BANK OF CANADA
BANQUE DU CANADA

Publication Date : March 1, 2024

Non-Sensitive - Non Délicat

Guideline for Designated Financial Market Infrastructures: Reporting Technology and Cyber Security Incidents

Context

Under the *Payment Clearing and Settlement Act*), the Bank of Canada (Bank) is responsible for the regulatory oversight of financial market infrastructures (FMIs) that have the potential to pose systemic risk or payments system risk in Canada.[1]

In its oversight role, the Bank ensures that designated FMIs[2] maintain appropriate risk management practices. Such practices must be consistent with the Bank's risk management standards, which adhere to the international *Principles for Financial Market Infrastructures* (PFMIs) and *Expectations for Cyber Resilience of Financial Market Infrastructures*.

Principle 17 of the PFMIs and Standard 12 of the Bank's Criteria and Risk-Management Standards for Prominent Payment Systems set out guidance for managing operational risk for FMIs that pose systemic or payments system risks, respectively. Operational risk is the risk that deficiencies in information systems, internal processes, and personnel or disruptions from external events will result in the reduction, deterioration, or breakdown of services an FMI provides. FMIs must identify the plausible sources of operational risk, both internal and external, and mitigate their impact using appropriate systems, policies, procedures, and controls.

Given FMIs' increased reliance on technology, risks to technology and cyber security can affect the availability, confidentiality, and integrity of the FMIs' systems. A technology failure or a cyber security incident could also have systemic implications if, for example, a cyber-attack were to disrupt an FMI's critical operations for an extended period.

[1] In this guideline, FMI refers to both the clearing and settlement system and its clearing house, which is the entity that operates the FMI. Both terms are defined in the Payment Clearing and Settlement Act.

[2] The *Payment Clearing and Settlement Act* provides the Governor of the Bank with the authority to designate an FMI if it is deemed to have the potential to pose systemic risk or payments system risk in Canada and the Minister of Finance agrees designation is in the public interest. See the Bank's oversight guideline for definitions of systemic risk and payments system risk.

The Bank, therefore, requires designated FMIs to establish a framework for managing operational risk—including technology and cyber risk—consistent with the Bank's risk management standards.[3] FMIs must take the necessary steps to enhance their overall operational resilience and to promptly notify the Bank of any material cyber security or technology incident.

Purpose

FMIs must report all types of operational incidents. However, this guideline sets out the Bank's specific reporting requirements for cyber security and technology incidents.

In this guideline, a technology or cyber security incident is defined as:

- An incident that has an impact, or the potential to have an impact, on the operations of an FMI, including on the confidentiality, integrity, or availability of its systems and information.

Criteria for reporting

The Bank expects FMIs to report all technology and cyber security incidents that are material to the FMI (the clearing and settlement system or its clearing house).

Materiality refers to the impact of the incident on the FMI, whether direct or indirect. Incidents classified at the highest two severity levels in an FMI's incident response framework are considered material and reportable to the Bank. An incident should be reported to the Bank if it has also been reported to another oversight, regulatory, law enforcement, or related authority.

In some cases, an FMI may need time to assess the nature and gravity of the incident and determine whether an incident is deemed to be material. In its assessment of the materiality of a technology or cyber security incident, an FMI is encouraged to rely on its business impact assessment and internal incident response framework. FMIs should notify the Bank of any incident with the potential to be material even before the full impact of the incident is known.

Reporting scope

A material incident could originate at the FMI or at an interconnected entity, such as a linked FMI, service provider, participant, member, vendor, or affiliated entity[3]. An incident that affects an interconnected entity could be transmitted to the FMI or disrupt critical services the entity provides to the FMI. For example, many FMIs rely on technology provided by a third-party service provider; hence, an incident that occurs at this third party could have a material impact on the FMI itself.

Table 1 sets out the reporting scope.

- Column 1 defines three areas of impact that the Bank expects FMIs to consider when assessing whether an incident is material and reportable.
- Column 2 provides examples of incidents that would be classified as material. This list of examples is not

[3] A service provider may be either an unrelated or an affiliated entity.

exhaustive.

