BANK OF CANADA
BANQUE DU CANADA

Publication Date : June 2021
Non-Sensitive - Non Délicat

Guideline for Cyber and Information Technology Incident Reporting

Context

Financial market infrastructures (FMIs) play an important role in the stability of the Canadian financial system. The services they provide are critical for individuals and firms to safely and efficiently purchase goods and services, invest in financial assets and manage financial risks. Given their central role, FMIs require strong risk management practices and must be resilient to shocks.

Under the Payment Clearing and Settlement Act (PCSA), the Bank of Canada (Bank) is responsible for the regulatory oversight of clearing and settlement systems (also known as FMIs[1]). The objectives of the Bank in its oversight role are to ensure that designated FMIs[2] operate in such a manner that risk is properly controlled and to promote efficiency and stability in the Canadian financial system. FMIs are required to maintain appropriate risk management practices, consistent with the Bank of Canada risk-management standards, which adhere to international standards – the Principles for Financial Market Infrastructures (PFMIs).[3] Principle 17 of the PFMIs sets out guidance for FMIs to manage operational risk, 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 provided by an FMI.

An important element to be addressed in an FMI's operational risk management framework is cyber risk – the likelihood of a cyber incident occurring and its impact. Over the past decade, the number of cyber incidents that have, or could have, resulted in substantial financial loss has been steadily increasing.[4] These incidents are more frequent and costly in the financial sector and have the potential to disrupt an FMI's critical operations. A cyber incident could also have systemic implications in some scenarios, for example, if 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, as defined in the PCSA. For simplicity, this guideline uses the term "operator" to refer to the FMI's clearing house.

2 The PCSA 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. See the Bank's Oversight Guideline for a definition of systemic risk and payments system risk.

3 The PFMIs are international standards for systemically important FMIs published in 2021 by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). The Bank's risk-management standards for prominent payment systems are based on the PFMIs, but are designed to be proportional to a level of risk that is relatively less than in systemic FMIs.

4 Bank of Canada Financial System Review 2019.

Operational incidents linked to failures in information technology (IT) systems could have a similar impact. For example, while the frequency of IT implementation and processing errors is low, the losses have been high relative to cyber incidents and some incidents have led to a prolonged system outage.[5] The Bank therefore requires designated FMIs to establish a framework for managing cyber and operational risk, consistent with the Bank's risk management standards.[6] FMIs are expected to take the necessary steps to enhance their cyber and overall operational resilience, and to promptly notify the Bank of any cyber or IT incident that is material.

Purpose

This guideline sets out the Bank's cyber and IT incident reporting requirements for designated FMIs. Recognizing that FMIs are currently required to report all types of operational incidents, this guideline provides additional transparency specific to the reporting of cyber and IT incidents. For the purposes of this guideline, a cyber incident is defined as follows:

> *A cyber incident is an event which jeopardizes the cyber security (including confidentiality, integrity or availability) of a system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.* [7]

The definition is intended to capture disclosure, modification, loss or misuse of information (from all sources, including insiders) as well as disruptions or outages occurring at the FMI.

Operational incidents linked to failures of IT systems, not related to cyber security, may also result in outages or disruptions as well as loss of information. Since it may be difficult for the FMI to initially distinguish between a cyber incident and an IT incident, this guideline applies to the reporting of both cyber and IT incidents.

Reporting Scope

The Bank expects FMIs to report all cyber and IT incidents (hereafter referred to as incidents) that are material to the FMI (i.e., the clearing and settlement system and/or its operator). Materiality is defined in relation to its impact on the FMI, whether direct or indirect. A material incident could originate at the FMI itself, or at an entity that is interconnected with the FMI (linked FMIs, service providers[8], participants or members, vendors or affiliated entities). An incident that affects an interconnected entity could be transmitted to the FMI itself, or disrupt critical services provided to the FMI by the interconnected entity. For example, many FMIs rely on IT that is provided by a third-party service

5 N. Chande, D. Yanchus, "The Cyber Incident Landscape," Bank of Canada Staff Analytical Note No. 2019-32 (December 2019).

