and incident response framework carries out an independent review of:

- the conformity of each element of the framework with the applicable requirements of section 5 of the RPAR; and
- the PSP's compliance with each of its obligations under sections 6 to 9 of the RPAR.

11.2 The independent review must assess the degree to which the framework, including its implementation and maintenance, complies with all aspects of the operational risk and incident response requirements established in the RPAA and associated regulations.

11.2.1 In particular, the independent review should provide assurance about whether the PSP is able to effectively identify and mitigate operational risk and respond to incidents so that the PSP can achieve its integrity, confidentiality and availability objectives. The independent review should consider the completeness and effectiveness of the framework, including whether the framework (and systems, policies, procedures, processes, controls and any other elements that make up the framework) has been established, implemented and maintained as intended.

11.2.2 When a PSP engages third-party service providers, or agents or mandataries, the scope of the independent review should include the services performed by those parties as well as the PSP's arrangements for selecting and exercising due diligence on those parties.

11.3 A PSP "has an external auditor" when it regularly uses the services of an external auditor to provide independent assurance, including assurance from a financial reporting perspective. Ad hoc use of an external auditor for specialized purposes, such as conducting specific testing, would not mean that the PSP "has an external auditor."

11.4 Under subsection 10(1) of the RPAR, a sufficiently skilled individual who has had no role in establishing, implementing or maintaining the PSP's framework must carry out the independent review.

11.5 The requirement to conduct an independent review complements but does not replace the requirement that a PSP must review its framework at least annually, as outlined in subsection 8(1) of the RPAR.

11.5.1 Nonetheless, the results of the independent review may be used as an input into a PSP's internal review of its framework. See Internal review.

11.6 As applicable, a PSP may use the results of an audit or independent review conducted for other purposes (e.g., independent certifications, systems and organizational controls reporting, etc.) to meet the independent review requirement. The PSP should demonstrate in writing that the scope of the audit or independent review is aligned with RPAR requirements and that the audit or independent review covers the PSP's retail payment activities, related assets, business processes, data, information systems or framework. If the scope is not aligned or is incomplete, the PSP should conduct an additional independent review to address elements not covered by the existing assurance activities.

Outcomes of independent review

11.7 The independent review should identify any gaps and vulnerabilities within the PSP's framework. This includes absences of or weaknesses in the systems, policies, procedures, processes, controls or other elements of the framework or how they are established, implemented and maintained.

11.8 After the independent review, PSPs should identify lessons learned and gaps or vulnerabilities that require additions or modifications to their framework. PSPs must implement any changes to their framework that are needed to ensure that they can continue to meet the operational risk and incident response requirements established in the RPAA and the RPAR. This includes their ability to achieve integrity, confidentiality and availability objectives. The Bank expects that PSPs will take a risk-based approach to prioritizing and implementing actions resulting from an independent review.

11.9 According to subsection 10(3) of the RPAR, the PSP must report any gaps and vulnerabilities identified by the independent review to the senior officer, along with any measures being taken to address them.

11.10 PSPs should verify that remedial actions have been implemented as planned (e.g., as part of the next internal review or as part of the next independent review).

Records

11.11 Subsection 10(2) of the RPAR states that "the payment service provider must obtain a record that sets out the independent reviewer's name—or, if the independent reviewer carried out the review on behalf of an entity other than the payment service provider, that entity's name—and the date of the review and describes the review's scope, methodology and findings."

12. Third-party service providers

This section provides guidance related to subsection 5(3) of the RPAR.

Outcomes

- A PSP's risk management and incident response framework manages the risks arising from the use of a third-party service provider.
- A PSP determines the materiality of engaging a third-party service to provide the required services and uses the result of this determination to inform its processes for assessing and monitoring the service provider.
- A PSP assesses the risks associated with its use of a third-party service provider annually as well as before entering into, renewing, extending or substantially amending a contract with a third-party service provider.
- Responsibilities between the PSP and the third-party service provider are clearly allocated.
- A PSP develops compensating controls, as applicable, to ensure its ongoing compliance with regulatory requirements when relying on third-party service providers.
- A PSP monitors the performance of the third-party service provider to ensure its ability to deliver services as expected and in compliance with the PSP's objectives and regulatory requirements.

Guidance

Scope of third-party service providers

12.1 Under section 2 of the RPAA, a third-party service provider is a person or entity that, under a contract, provides a PSP with a service related to a payment function and is not an employee, agent or mandatary of the PSP.

12.1.1 The focus of this guidance is on third-party service providers that provide services that are relevant to the PSP's compliance with the RPAA and the RPAR. The Bank expects these services to generally include those that, if they were to be impaired or fail, would or could reasonably be expected to result in the reduction, deterioration or breakdown of the PSP's ability to provide its retail payment activities or to identify and mitigate its operational risks and respond to incidents. See Appendix I for examples of services that may be related to a payment function.

12.1.2 The exact services related to a PSP's payment functions will depend on the PSP and its arrangements; ultimately, each PSP must assess which of its third-party service providers are in scope.

12.1.3 Services that are only tangential to the provision of a PSP's retail payment activities or tangential to its operational risk management may be considered outside the scope of these requirements (e.g., third-party service providers that support only sales, advertising or payroll or that provide only legal services may not be in scope).

12.2 The definition of third-party service provider:

- includes entities affiliated with the PSP that, under a contract, provide a service related to a payment function that the PSP performs;
- includes other PSPs (regardless of whether the RPAA applies to those PSPs) that, under a contract, provide a service related to a payment function that the PSP performs, this would include a PSP that provides access to banking services related to the holding of funds;

- includes individuals (i.e., any person) and entities who provide services under contract; and
- applies regardless of the geographic location of the third-party service provider or the geographic location of the technologies that the third-party service provider uses to provide services to the PSP.

12.3 When a PSP relies on an affiliated entity to provide retail payment activities or manage operational risk, the Bank recommends that they use a contractual arrangement to govern the relationship. The PSP should therefore treat the affiliated entity as a third-party service provider. However, regardless of whether a contractual arrangement is in place, the PSP should use its framework to manage the risks associated with an affiliated entity or any other third party, as established under the RPAA.

Third-party risk management

12.4 According to their obligations to identify operational risks, PSPs must identify and mitigate the risks associated with the use of third-party service providers. Consequently, PSPs should address the use of third-party service providers in their framework (as per paragraphs 5(1)(f) and 5(1)(g) of the RPAR).

12.5 That notwithstanding, this section of the guideline refers specifically to the arrangements that PSPs should establish, implement and maintain to understand, assess and monitor third-party relationships and the associated operational risks. A PSP should establish, implement and maintain mechanisms to:

- understand the materiality of using a third-party service provider and changes to the PSP's risk profile that arise from the use of a third-party service provider;
- assess a third-party service provider before engaging its services, including its risk management practices and operational performance;
- establish contracts with the third-party service provider and clearly allocate roles and responsibilities, including in relation to the ownership, integrity, confidentiality and availability of data and information;
- assess and monitor engaged third-party service providers; and
- create compensating controls, as necessary, including termination plans.

12.6 We further explore each of these mechanisms in the following sections of the guidance.

12.7 A PSP must meet regulatory requirements, including when relying on third parties providing services related to its retail payment activities. Under section 87 of the RPAA, a PSP is liable for a violation that is committed by any of its third-party service providers acting in the course of its contract.

12.8 A PSP must not conduct its use of third-party service providers in a way that would impair the Bank's ability to supervise the PSP's compliance with the RPAA. In addition, a PSP must still be able to meet all reporting requirements, including reporting of records and requests for information.