Table 1: Incident reporting scope

Impact areas	Example of material impact
1. The FMI's critical services for: • payments, • central clearing, • securities settlement, or • securities depositing. These services include any functions or technology supporting them, whether provided by the FMI itself (either the clearing and settlement system or the clearing house) or outsourced to another entity.	▪ The FMI's critical systems, or key parts of those systems, are unavailable. ▪ The FMI's corporate systems are breached, and some functions are disabled. ▪ The FMI or its participants will not meet settlement obligations. ▪ Clearing members are unable to submit their margin payments or collateral requirements. ▪ Participants are not able to exchange payment messages or send them for clearing and settlement. ▪ Participants cannot transfer securities between themselves. ▪ A third-party supplying technology for the FMI's critical services experiences an outage. ▪ An incident at a data centre that the FMI uses takes the data centre offline, affecting the FMI's operations.
2. An affiliated entity performing activities essential to the critical services for: • payments, • central clearing, • securities settlement, or • securities depositing.	▪ The FMI, affiliated entity or third-party service provider experiences a technology or cyber security incident that leads to: ○ systems being breached or preventing delivery of FMI critical services, ○ financial loss, or ○ reputational damage.
3. The confidentiality, integrity, or availability of the information that the FMI or its clearing house processes, stores or transmits.	▪ The FMI inadvertently releases sensitive information (e.g., clearing members' positions). ▪ A cyber security incident leads to a compromise of the integrity of the FMI's critical data (e.g., business transactions, reference data or risk models). ▪ The FMI cannot access its critical data.

Reporting procedures

FMIs must report incidents in three stages:

1. **Immediate notification**—When an FMI identifies a material incident, or an incident that has the potential to become material, it must immediately notify the Bank's oversight team by email.

2. **Initial reporting**—Within 24 hours, or sooner, if possible, FMIs must update the Bank's oversight team on the incident. The report must include the details outlined in the "Initial reporting requirements" section below.

3. **Subsequent reporting**—Within 20 business days of the incident, FMIs must provide further details on the incident, including a root cause analysis. The report must include the details outlined in the "Subsequent reporting requirements" section below. FMIs should send the report to the Bank's oversight team by email.

In addition, an FMI must provide updates when the status of the incident has changed, at a minimum:

- once service has resumed; and
- once the incident has been fully rectified.

Initial reporting requirements

- Short description of what occurred
- Current incident status
- Date and time the incident occurred
- Date and time the incident was discovered or detected
- Date and time the immediate notification was submitted to the Bank
- Description of the workaround
- Estimated recovery time
- Notification status of:
  - system participants (if, and when they were notified, incident name)
  - senior management of the FMI
  - board of directors of the FMI
  - internal or external incident management groups (e.g., the Canadian Financial Sector Resiliency Group)
  - other regulators or supervisory authorities
- FMI key contacts:
  - name
  - email address
  - phone number
  - position
- Date of the incident
- Internal classification of this incident
- Type and category of the incident
- Designated system(s) [affected/this report concerns]
- Indicate if Senior Management of the FMI have been notified about this incident
- Indicate if Board of Directors of the FMI have been notified about this incident
- If known, relation of this incident to any previously reported incident

Subsequent reporting requirements

- Incident start time, end time and total duration
- Description of the problem, including comprehensive details of the issue, timeline of the incident and actions taken
- Impact to the FMI's critical services (e.g., payment deadlines missed)
- How this incident was discovered
- Contingency measures invoked during the incident, if any, and whether the measures remain in place, including any applicable timelines.
- What FMI critical services have been impacted due to this incident?
- Investigation results
- Root cause:
    - If the root cause is known, the steps taken to establish it
    - If it is unknown, details of the ongoing investigation and the outlook for completion
- Action plan to prevent reoccurrence of this incident or others like it (e.g., improved monitoring, quicker response times, more controls or new technology):
    - Actions completed and their completion dates
    - Actions outstanding, including target dates
- If the incident was due to a malicious attack, details about the threat actor, if known
- Relationship of incident to change activity, if any
- Impacts of the incident on other stakeholders (clients, suppliers, shareholders, government or regulatory bodies, etc.)
- Asset(s) affected by this incident, if any
- Site(s) and location(s) affected by this incident, if any

Record keeping

FMIs must maintain a record of all technology and cyber security incidents, material and non-material, and make this information available to the Bank, if requested. The Bank may require access to these records to:

- conduct its core assurance reviews
- assess whether the materiality thresholds developed by FMIs are effectively capturing the types of technology cyber security incidents it is interested in

The Bank requires FMIs to retain these records for a minimum of three years.