6 In addition to the PFMIs, the Bank requires FMIs to observe the Guidance on Cyber Resilience for Financial Market Infrastructures, developed by the CPMI and IOSCO to supplement the PFMIs, in recognition of the escalating risks that cyber threats pose to financial stability.

7 Adapted from the National Institute of Standards and Technology (NIST) definition of "computer security incident" available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. See also National Instrument NI 24-102 (Clearing Agency Requirements) and Companion Policy.

8 A service provider may be either an unrelated or an affiliated entity.

provider, hence an incident that occurs at the IT service provider could have a material impact on the FMI itself.

The reporting scope is set out in the table below. In column 1 we define three categories of impact that the Bank expects FMIs to consider when assessing whether an incident is material and reportable. In column 2 we provide examples of the types of adverse impact that would result in an incident being classified as material. This list of examples is not intended to be exhaustive.

Incident Reporting Scope	
Impact Category	**Example of Adverse Impact**
An incident is material if it has or could have an adverse impact on:	Adverse impacts that would trigger reporting include:
1. The FMI's critical payment, central clearing or securities settlement/depository services, including any functions or technology supporting those services, whether provided by the FMI itself or outsourced to another entity	▪ The FMI may not be able to meet the two-hour resumption time objective for critical operations ▪ The FMI or its participants, will not meet its settlement obligations ▪ Clearing members are unable to submit their margin payments ▪ Participants are not able to exchange payment messages or submit them for clearing and settlement ▪ Securities cannot be transferred between participants ▪ The third-party supplying IT for the FMI's critical services experiences an outage ▪ An incident occurring at a data centre used by the FMI takes the data centre offline for an extended period
2. The operator of the FMI, or an affiliated entity performing activities essential to the critical payment, central clearing or securities settlement/depository services.	▪ The FMI's corporate systems are breached, and some functions disabled ▪ An affiliated entity has suffered an attack that may lead to a large financial loss or reputational damage ▪ An incident that occurs at an affiliated entity may compromise the affiliated entity's ability to provide services essential to the FMI's critical services ▪ An incident at a third-party service provider results in a realized, or credible, threat to the brand, reputation, trust or strategic goals of the FMI
3. The confidentiality, integrity or availability of the information that the system or the FMI operator processes, stores or transmits.[9]	▪ The FMI inadvertently releases sensitive information (e.g., clearing members' positions) ▪ A cyber incident leads to a compromise of the integrity of the FMI's critical data (e.g., business transactions, reference data, risk models) ▪ The FMI is prevented from accessing its critical data

It is the responsibility of each FMI to determine which incidents are material and therefore reportable to the Bank. In its assessment of the materiality of a cyber incident, an FMI is encouraged to rely on its business impact assessment and internal incident response framework for cyber and IT incidents. Those

9 Principle 17 (3.17.12) of the PFMIs requires that FMIs have sound and robust information security policies, standards, practices and controls to ensure an appropriate level of confidence and trust in the FMI by all stakeholders and that an FMI's information security objectives and policies should conform to reasonable standards for confidentiality, integrity and availability among others.

incidents classified at the highest two severity levels in the FMI's incident response framework would be considered material and reportable to the Bank. If an incident has been reported to another oversight/regulatory authority, law enforcement or related authority then it should also be reported to the Bank.

Reporting Procedures

Upon identification of a material incident, FMIs are expected to immediately notify the director responsible for oversight of the FMI.[10] Details of the incident are to be sent in writing, copying the senior director of the Bank's oversight division and any other contacts that the Bank has specified. The FMI should provide updates if there are changes in the status of the incident, at a minimum at resumption of service and once the incident has been fully rectified. FMIs are expected to use the Bank's operational incident reporting template to communicate the details of the incident, updating the template as required at specific points during the lifecycle of the cyber incident.

Record Keeping

FMIs are required to maintain a record of all cyber incidents, material and non-material, and make this information available to the Bank, if requested. The Bank may require access to these records for the purpose of conducting its core assurance reviews, and to assess whether the materiality thresholds developed by FMIs are effectively capturing the types of cyber incidents of interest to the Bank. The Bank requires an FMI to retain these records for a minimum of three years.

10 To reduce regulatory burden, the FMI can meet this expectation by providing simultaneous updates to the Bank and other regulators, where appropriate.