12.9 Engaging a third-party service provider, or changes to the use of a third-party service provider, may be considered a significant change and, among other things, should be reported to the Bank of Canada (see subsection 22(2) of the RPAA). See the supervisory guideline Notice of Significant change or new activity for more information.

Materiality of service being outsourced

12.10 Before engaging a third-party service provider for a service related to a payment function, a PSP should understand the materiality of the service to its retail payment activities. To do this, a PSP should consider the impact on its retail payment activities if the service was to be impaired. A PSP should develop a formalized and documented approach to determining the materiality of the services it intends to outsource.

12.11 Determination of the materiality of the service should inform a PSP's risk-based approach to third-party risk management. This includes informing the rigour of assessments of third-party service providers; contracting, monitoring and termination activities; and any compensating controls the PSP undertakes.

12.12 A PSP should periodically review the materiality of services it receives from third-party service providers to determine if the nature of the service performed is still or is now considered material to the PSP's retail payment activities.

Assessment of third-party service provider

Objectives, methodology and scope

12.13 Subparagraphs 5(3)(a)(i) to (v) of the RPAR state that if a PSP receives services from a third-party service provider for the provision of a service related to a payment function, the PSP's framework must address how the PSP will assess:

- "the third-party service provider's ability to protect data and information that they obtain from the payment service provider or in the course of performing services for it;
- the security of the third-party service provider's connections to and from the payment service provider's systems;
- the manner in which the third-party service provider will consult or inform the payment service provider prior to making changes to the services that they provide, the manner in which they are provided or their practices for managing operational risk;
- the manner in which the third-party service provider's performance may be monitored, including the time and manner in which the third-party service provider will inform the payment service provider of any detected breach of the payment service provider's or the third-party service provider's data, information or systems and of any other deterioration, reduction or breakdown in the services provided to the payment service provider; and
- the third-party service provider's risk management practices in relation to the services that they provide to the payment service provider."

12.14 PSPs should establish, implement and maintain a formalized and documented approach to assess third-party service providers.

12.15 Detailed assessments (due diligence) support a PSP's understanding of:

- the third-party service provider's risk management arrangements;
- the third-party service provider's actual performance as well as its ability to perform the requested services, including its experience, technical capabilities, financial strength and operating effectiveness; and
- the risks the PSP faces using the third-party service provider and the implications for the PSP's compliance with the RPAA.

12.16 For example, with respect to the third-party service provider's risk management arrangements, it is particularly important that a PSP understands the third-party service provider's:

- operational reliability targets and indicators, performance against those targets and indicators, and monitoring arrangements related to the services to be provided to the PSP.
- internal control environment related to the services to be provided to the PSP.
- information and cyber security risk management arrangements and how the third-party service provider monitors and tests its own compliance with its information and cyber security framework.
- arrangements to respond to, and recover from, a breach to the PSP's or the third-party service provider's data, information and systems or any other deterioration, reduction or breakdown in services provided to, or on behalf of, the PSP. A PSP should consider what assistance would be available from the third-party service provider in the event of such a breach.
- business continuity management and disaster recovery arrangements, along with the third-party service provider's testing of these arrangements.
- subcontracting arrangements, meaning the third-party service provider's reliance on subcontractors and how the third-party service provider manages risk arising from its own outsourcing (fourth-party risk), which may affect the PSP's ability to monitor the performance of the third-party service provider.
- processes for verifying its adherence to industry standards as well as which industry standards the third-party service provider adheres to.

12.17 Appendix I includes examples of tools and sources that PSPs could use to gather information to support their assessment of a third-party service provider and examples of factors to consider when assessing a third-party service provider.

12.18 PSPs should also assess how they will be informed of changes at the third-party service provider that apply to the services they receive and how they will monitor the third-party service provider's performance.

Risk-based approach

12.19 As part of a risk-based approach, PSPs may tailor their approach to assessments as long as they continue to meet all the regulatory requirements of subsection 5(3) of the RPAR. This means that PSPs may tailor the depth of the assessment to align with the materiality of the third-party service provider.

12.19.1 A risk-based approach, in this context, should allow a PSP to focus on third-party service providers that present the most risk while still providing sufficient oversight over a PSP's other third-party service providers. For example, if an arrangement is determined to be non-material, it may be appropriate for a PSP to conduct a streamlined assessment process to address only key requirements.

12.19.2 Some third-party service providers will be regulated entities. If the regulation of the third-party service provider covers the service that entity is providing to the PSP (especially if they are regulated for similar risks as those addressed in section 17 of the RPAA), the PSP may take this into account when determining the level of assessment of these entities.

12.19.3 PSPs may also take a tailored approach to assessing third-party service providers that are affiliated entities.

Frequency

12.20 Under paragraph 5(3)(a) of the RPAR, the framework must address how PSPs will conduct these assessments no less than once a year for each of their third-party service providers and before entering into, renewing, extending or substantially amending a contract with a third-party service provider for the provision of a service related to a payment function.

12.20.1 This means that—in addition to assessing a third-party service provider before entering into, renewing, extending or substantially amending an arrangement with that third-party—PSPs must also assess each third-party service provider at least annually.

Records

12.21 According to paragraph 5(3)(b) of the RPAR, the framework must require PSPs to keep a record of the dates, scope and findings of the assessments referred to above.

12.22 This documentation should also set out the risks that PSPs identify as arising from the use of the third-party service provider and any compensating controls that PSPs establish within their own framework to mitigate those risks (see also 12.27 Compensating controls, below).

Contracting and allocation of responsibilities

12.23 When entering into, renewing, extending or substantially amending a contract with a third-party service provider, PSPs should consider whether the contractual arrangement would support their ability to consistently meet integrity, confidentiality and availability objectives and maintain compliance with regulatory requirements.

12.24 Under paragraph 5(3)(c) of the RPAR, a PSP's framework must "clearly allocate responsibilities between the payment service provider and the third-party service provider, including in relation to the ownership, integrity, confidentiality and availability of data and information."

12.24.1 PSPs should ensure that the allocation of responsibilities between the third-party service provider and the PSP are clear and documented. The Bank expects PSPs to reflect this allocation of responsibilities in the contract between the PSP and the third-party service provider.

12.25 Appendix I includes examples of other terms that PSPs are encouraged to consider in a contractual arrangement with a third-party service provider.

12.26 PSPs should also ensure they conduct a periodic formal review of arrangements (e.g., contract review) to ensure the continued adequacy of the contract.

Compensating controls

12.27 However, contracts alone are not sufficient controls. The ability to establish specific, tailored contractual terms may vary across PSPs and third-party service providers. In some cases, a PSP may not be able to negotiate all contractual terms. Even when contractual terms are negotiated, the contract may not be enough to mitigate the operational risks that arise from relying on the third-party service provider. In either case, a PSP may also need to establish additional systems, policies, procedures, processes or controls (i.e., compensating controls) to manage these risks.

12.28 For example, compensating controls could include:

- broader monitoring of the third-party service provider's ability to continue providing the service, such as financial standing and, when relevant, regulatory standing;
- ongoing security monitoring and testing conducted by the PSP, such as monitoring data and monitoring and testing technical interconnections with third-party service providers; and
- integration of third-party service providers, or the services they provide, in the PSP's operational risk framework (e.g., including the services provided in the PSP's testing methodology, and including reductions, deteriorations or breakdowns of the service in the incident response plan).

12.29 Another key compensating control to manage the risk of a third-party relationship is the development of termination plans. A PSP may be required to terminate its relationship with a third-party service provider for a variety of reasons. Regardless of the reason, the Bank encourages PSPs to develop a termination plan to ensure that PSPs are still able to meet their objectives of integrity, confidentiality and availability.

