Autorité
des marchés
financiers

11 April 2025

Application and implementation guide

Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

Table of contents

1. Introduction

The framework developed by the Autorité des marchés financiers (**AMF**) for the management of information security incidents (Incidents) stems from the legal obligation financial institutions[1] (**FIs**) and credit assessment agents (**CAAs**) are under to follow sound and prudent management practices.[2]

The Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents[3] (**Regulation**), made on the basis of this obligation, defines what constitutes an Incident. It also sets out the obligations of organizations subject to the Regulation with respect to the reporting of incidents to the AMF. The obligations under the Regulation are based on the definition of Incident.

An Incident means an attack on the availability, integrity or confidentiality of information systems or the information they contain.[4]

The AMF has developed guidelines to inform FIs and CAAs of the actions that, in its opinion, may be taken to meet their obligations under the laws that apply to them. The Incident management framework is composed of regulatory obligations and expectations formulated in the various guidelines.

For a reminder of the AMF's Incident management expectations, see the following guidelines:

For the foundations:

- *Governance Guideline*
- *Integrated Risk Management Guideline*
- *Compliance Guideline*

For more specific expectations:

- *Guideline on Information and Communications Technology Risk Management*
- *Operational Risk Management Guideline*
- *Business Continuity Management Guideline*
- *Guideline applicable to credit assessment agents*

[1] Section 485 of the *Insurers Act*, CQLR, A-32.1, section 601.1 of the *Act respecting financial services cooperatives*, CQLR c. C-67.3, paragraph (u) of section 43 of the *Deposit Institutions and Deposit Protection Act*, CQLR, c.-I-13.2.2, section 277 of the *Trust Companies and Savings Companies Act*, CQLR, c.-S-29.02.

[2] Sections 47 and 66 of the Credit Assessment Agents Act, CQLR, c. A-8.2. In the case of credit assessment agents, the obligation is to adhere to appropriate management practices ensuring that the rights conferred by this Act are respected.

[3] M.O. 2024-13, G.O. II, 6381. Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

[4] Section 2 of the Regulation.

2. Purpose of the guide

Organizations subject to the Regulation include authorized insurers, federations of mutual companies, federations of credit unions and credit unions not members of a federation, authorized deposit institutions, authorized trust companies and credit assessment agents designated by the AMF (Organizations).

Federations of credit unions are responsible for ensuring compliance with their obligations under the Regulation, including the obligation to develop and implement an Incident management policy in respect of its member credit unions, and for notifying the AMF if there is an Incident.

In the case of mutual companies, each company is responsible for developing and implementing an Incident management policy and notifying the AMF if there is an Incident. Federations of mutual companies, like mutual companies, must also comply with the regulatory obligations.

3. Organizations subject to the Regulation

Organizations subject to the Regulation include authorized insurers, federations of mutual companies, federations of credit unions and credit unions not members of a federation,[5] authorized deposit institutions, authorized trust companies and credit assessment agents designated by the AMF (**Organizations**).

Federations of credit unions are responsible for ensuring compliance with their obligations under the Regulation, including the obligation to develop and implement an Incident management policy in respect of its member credit unions, and for notifying the AMF if there is an Incident.

In the case of mutual companies, each company is responsible for developing and implementing an Incident management policy and notifying the AMF if there is an Incident. Federations of mutual companies, like mutual companies, must also comply with the regulatory obligations.

4. Incident management policy

The Regulation requires Organizations to develop and implement an Incident management policy. As with other policies, the Incident management policy can take different forms: it can be a separate specific policy or incorporated into another policy, such as an information security policy.

The policy should include all the attributes of a policy and provide a clear description of roles and responsibilities. In this regard, good practice calls for the development and periodic review of a policy by senior management and approval of the policy by the board of directors.

The Incident management policy must, at a minimum, make reference to the official documents describing the Organization’s procedures and mechanisms for detecting, assessing and responding to Incidents. If practices for detecting, assessing and responding to Incidents are based on standards and other technical documents from recognized sources, the sources should be mentioned in the policy.

As the Regulation is principles-based, Organizations have flexibility to determine the content of the policy and how it is to be implemented.

[5] *Act respecting financial services cooperatives*, CQLR, c.-67.2

5. Procedures and mechanisms for detecting, assessing and responding to Incidents

The AMF encourages Organizations to draw from publications by national and international bodies such as the International Organization for Standardization (ISO),[6] the Information Systems Audit and Control Association (ISACA), the National Institute of Standards and Technology (NIST) or Control Objectives for Information and related Technology (COBIT) when developing their mechanisms and procedures. These bodies recommend implementing a number of good practices that contribute to sound Incident management.