12.30 Termination plans could consider:

- the ability of a new party (a particular service provider or internal resources) to meet the required capabilities, resources and time frame required to perform such services or activities;
- risks associated with enacting the termination plan;
- the PSP's ability to meet its objectives of confidentiality, availability and integrity; and
- the PSP's ability to maintain compliance with regulatory requirements.

12.31 PSPs should document additional compensating controls established to mitigate risks arising from contractual negotiations, including where they could not negotiate specific contractual terms.

Monitoring

12.32 PSPs are expected to assess how they will monitor the performance of their third-party service providers and to conduct that monitoring (subparagraph 5(3)(a)(iv) of the RPAR).

12.33 The Bank expects PSPs to monitor all third-party service providers, including those that are affiliated entities.

12.34 Monitoring activities should be designed to ensure that:

- the third-party service provider continues to meet agreed-upon service standards in the manner expected;
- the PSP's objectives are met; and
- the PSP's compliance with regulatory requirements is maintained.

12.35 Monitoring should cover breaches of the PSP's or the third-party service provider's data, information or systems and of any other deterioration, reduction or breakdown in the services provided to the PSP. The Bank also encourages PSPs to monitor the third-party service provider's compliance with contractual terms as well as performance against targets and service-level agreements. Monitoring may also support PSPs in detecting changes to the level and type of risks associated with their relationship with the third-party service provider.

12.36 As part of a risk-based approach, PSPs should align the rigour of their monitoring with the materiality of the third-party service provider.

12.36.1 PSPs should robustly monitor material third-party service providers, which may include increasing the frequency and sophistication of monitoring and the number of dedicated resources.

12.36.2 Adequate oversight for third-party service providers with a lower risk profile could include monitoring the operational performance of the third-party service provider against agreed-upon standards and contractual terms. Monitoring should be conducted at least once a year.

12.36.3 Even when a third-party service provider is a regulated entity, the Bank encourages PSPs to regularly monitor it to confirm that the third-party service provider continues to be regulated under the relevant regulatory regime.

12.37 Monitoring should include third-party service providers notifying a PSP of issues and risk events, including detected breaches of data, information or systems and any other deterioration, reduction or breakdown in services. PSPs should ensure that they receive notifications in a timely manner.

12.38 Monitoring may also lead to the identification of incidents, anomalous events or lapses in the implementation of the framework. Refer to Detect and Response and recovery. When a third-party service provider informs a PSP of a breach, reduction, deterioration or breakdown in the services it provides, the PSP is responsible for determining whether the event meets the incident notification requirements established under section 18 of the RPAA. See the supervisory guideline Incident notification.

12.39 PSPs should document outcomes of monitoring activities. PSPs should also report monitoring activities to the applicable decision-maker (including, as relevant, the senior officer) to facilitate decision-making for third-party risk management practices.

13. Agents and mandataries

This section provides guidance related to subsection 5(4) of the RPAR.

Outcomes

- A PSP's risk management and incident response framework manages the risks arising from the use of an agent or mandatary.
- A PSP ensures that its agents and mandataries meet a set of minimum criteria for managing operational risks before entering into an agreement.
- Responsibilities between a PSP and its agent or mandatary are clearly allocated.
- A PSP performs assessments, at least once a year, to ensure the ability of the agent or mandatary to deliver services as expected and in compliance with the PSP's objectives and regulatory requirements.
- A PSP develops compensating controls, as applicable, to ensure its ongoing compliance with regulatory requirements when relying on agents and mandataries.

Guidance

Scope of agents and mandataries

13.1 In the context of the RPAA, an agent or mandatary is an individual or entity that performs retail payment activities within the scope of its authority as agent or mandatary of a registered PSP. In this type of relationship, a PSP uses an individual or entity (the agent or mandatary) to perform retail payment activities on its behalf.

13.2 According to its obligations to identify and mitigate operational risks, PSPs must identify and mitigate the risks associated with the use of agents or mandataries. Consequently, a PSP's framework should address the use of agents and mandataries.

13.3 That notwithstanding, this section refers specifically to the arrangements that PSPs should establish, implement and maintain to understand, monitor and verify the risk management practices of its agents and mandataries. PSPs should establish, implement and maintain mechanisms to:

- conduct detailed assessments of agents or mandataries before engaging their services to ensure they meet minimum criteria;
- build suitable contracting arrangements with agents or mandataries and clearly allocate roles and responsibilities, including in relation to the ownership, integrity, confidentiality and availability of data and information;
- assess and monitor engaged agents or mandataries; and
- create compensating controls, including termination plans.

13.4 We further explore each of these mechanisms in the following sections of this guideline.

13.5 PSPs must meet regulatory requirements, including when services are provided on their behalf by an agent or mandatary. Under section 87 of the RPAA, a PSP is liable for a violation that is committed by any of its agents or mandataries acting in the course of their scope of authority as agent or mandatary.

13.6 Use of agents and mandataries must not be conducted in a way that would impair the Bank's ability to supervise a PSP's compliance with the RPAA. In addition, PSPs must still be able to meet all reporting requirements, including reporting of records and requests for information.

Criteria for and assessment of agents and mandataries

Objectives, methodology and scope

13.7 Paragraph 5(4)(a) of the RPAR states that if a PSP intends to have agents or mandataries perform retail payment activities, the PSP's framework must "set out criteria in relation to the management of operational risks that those agents or mandataries must satisfy"

13.8 Ultimately, the objective of these criteria should be to ensure that the agent or mandatary will be able to perform retail payment activities on behalf of the PSP in a manner that complies with operational risk management and incident response requirements established under section 17 of the RPAA.

13.9 The established criteria will depend on the PSP's relationship with the agent or mandatary. The approach the PSP takes to develop its criteria may differ depending on the nature of the relationship.

13.10 A PSP's criteria should address, at a minimum, the agent or mandatary's:

- information technology and cyber security risk management arrangements, including how it monitors and tests its own compliance with its information technology and cyber security framework;
- incident management arrangements, including how it will report incidents to the PSP;
- operational reliability targets and indicators and its performance against those targets and indicators;
- business continuity management and disaster recovery arrangements and its testing of these arrangements;
- third-party risk management arrangements to allow the PSP to understand how it manages risk arising from its own outsourcing;
- capacity planning and change management arrangements to allow the PSP to understand how it will be made aware of changes that the agent or mandatary intends to make to its services;
- adherence to industry standards and its processes for verifying adherence to those standards;
- arrangements for notifying the PSP of changes to its systems, policies, procedures, processes or controls;
- ability and arrangements to have its performance monitored by the PSP;
- capacity to adhere to its own systems, policies, procedures, processes or controls; and
- capacity to adhere to any contractual arrangements negotiated with the PSP.

13.11 The established criteria will depend on the PSP's relationship with the agent or mandatary. The approach the PSP takes to develop its criteria may differ depending on the nature of the relationship.

13.12 As outlined in paragraph 5(4)(b) of the RPAR, the PSP's framework must "prohibit the payment service provider from having an agent or mandatary perform retail payment activities on its behalf if the agent or mandatary does not satisfy those criteria."

13.12.1 Therefore, a PSP will need to assess an agent or mandatary before entering into an arrangement with that agent or mandatary. If the outcome of the assessment is that the agent or mandatary does not, or will not be able to, meet the PSP's criteria, then the PSP should not enter into or continue an arrangement with that agent or mandatary.

13.13 Given a PSP's responsibility for the actions of agents and mandataries, a PSP should be able to understand and verify the risk management practices of its agents and mandataries. Detailed assessment (due diligence) supports a PSP's understanding of:

- the agent or mandatary's continued observance of the PSP's criteria;
- the agent or mandatary's risk management arrangements;
- the agent or mandatary's performance; and
- the risks the PSP faces by using the agent or mandatary and the implications for the PSP's compliance with the RPAA.