In order to ensure consistency and objectivity in detecting, assessing and responding to incidents, the bodies mentioned above have identified good practices that the Organizations could adopt, including:

- Categorizing Incidents based on criteria such as type of event and causes
- Classifying Incidents to determine how they are to be treated and the required level of internal escalation
- Using pre-defined ratings to determine an Incident's severity and classification
- Ensuring that all implemented processes, procedures and mechanisms are part of a broader Incident management process
- Developing incident documentation standards to ensure consistency in assessing Incidents
- Putting in place control and supervision measures to ensure that Incidents are managed to achieve the following objectives:
    - Minimize injury
    - Reduce the risk of Incident recurrence
    - Report their occurrence
- Annually updating and testing all Incident detection and response mechanisms
- Continually collecting information in the information system logs in order to record user activities, exceptions, system failures and other information security-related events
- Checking and updating the information system logs
- Obtaining information on information systems' technical vulnerabilities on a timely basis

An Organization's exposure to such vulnerabilities should be assessed, and appropriate measures should be taken to address all the associated risks.

- Asking employees and third parties who use the Organization's information systems and information and communications technology services to report any observed or suspected information security weaknesses in systems or services
- Obtaining reasonable assurance before entering into a business relationship with a third party that the latter has procedures and controls in place to ensure sound management of its Incidents

[6] 27 035

6. Incident reporting

Reporting to officers and managers

The Organization's policy must include criteria for internal reporting (escalation) to the different levels of the Organization, including officers or managers.[7]

The Organization's policy should also cover, based on the various obligations applicable to it, reporting to the AMF and to any stakeholders, such as clients, third parties, consumers and other regulatory bodies.

The reporting timeframe and method should be indicated in the policy. When developing the various reporting types, the Organization should also consider Incidents that occur at a third party to which it has entrusted the performance of any part of an activity if the Incident affects the activity entrusted to the third party.

Good practices recommend that the following be considered when determining Incident reporting criteria:

- categorization
- severity
- classification

Categorization allows Incidents to be grouped to facilitate incident management. It is based on the nature of the Incident, including:

- the incident type, meaning the event (data theft, outage, etc.); or
- the causes (cyber attack, human error, etc.).

The **severity** of an Incident indicates the importance and sense of urgency that the Organization gives to bringing the Incident under control and closing (resolving) it. The criteria used to determine severity should consider factors such as:

- the amount of time it is expected to take for operations to return to normal;
- the impact on clients;
- the extent of confirmed or anticipated financial, reputational, regulatory and/or other impacts of the Incident on the Organization's operations;

The extent of the impacts may be assessed taking into account the following data: personal information, information assets or users affected by the Incident.

- the time the Incident occurred and the estimated time for closure (resolution) of the Incident.

[7] The terms "officers" and "managers" reflect the terminology used in the laws underpinning the Regulation. In the case of credit unions or a federation of credit unions, the term "managers" is used; the more commonly used term in other Organizations is "officers". In both cases, the term refers to an Organization's senior management.

Classification serves to qualify the Incident so as to confirm its status and prioritize its management. It should take into account all the information obtained, including:

- categorization (type, cause)
- severity of the Incident
- severity of the impacts for the Organization, its clients and the financial system
- any other relevant factors

Person responsible for Incident management

In its policy, the Organization must provide for the appointment of a person responsible for Incident management and reporting. This person should be responsible for ensuring that the policy is developed and implemented in the Organization.

A space to designate the person responsible for Incident management is provided in E-Services.

Reporting Incidents to the AMF is the responsibility of the person responsible for Incident management and reporting, but that person may delegate this responsibility to another party.

If the Organization has any doubts about the materiality of an event or an Incident, it can consult its person in charge of relations with the institution or contact the AMF directly.

7. Incident register

Each Organization should maintain an up-to-date Incident register. The information recorded in the register should be kept in a secure and confidential manner for a period of five years from the date of the end-of-Incident report.

All information relating to the Incident management lifecycle should be recorded in the register. The information should be as complete as possible and support the assessments, decisions and actions to be taken. The register should provide an accurate historical record of all the information collected and actions taken throughout the Incident management lifecycle.

In addition to being used for analytical purposes, the information recorded in the register may make it possible to see Incident trends, contributing to the sound management of all of an Organization's risks.

At a minimum, the following information should be recorded in the register.

Information to be recorded in the register	Clarifications	Corresponding space on the web form, where applicable
Date and time of the Incident	Means the date and time the Incident was **detected and occurred**. "Detected" means when the Incident was reported within the Organization for the first time; "occurred" means when the Incident happened (if known).	**When the incident was reported** Page 3, question 7 **When the incident occurred** Page 3, question 8
Location of the Incident	Means where the Incident originated, i.e., from an internal party (employee) or an external party (consultant, third party or recognized malicious organization). If it originates from an external party, the country should be specified.	Page 3, question 12
Nature of the Incident	The nature of the Incident may be determined by the type of Incident (data theft) or by the causes of the Incident (cyber attack).	**Main type of Incident** Page 3, question 5 **Cause(s) of the incident** Page 5, question 5
Detailed description of the Incident	The description should be exhaustive and include, without being limited to, the following information: • categorization • severity rating • classification for the purposes of Incident handling and reporting • identified vulnerabilities • availability, integrity and confidentiality impacts • nature of the data involved The following information may also be included: • assessment regarding a potential recurrence of an Incident of a similar nature • actions taken to address identified vulnerabilities • conclusions upon closing the Incident	Page 3, question 4