13.14 Appendix J includes examples of tools and resources that PSPs could use to gather information to support their assessment of agents and mandataries against these criteria.

Frequency and records

13.15 Paragraph 5(4)(c) of the RPAR states that the PSP's framework must also "address the means by which the payment service provider must, at least once a year, assess the extent to which its agents and mandataries satisfy those criteria and the agents' and mandataries' practices for managing operational risk"

13.15.1 This means that—in addition to assessing an agent or mandatory before entering into an arrangement with that agent or mandatary—PSPs must also assess their agents and mandataries at least annually.

13.16 The framework must require PSPs to keep a record of the date and findings of each assessment referred to above (paragraph 5(4)(d) of the RPAR).

Contracting and allocation of responsibilities

13.17 When a PSP enters into an arrangement with an agent or mandatary, the Bank expects the PSP to establish contractual terms to govern the arrangement. These terms will depend on the nature of the arrangements between the PSP and the agent or mandatary. A PSP should establish contractual arrangements with an agent or mandatary to ensure that the PSP can consistently meet its objectives for integrity, confidentiality and availability and maintain compliance with regulatory requirements.

13.18 According to paragraph 5(4)(e) of the RPAR, a PSP's framework must "clearly allocate responsibilities between the payment service provider and its agents and mandataries, including in relation to the ownership, integrity, confidentiality and availability of data and information."

13.18.1 A PSP should ensure that the allocation of responsibilities between any agent or mandatary and the PSP is clearly documented. The Bank expects that the contract between the PSP and the agent or mandatary will reflect the allocation of responsibilities.

13.19 PSPs should also periodically conduct a formal review of arrangements (e.g., contract review) to ensure the continued adequacy of the contract.

Compensating controls

13.20 PSPs should develop compensating controls to manage the risks associated with the use of agents and mandataries. PSPs should determine the compensating controls using the level of risk associated with an agent or mandatary.

13.21 A key compensating control to manage the risk of an agent or mandatary includes the development of termination plans. A PSP may be required to terminate an agent or mandatary for a variety of reasons. Regardless of the reason, the Bank encourages PSPs to develop a termination plan to ensure the termination is handled in such a way that PSPs are still able to meet their integrity, confidentiality and availability objectives.

13.22 Termination plans could consider:

- the capabilities, resources and time frame required to perform such services or activities or transfer them to another agent or mandatary;
- the risks associated with enacting the termination plan;
- the PSP's ability to meet its confidentiality, availability and integrity objectives; and
- the PSP's ability to maintain compliance with regulatory requirements.

Monitoring

13.23 The Bank encourages PSPs to monitor agents or mandataries to detect and respond to changes to the level and type of risks associated with the relationship. PSPs should monitor the agent or mandatory's overall performance as well as its compliance with contractual terms, performance targets and service-level agreements.

13.24 PSPs should use a risk-based approach to monitoring and document this approach to justify the rigour of monitoring activities related to certain agents or mandataries.

Appendix A: Glossary

agent or mandatary

An individual or entity that performs retail payment activities within the scope of its authority as the representative of a PSP. This relationship is arranged by the principal of a PSP. Agents and mandataries are, for all intents and purposes, considered the same under the *Retail Payment Activities Act*.

anomalous event

An event or activity that deviates from standard or normal operations.

availability[2]

Services being accessible and usable on demand by an authorized entity; ensuring timely and reliable access to and use of a payment service, system, data or information.

confidentiality

Ensuring that data or information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems; preserving authorized restrictions on data and information access and disclosure.

incident

As defined in section 2 of the *Retail Payment Activities Act*, "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 the reduction, deterioration or breakdown of any retail payment activity that is performed by the payment service provider."

Further guidance is available in the supervisory guideline Incident notification.

indicators

Metrics (quantitative or qualitative) to monitor exposure to risk; used to assess compliance with a PSP's integrity, confidentiality and availability objectives.

integrity

Accuracy and completeness; no improper modification or destruction of a system, data or information.

mandatary

See agent or mandatary.

---

2 The definitions of "availability," "integrity," and "confidentiality" align with:

- ISO 27000:2018, Information technology, *Security techniques—Information security management systems*, "Overview and vocabulary"; and
- National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

operational risk

As defined in section 2 of the *Retail Payment Activities Act*, "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. a deficiency in the payments service provider's information system or internal process;
b. a human error;
c. a management failure; or
d. a disruption caused by an external event."

outcomes

Key expectations that a PSP is expected to meet in relation to requirements set out in the RPAA and RPAR.

payment service provider

Section 2 of the *Retail Payment Activities Act* defines a payment service provider as "an individual or entity that performs payment functions as a service or business activity that is not incidental to another service or business activity."

proportionality

The balance of risk management rigour with the impact that a reduction, deterioration or breakdown of the PSP's retail payment activities could have on end users and other PSPs, indicated by factors including but not limited to the PSP's ubiquity and interconnectedness.

protective elements

Framework elements, including systems, policies, procedures, processes, controls and other means that are implemented to mitigate operational risks and protect assets and business processes.

reliability target

Quantifiable measures of the performance level used to assess compliance with a PSP's availability objectives.

response

Action taken to contain the impact of an incident; includes recovery, which is action taken to restore operations.

risk-based approach

Alignment of supervisory rigour with the nature and amount of risk posed by the payment service provider (PSP) and that PSP's particular circumstances.

root cause

The underlying driver(s) of an operational risk incident.

RPAA

Retail Payment Activities Act

RPAR

Retail Payment Activities Regulations

senior officer

Section 1 of the *Retail Payment Activities Regulations* defines a senior officer, in respect of an entity, as:

a) "a member of its board of directors who is also one of its full-time employees;
b) its chief executive officer, chief operating officer, president, chief risk officer, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs functions similar to those normally performed by someone occupying one of those positions; or
c) any other officer who reports directly to its board of directors, chief executive officer or chief operating officer."

third party

Parties that a payment service provider (PSP) has a contract with, as well as those that it does not, depending on the PSP's business arrangements and organizational structure. Examples include:

- third-party service providers
- agents and mandataries
- affiliated entities
- other PSPs
- financial market infrastructures (also known as clearing and settlement systems)

third-party service provider

As defined in section 2 of the RPAA, "an individual or entity that, under a contract, provides a payment service provider with a service related to a payment function and that is not an employee or agent or mandatary of the payment service provider."

ubiquity and interconnectedness

Indicators of the impact that a reduction, deterioration or breakdown of a payment service provider's (PSP's) retail payment activities could have on end users and on other PSPs. Information the Bank of Canada would use to establish a PSP's ubiquity and interconnectedness includes:

- the number of end users to which the PSP provides retail payment activities;
- the value of end-user funds held by the PSP;
- the value of electronic funds transfers in relation to which the PSP performed a retail payment activity;
- the number of electronic funds transfers in relation to which the PSP performed a retail payment activity; and
- the number of PSPs to which the PSP provides retail payment activities.

Appendix B: Documenting the framework

1. This list sets out the types of documentation that PSPs should consider establishing and maintaining as part of their framework. The list is not intended to be comprehensive.
    - a description of the approach to operational risk management and incident response, including references to relevant policies and procedures
    - objectives, reliability targets and indicators, and a rationale for how these were set, including:
        - a clear definition of the relationship between the PSP's objectives, reliability targets and indicators;
        - a description of how the PSP has considered the principle of proportionality; and
        - the sources of data as well as the frequency of monitoring and analysis performed
    - roles and responsibilities for operational risk management and incident response, including job descriptions, reporting lines and approval arrangements, organizational structures and other documentation that specifies how the PSP's roles and responsibilities provide for oversight and challenge
    - procedures for assessing the adequacy of human and financial resources (including the skills and training of human resources), whether the PSP has timely and reliable access to those resources, and the outcomes of such assessments; supporting documentation includes records of staff qualifications and of training provided (content, delivery, attendance, etc.)
    - policies and procedures for the identification of operational risks as well as descriptions of identified risks and their causes
    - policies and procedures for identifying and categorizing assets and business processes as well as descriptions of the PSP's assets and business processes and their criticality and sensitivity
    - documentation of systems, policies, procedures, processes, controls and other means used to mitigate operational risks and protect assets and business processes; to detect incidents, anomalous events and lapses in implementation of the framework; and to respond to incidents
    - system documentation, including development, implementation, operation, configuration and user manuals, for systems related to providing retail payment activities or managing operational risks
    - incident response and recovery plans and incident investigations
    - policies and procedures for reporting, reviewing, approving, testing, conducting independent reviews and maintaining the framework
    - descriptions and other supporting documentation for reviews, tests and independent reviews, including plans, dates performed, staff and stakeholders involved, scope, outcomes, follow-up actions and plans to implement those actions, and reasoning why certain actions are or are not recommended
    - a rationale for approaches taken

Appendix C: Objectives, reliability targets and indicators

Objectives, targets and indicators

1. PSPs set objectives to formalize the integrity, confidentiality and availability boundaries in which their retail payment activities are to operate.
2. Reliability targets and indicators represent key performance, risk or control metrics that describe the underlying measurement of the PSP's objectives. PSPs use reliability targets and indicators to provide a breakdown of how they measure a specific objective.
    - For example, a PSP could measure the performance against an availability objective by monitoring the performance of several systems and business processes that support retail payment activities, each having their own performance targets and risk and control indicators. The PSP could then aggregate the data from the targets and indicators to determine whether it is meeting its availability objective.
    - Reliability targets in this example could include the number of hours of downtime for a payment function or the number or percentage of affected customers. Indicators could include incidents impacting the relevant business process or system or the number or percentage of end-of-life assets used (see further examples below).
3. PSPs should ensure that their objectives, reliability targets and indicators are set in a consistent manner. PSPs are required to set objectives to preserve the integrity, confidentiality and availability of their retail payment activities and the systems, data and information involved in the performance of those retail payment activities. Depending on the PSP's operations, the achievement of these objectives may depend on multiple assets and business processes. The PSP may also need to set integrity, confidentiality and/or availability objectives for such assets and processes. PSPs should ensure that any reliability targets and indicators they set for individual assets and business processes align with the achievement of their overall objectives.

Reliability targets and indicators

4. PSPs should consider several factors when establishing reliability targets and indicators:
    - The reliability target or indicator should have a strong relationship to the risk (including driver or cause), objective or other relevant relationship.
    - The established reliability targets or indicators should provide early warnings of objectives that are at risk (in other words, the PSP should consider setting leading as well as lagging indicators).
    - The data underlying the reliability target or indicator should be available or attainable in a consistent manner and frequency, and the PSP should be confident in the integrity of the data.
    - The specifics of reliability targets or indicators should be tailored to the level of detail needed to monitor the desired objective. This could mean that reliability targets or indicators are set at the system or asset level, product or service level, business unit or sector level, or any other level that is relevant.
    - The reliability target or indicator should reflect interdependencies between systems or assets, products or services, business units or sectors, or any other relevant interdependencies.
    - The reliability target or indicator should be aligned with other elements of a PSP's framework (e.g., reliability targets should be consistent with the PSP's incident response plans).

5. As noted in paragraph 4.7 in Objectives, the Bank recommends that relatively highly ubiquitous or interconnected PSPs should, at a minimum, establish certain reliability targets (targets related to availability). PSPs should consider the following when setting the various reliability targets:
    - system availability targets should indicate the percentage of time that a system, process, service or function should be fully functional and available;
    - a recovery time objective should indicate the maximum amount of time, as defined by the PSP in which a disrupted system, service, process or function should resume operations;
    - maximum tolerable downtime should indicate the maximum time, as defined by the PSP, that a particular system, service, process or function can be unavailable:
        - This would encompass the PSP's recovery time objective and work recovery time for the system, service, process or function. "Work recovery time" is the amount of time that a PSP would need to verify the integrity of the system and any relevant data and bring it up to date (e.g., entering data that were collected manually during the outage).
        - A PSP's maximum tolerable downtime is the sum of its recovery time objective and its work recovery time; and
    - recovery point objectives should indicate the maximum amount of data loss, measured by time, that a PSP is willing to accept for a particular system or set of data.
6. Indicators related to availability could also include non-time-based metrics, such as the number of affected customers or transactions.
7. Examples of indicators for assessing whether a PSP is meeting its integrity and confidentiality objectives could include but are not limited to:
    - number of data breaches reported over a particular time period;
    - indicators of compliance with the PSP's policies regarding data protection (e.g., the percentage of critical data storage protected according to the PSP's standard, the percentage of critical servers protected by security software, the percentage of third parties that are onboarded with complete vendor risk assessment); and
    - tracking completion of actions to address issues (e.g., number of outstanding vulnerabilities for critical applications or desktops; number of outstanding actions or vulnerabilities identified in incident response, testing or independent reviews).

Review of performance against objectives

8. In most cases, when monitoring indicates that a PSP has not met its objectives, reliability targets or indicators, the PSP would be required to improve its framework so it can meet its objectives going forward. However, exceptions to this could arise, including cases where the PSP could not meet its objectives due to circumstances beyond its control (e.g., due to one-off events that could not have been predicted). If such an event happens, the Bank would expect PSPs to assess the likelihood of it recurring and, based on that assessment, to review their framework to determine whether they should make any improvements.
9. The Bank encourages PSPs to regularly review whether their objectives, targets and indicators continue to be appropriate. PSPs should consider any developments in their operations, including their ubiquity and interconnectedness.

Appendix D: Information technology and cyber security protective elements

This list provides further details on the recommended concepts and outcomes related to information technology and cyber security that PSPs should consider adopting as part of their overall protective elements.

1. **Access controls:** PSPs should establish, implement and maintain protective elements to mitigate the risks associated with unauthorized access to critical or sensitive assets. PSPs should track, log and review the activity history of both internal and external access to critical and sensitive assets.
    - Access controls should include both physical and virtual controls, in line with the source of the risk that PSPs are mitigating.
    - To manage internal and external user identities and accounts, PSPs should consider establishing a process to grant, withdraw or modify access rights in a timely manner according to predefined approval processes. Approval processes should involve the business owner of the information being accessed (information asset owner at the PSP) within the access management process. The Bank also encourages PSPs to define individual access to specific assets. This may be achieved by adopting access matrices that clearly state the roles related to payment activities and the associated level of access (privilege) required for each role. When implementing access matrices, a PSP should ensure that:
        - it permits access to assets based on the role the person or system requiring access plays in the PSP's payment activities;
        - sensitive or critical payment processes or tasks are not completed by one person; these processes or tasks should require validation by another person (separation of duties) before they can be completed, and the person charged with validation should be familiar with the process or task and the risks thereof; and
        - it grants only the minimum access (least privilege) required to complete and validate a task to people or systems involved in payment activities; this means that the PSP should consider the role of the person or system and ensure that they are provided no more than the minimum level of access and least privileges required to fulfill their roles (e.g., administrative privileges should be restricted, and access to systems outside the scope of a role should be denied).
    - The process of granting, withdrawing or modifying access rights should consider cases of termination of employees or other human resources or changes in responsibilities. In the case of termination of employment, access rights should be promptly withdrawn. A PSP may consider establishing, implementing and maintaining an account and identifier management program (a program to issue user IDs) that outlines the steps for receiving authorization, assignment and disabling of identifiers. This process should:
        - grant access rights and system privileges according to the roles and responsibilities of human resources and obtain approval by the applicable parties within the PSP;
        - require additional access controls for privileged access users (e.g., privileged users should require stronger authentication to access sensitive or critical assets). This includes stronger password complexity requirements and separation of privileged user accounts from regular user accounts. When possible, the Bank encourages PSPs to leverage automated solutions that help mitigate risks associated with privileged access. PSPs should not use generic or shared access accounts and should ensure they can identify internal and external users;
        - regularly review the access and permissions provided to users to ensure they are necessary and current (as outlined in the paragraph on least privilege above);

- implement multi-factor authentication for users with access to critical assets to safeguard the systems and data from unauthorized access;
- implement multi-factor authentication for users with access to sensitive system functions; these users include but are not limited to those managing financial accounts, system administrators, cloud administrators, privileged users and senior executives;
- establish a password policy to enforce strong password controls for internal and external users' access to IT systems;
- offer an option for multi-factor authentication; and
- ensure the password policy includes directives on password length, secure storage and transmission.

- The access controls should allow for the tracking, logging and reviewing of access and activity history for identified assets to enable PSPs to ensure the effectiveness of their implemented access controls. This should include tracking, logging and reviewing both virtual and physical access (e.g., maintenance and repairs) to assets, including data, information and systems.

2. **Vulnerability management, remediation and patching**: The software and firmware PSPs use to provide or facilitate retail payment activities face the risk of security vulnerabilities. PSPs should consider several processes and practices to protect against these threats:
   - Establish, implement and maintain remediation and patching practices for all software and firmware. This should include a systemic approach for discovering and assessing known vulnerabilities and patches to determine the risk posed to PSPs and the relative priority for patch deployment. This is a continuous process that requires identifying and remediating vulnerabilities throughout the software development's life cycle. When a third party develops the software, the Bank encourages PSPs to conduct due diligence on the supplier's software development life cycle, which includes ensuring that the suppliers have a strong vulnerability management program.
   - Establish, implement and maintain vulnerability remediation timelines that are proportional to the sensitivity and criticality of the asset and the severity of the vulnerability. Generally, this implies that assets that are more sensitive and/or critical to payment activities should be accorded remediation priority. Also, PSPs should prioritize vulnerabilities that pose the highest risks.
     - Additionally, PSPs should actively identify software and hardware that can no longer receive updates (end of life) and known vulnerabilities in those assets that may not be patched. PSPs should consider next steps for any end-of-life assets, including but not limited to replacing the assets or applying compensating controls to mitigate risks.
   - Establish, implement, and maintain vulnerability and patch management solutions. These technical solutions facilitate the scanning, testing and installation of patches to protect the operating environment.
3. **Security software:** PSPs faces a host of malware threats, including but not limited to viruses, worms, trojan horses, ransomware and spyware. To protect itself from such threats:
   - PSPs should consider establishing, implementing and maintaining elements to protect assets they use to conduct payment activities. Examples of such protective elements could include endpoint detection and response systems, anti-virus systems, anti-malware systems or software firewalls.
   - PSPs should ensure that anti-virus, anti-malware, intrusion prevention or detection systems, network firewalls, endpoint detection or other security software is automatically updated with the most recent signatures, rulesets, threat intelligence, threat database or similar, when applicable.
   - PSPs should configure security software for regular, automated scanning, when applicable.

4. **Securely configure devices:** Information technology systems that support a PSP's payment activities could be configured in a way that could leave the PSP's systems susceptible to cyber attacks. PSPs should consider the following actions to mitigate this risk:
    - Adhere to baseline configuration guidelines of the original equipment manufacturer (OEM). In the absence of these OEM baseline configuration recommendations, the Bank encourages PSPs to adhere to baseline recommendations of trusted independent sources.
    - Establish, implement and maintain secure configurations for all its devices (e.g., hardening the system, which includes but is not limited to changing all default passwords, avoiding the use of generic accounts, limiting needless features and allowing all security features in proportion to the level of risk the asset poses to the PSP and its payment activities).
    - Regularly review these secure configurations to ensure continuous adherence.
5. **Network security defences:** PSPs should protect their networks from internal and external threats. The Bank recommends that PSPs consider the following strategies, when applicable:
    - Establish, implement and maintain dedicated firewalls at the boundaries between the corporate network and the internet.
    - Isolate internet-facing servers from the rest of the corporate network.
    - Establish, implement and maintain network security solutions that prevent network users and systems from connecting to known malicious internet locations (e.g., content firewall, domain name system firewall or other gateway filter technology).
    - Require secure connectivity (e.g., authentication to shared resources, encryption in transit) to all corporate information technology resources and require virtual private network connectivity with multi-factor authentication for all remote access into corporate networks. A PSP should only permit administrative access to critical and sensitive assets from its internal internet protocol addresses.
    - Strictly enforce Wi-Fi security configuration items (e.g., Wi-Fi encryption setting, authentication, changing default settings and passwords).
    - Segment and separate networks (e.g., separate public Wi-Fi and corporate networks, clearly segmented according to differing security requirements).
    - Isolate point-of-sale systems and other critical or sensitive systems from the internet and other areas of the corporate network. PSPs should consider following relevant payment-industry standards, including where it stores, processes or transmits payment cards.
    - Establish, implement and maintain email security and authentication protocols on all email services.
    - Establish, implement and maintain email filtering at points of entry and exit.
6. **Secure cloud and outsourced information technology services**: PSPs that rely on third-party service providers face additional operational risks that must be mitigated. A PSP should consider the following strategies to protect data and information that are transmitted between the PSP and third-party service providers or are used by or stored at the third-party service provider:
    - Establish, implement and maintain an approach to:
        - evaluate its level of acceptance of how its third-party service providers handle and access sensitive information; and
        - evaluate its level of acceptance with the legal jurisdictions where its third-party service providers store or use sensitive information.
    - Ensure that information technology infrastructure and users communicate securely with all cloud services and applications.

- Ensure that administrative accounts for cloud services use multi-factor authentication and differ from internal administrator accounts.
- Ensure that data encryption is enabled in transit and at rest.

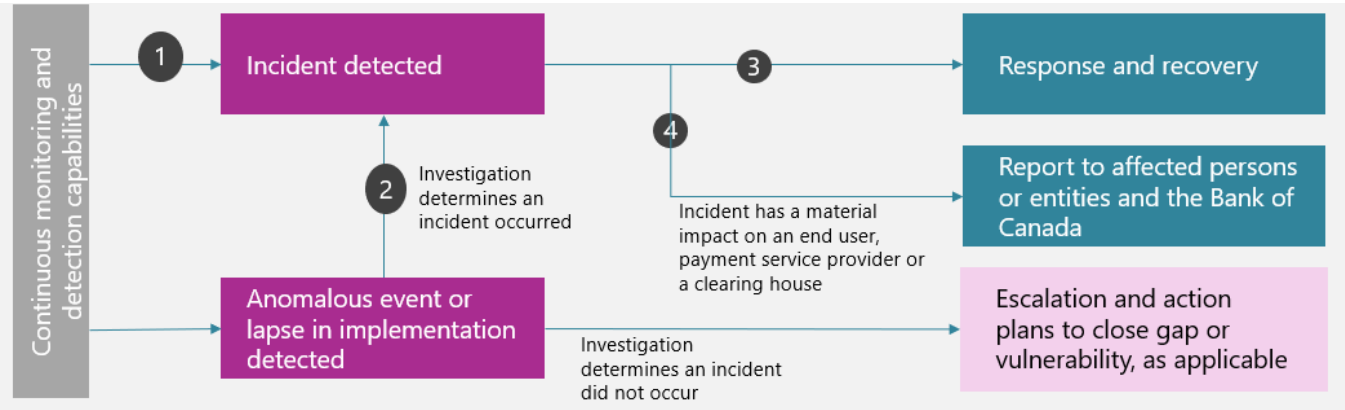
7. **Secure information system media:** PSPs using information system media (digital, such as flash drives, compact disks and external hard drives, and non-digital, such as paper and microfilm) face heightened threats against the integrity and confidentiality of the data, systems and information used to facilitate retail payment activities. PSPs should consider the following strategies to reduce these threats:
    - Protect and securely store information system digital media.
    - Maintain accountability for information system media during use or transport outside of controlled areas.
    - Sanitize information system media before disposal, release from the PSP's control or release for reuse.
    - Ensure that full-disk encryption is implemented for removable or portable media.
    - Leverage mobile device management solutions, including but not limited to disk encryption and remote wipe functionalities.
8. **Secure system development life cycle:** PSPs should incorporate security considerations at all points in the life cycle of both custom and off-the-shelf systems and software. The successful establishment, implementation and maintenance of a system development life cycle approach should, at a minimum include the following:
    - Incorporate security considerations into the acquisition, development and management of a PSP's systems.
    - Develop security architectures for systems, including requirements and approaches to protect the integrity, confidentiality and availability of the system.
    - Describe any dependencies on other systems and services, both internally and externally.
    - Describe security roles and responsibilities.
    - Protect preproduction environments (development, testing), when applicable, according to the risks presented to the system or system component.
    - Describe security requirements, controls, documentation and allocation of responsibilities when acquiring systems or services.
9. **Other controls based on the nature of a PSP's operations.** PSPs should adopt any other systems, policies, procedures, processes or controls necessary to mitigate against and protect their assets and business processes from information and cyber security risks.

Appendix E: Relationship between continuous monitoring, incident detection and response and recovery

Detection

1. Figure E-1 demonstrates the relationship between continuous monitoring, incident detection and response and recovery.
   - Generally, an incident may be detected using continuous monitoring or detection capabilities (Figure E-1, number 1).
   - An anomalous event or lapse in implementation of the framework can be detected using continuous monitoring or detection capabilities; it can be determined that an incident occurred after further investigation (Figure E-1, number 2).
2. When an incident has been detected, a PSP should activate response and recovery plans, as depicted in point 3 below. A PSP must report incidents determined to have a material impact on an end user, a PSP or a clearing house to the materially affected individuals or entities and to the Bank of Canada without delay, no later than 24 hours after detection of the incident (Figure E-1, number 4).

Figure E-1: Relationship between continuous monitoring, incident detection and response and recovery



Appendix F: Information technology and cyber security controls

This list provides further details on the recommended continuous monitoring and detection capabilities related to information and cyber security.

1. **Network defences:** These involve detecting malicious activity (such as cyber attacks) from outside the PSP's corporate network by analyzing incoming and outgoing data. It may be achieved by using perimeter firewalls, secure gateways, demilitarized zones, etc.
2. **Malware detection:** This may be achieved by installing software on endpoints to detect malware, including but not limited to trojans, spyware, keyloggers and viruses. "Endpoints" refers to a computing device that communicates with a network that it is connected to. This includes servers, smartphones, laptops, tablets and point-of-sale terminals.
3. **Intrusion detection and prevention:** This refers to the ability to identify events where an unauthorized person gains, or attempts to gain, unauthorized access to an IT asset. It can be achieved by leveraging tools such as intrusion detection systems, file integrity monitors, implementing malicious activity triggers and alerts.
4. **Vulnerability detection:** This includes activity to detect exploitable weaknesses in software code, configuration, endpoints in operation, etc. It may be done by leveraging vulnerability scanning tools, threat models, threat intelligence, baseline configuration audits, etc.
5. **Security monitoring:** This includes putting measures in place to proactively monitor unauthorized or malicious activity related to the PSP's systems to detect and respond to such anomalies. It could be achieved by leveraging tools such as a security information and event management (SIEM) solution to review logs from sources such as video surveillance, endpoint performance monitoring solutions and user behavioural analytics. To foster prompt detection and response, the Bank encourages PSPs to put solutions in place that can collect and correlate logs from various sources, such as described in point 1 to 4 above, by leveraging the functionalities of a SIEM.
6. Threat intelligence: This involves obtaining information about cyber security threats that may affect a PSP's business. A PSP can then leverage this information to proactively put controls in place to mitigate risks that it may be exposed to. Sources of threat intelligence include, but are not limited to, log collection and analysis, threat feeds, and online communities and forums.
7. **Other controls based on the nature of a PSP's operations:** These include any other systems, policies, procedures, processes or controls that a PSP could adopt to perform continuous monitoring and detection with respect to information and cyber security risks.

Appendix G: Internal review

1. The factors and sources of information that PSPs should consider in an internal review may depend on the context for the review (annual review or review due to material change), but could include:
    - any changes in retail payment activities or in how a PSP delivers its existing payment activities, including changes to technology or operations;
    - broader changes in a PSP's business, technology or operations that are relevant to its retail payment activities and the mitigation of operational risk related to its retail payment activities;
    - material changes in volumes and values of retail payment activity;
    - developments in the risk landscape or external environment;
    - observed outcomes regarding the effectiveness of the risk management and incident response framework, such as:
        - performance against targets, indicators, internal risk thresholds and risk appetite, when applicable;
        - lessons learned from incidents (including incidents that do not meet notification thresholds) and any detected anomalous events and lapses in the implementation of the framework;
    - lessons learned from audits, reviews, testing and the status of actions to implement any resulting changes to the framework; and
    - performance of agents, mandataries and third-party service providers, including lessons learned from a PSP's assessments of those parties.

Appendix H: Testing

Objectives and scope

1. To minimize the effect of testing on operations and production data or information, when relevant, PSPs should ensure that their testing and production environments are separate. Testing environments and data or information used for testing should be subject to access and other security controls. See Protect.
2. As applicable, PSPs may use the results of testing conducted for other purposes to demonstrate their compliance with the testing requirements in the RPAR, provided that they meet the objectives and outcomes of testing required under section 9 of the RPAR. PSPs should be able to demonstrate to the Bank how they are meeting the RPAR requirements. If the scope of the testing does not fully address the requirements, PSPs should conduct additional testing.

Types of tests

3. Testing may include a range of approaches, including:
    - tests that seek to assess how well a system, policy, procedure, process or control could be expected to perform in the future, including under specific circumstances;
    - exercises to review and verify how well-established policies, procedures and processes have been adhered to or how a control was performed in the recent past; and
    - verifying or testing the awareness or understanding of employees and other human resources, such as walk-throughs of the incident response plan (see further discussion below) or phishing exercises.
4. Testing could be performed in several ways, including:
    - documentation review;
    - interviews;
    - sample-based testing;
    - desktop reviews;
    - tabletop exercises;
    - walk-throughs; and
    - simulations.
5. When taking a proportional approach to testing, highly ubiquitous or interconnected PSPs could adopt additional testing for cyber and information technology risks, including penetration tests and attack simulation exercises:
    - penetration testing: The intent of a penetration test is to assess the overall strength of an organization's defence (the technology, processes and people) by simulating an attacker's objectives and actions. Parties and teams that conduct penetration testing should have demonstrable skills and experience, including technical expertise in network, operating system or application-level security.
    - attack simulation exercises: These extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability of implementing effective cyber defences. Such exercises simulate attempts by adversaries to compromise mission and business functions and provide an assessment of the security and privacy posture of systems and organizations.
6. Tests may be conducted internally or by a third-party. While this is largely at the discretion of the PSP, the Bank notes that qualified parties should conduct specialized testing, such as penetration testing.

Scenario-based testing

7. Not all tests will be scenario-based. However, scenario-based testing can provide detailed insight into how a PSP's framework can be expected to perform under specific circumstances. Scenario-based testing should include:
    - testing of incident response plans, where scenarios test the categories of incidents covered in the plan; and
    - information security testing, where scenarios test, for example, the PSP's ability to withstand certain types of cyber attacks.
8. Scenarios should be based on relevant and known operational risks. Scenarios should be stringent enough to test the full extent of the operation of the relevant elements of the framework, within the bounds of scenarios that the PSP could reasonably be expected to encounter (e.g., referring to the identified risks and causes).
9. Scenarios should evolve over time, as the PSP's operations develop or as the threat landscape evolves (e.g., to reflect more sophisticated information security threats).
10. PSPs should document their rationale behind their choice of scenarios.

Incident response plan testing

11. As part of its testing methodology, PSPs should conduct regular tests of their incident response plan. Testing the incident response plan fulfills multiple purposes, including:
    - confirming the completeness and effectiveness of the plan;
    - ensuring that the PSP's reliability targets can be met; and
    - verifying and maintaining organizational preparedness to implement the plan, when required.
12. PSPs should test their incident response plan (possibly across multiple exercises), including to cover escalation channels, decision-making or governance arrangements, and the capability of relevant staff and other stakeholders to follow and implement the plan and to return to normal operations.
    - Testing should also assess that backup processes are working and that backed-up data and information can be reliably retrieved.
    - If, as part of its incident response plan, a PSP intends to use alternative processing arrangements or manual workarounds, it should also test its ability to use these alternative arrangements.

Appendix I: Third-party service providers

Examples of services that may be related to a payment function

1. Examples of services that may be related to a payment function include services where a third-party service provider:
    - stores, processes, transmits or accesses data or information involved in the PSP's performance of retail payment activities or created in the provision of those activities (including cloud service providers and backup storage facilities);
    - manages or maintains information systems, software, hardware, technology or relevant assets for the PSP that are associated with its provision retail payment activities;
    - provides operational risk services for the PSP (e.g., services related to or supporting the establishment, implementation or maintenance of the PSP's framework or elements of the framework, which could include services to support the PSP's mitigation of, or response to, cyber, information or physical security risks and incidents);
    - provides, or has committed to provide, financial or human resources to the PSP related to the provision of its retail payment services or to the establishment, implementation or maintenance of the PSP's framework; such resources could include resources from a third-party service provider that the PSP accesses on an ongoing basis to support its business-as-usual operations as well as additional resources that the PSP intends to access as part of its response to, or recovery from, an incident (e.g., human resources such as external experts or contingency financial resources provided by a parent entity or investors);
    - provides testing or independent review functions; and
    - provides an account, insurance or guarantee to the PSP for the purpose of safeguarding end-user funds.

Materiality

2. Examples of factors to consider as part of determining the materiality of a third-party service provider arrangement include:
    - the impact of a third-party service provider arrangement on a PSP's retail payment activities, including the impact if a third-party service provider were to fail to perform activities for a certain time period or fail completely;
    - the ability of a PSP to maintain sufficient internal controls and meet regulatory requirements, including if a third-party service provider were to fail to perform activities for a certain time period or fail completely;
    - the substitutability of the service being provided, including whether the service can be effectively transferred to and delivered by an alternative provider, or by the PSP, in a timely manner; and
    - the degree of concentration risk—using the same third-party service provider for several services may pose a higher risk.

Assessment of third-party service providers

3. Assessments require a PSP to access various types of information about the third-party service provider to understand whether the third-party service provider can provide the required services, align with the PSP's objectives and maintain compliance with regulatory requirements and for the PSP to understand whether additional compensating controls are required. PSPs can use a range of tools and sources to gather supporting information, including:
    - analysis of financial statements;
    - certifications from independent parties, audit results, test results or other independent reports about the service provider's control environment and performance;
    - questionnaires or surveys;
    - prepared materials from the third-party service provider (e.g., descriptions of risk management practices);
    - reporting of agreed-upon statistics (metrics such as service-level agreements) and other items (such as changes to the service or how it is delivered) by the service provider;
    - audit rights, on-site visits and meetings with the service provider; and
    - disclosure of the nature and extent of fourth-party relationships that are material to the PSP's payment functions—this may also provide a PSP with insights on concentration risks.
4. The exact arrangements and tools used will vary across PSPs and may depend on the relationship between the PSP and the third-party service provider.

Contracting and allocation of responsibilities

5. The Bank recognizes that the ability of a PSP to establish specific, tailored contractual terms may vary across PSPs and third-party service providers. Nonetheless, the Bank encourages PSPs to consider whether certain terms can be established in contractual arrangements, including:
    - the nature and scope of the services to be provided;
    - service-level agreements and performance targets for operational reliability, integrity, confidentiality, availability and other necessary measures;
    - reporting obligations (including type and frequency of reporting) and other oversight mechanisms (such as the PSP having the right to evaluate, or have an independent auditor evaluate, the service provided by the third-party service provider) to allow the PSP to monitor the performance of the third-party service provider;
    - reporting of breaches or other reductions, breakdowns or deteriorations in services provided to the PSP;
    - obligations regarding notification by the third-party service provider of its use of other material service providers, through subcontracting or other arrangements;
    - obligations regarding notification of changes third-party service providers make to their technology, services, risk management processes or use of other material service providers, including subcontractors;
    - audit or testing access and obligations;
    - communication arrangements between the PSP and the third-party service provider, including in business-as-usual operations and if incidents and other anomalous activities or events were to occur;
    - cyber and physical security information and requirements, including data protection arrangements;

- ownership of assets;
- contingency planning, such as business continuity, incident response plans and disaster recovery, including the third-party service provider's arrangements for responding to a breach to the PSP's or the third-party service provider's data, information and systems, or any other deterioration, reduction or breakdown in services provided to, or on behalf of, the PSP;
- arrangement for provision of assistance by the third-party service provider to the PSP;
- liability and indemnity;
- dispute resolution arrangements; and
- termination arrangements for both the PSP and the third-party service provider, covering the time frame for termination and how data will be handled.

Appendix J: Agents and mandataries

Criteria for and assessment of agents and mandataries

1. Assessments require PSPs to access various types of information about the agent or mandatary to understand whether the agent or mandatary can provide the required services, align with the PSP's objectives and maintain compliance with regulatory requirements and for the PSP to determine whether additional compensating controls are required. PSPs can use a range of tools and sources to gather supporting information, including:
    - audits, on-site visits and meetings with the agent or mandatary;
    - analysis of the agent or mandatary's financial statements;
    - reporting by the agent or mandatary to the PSP—this could include reporting of statistics (metrics such as service-level agreements) and other items (such as changes to the service or how it is delivered);
    - audit results, certifications from independent parties, test results or other independent reports about the agent or mandatary's control environment and performance;
    - questionnaires or surveys administered to the agent or mandatory by the PSP; and
    - prepared materials from the agent or mandatary (e.g., descriptions of risk management practices).
2. The exact arrangements and tools used will vary across PSPs and may depend on the relationship between the PSP and the agent or mandatary.