Information to be recorded in the register	Clarifications	Corresponding space on the web form, where applicable
Injury caused by the Incident	The criteria to determine injury should consider the services and resources affected and an assessment of the Incident's impacts.[8]	
Third parties involved in the Incident	All third parties involved in the Incident. Includes the recipients of the Incident report, in accordance with the provisions of the Organization's policy. **A good practice is to identify the type of client affected by the Incident and provide an estimate of the volume of clients affected.**	**Internal and external parties involved** Page 3, question 12 **Clients affected** Page 4, question 3 **Financial or non-financial organizations informed** Page 3, question 15
Actions taken	The actions taken include: • strategies, procedures or mitigating measures put in place to bring the Incident under control and prevent a recurrence • communications issued under the Organization's policy • date(s) and time(s) of report(s)	**Stakeholders involved** Page 3, questions 13 **Date and time of reports** Page 3, question 14 **Action taken** Page 5, questions 1 to 4
Organization's assessment regarding a potential recurrence of the Incident	Assessment of the likelihood of the Incident occurring again. This assessment may be reviewed based on new information about the Incident. A good practice is to document any changes in the Organization's assessment.	Page 6, question 2
Actions planned	Actions may include steps to reduce the likelihood of new Incidents of a similar nature occurring in the future (if such steps have not yet been taken).	Page 6, question 1

[8] For more information, see page 59 of *Format for Incident Reporting Exchange (FIRE)*: Final report, 15 April 2025, Financial Stability Board.

Date Incident brought under control	Date the Organization has brought the Incident under control and operations have been returned to normal. When Incidents involve personal information, operations are not necessarily disrupted. If such an Incident does not disrupt operations, it is considered to have been brought under control when the practice or process that is at the origin of the Incident has ceased or been corrected.	Page 3, question 10
Incident close date	Date the Incident is closed, i.e., when all action plans have been executed.	Page 3, question 11

In addition to the above information, the register should contain all the information about the Incident that the Organization requires in order to make a complete report to the AMF.

8. Process for reporting Incidents to the Autorité des marchés financiers

An Organization must notify the AMF when an Incident is reported to its officers, or, where applicable, its managers, in accordance with its criteria for escalating Incidents to the various levels of the Organization. The Organization must notify the AMF of these Incidents via ***E-Services*** no later than 24 hours from the time an officer, or, where applicable, a manager, is informed of the situation.

The Organization must, to the best of its knowledge, provide the AMF with all the required information specified in the reporting form until such time as the reported Incident has been brought under control and the end-of-Incident report has been submitted.

When referring to an Incident, "has been brought under control" generally means that operations have resumed without management of the Incident necessarily being totally over.

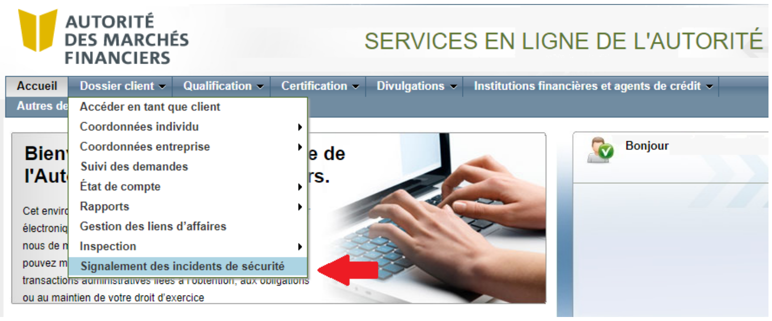
After an Incident is originally reported to the AMF, the Organization must use ***E-Services*** to submit any corrections or new information regarding the Incident. Subsequent reports must be made to the AMF, for every Incident, within no more than three (3) calendar days, even if there are no new developments to report or information to add.

Throughout the time that an Incident is being handled and reports are being submitted via E-Services, the AMF may require clarifications regarding information that is reported. The Organization will be able to attach additional documents to the AMF reporting form for this purpose.

All information stemming from the report must be provided using the appropriate fields on the form. The information, together with a report confirming that the Incident has been brought under control and normal operations have resumed, must be submitted no later than 30 days after the Incident has been brought under control. Also, a report containing additional relevant and previously undisclosed information may be submitted in E-Services in the "Additional documents" section.

9. Assistance

Organizations requiring assistance in using ***E-Services*** are invited to refer to the How to register for AMF E-Services - Representatives and future professionals | AMF web page or contact the AMF at 1-877-525-0337.


AUTORITÉ
DES MARCHÉS
FINANCIERS
SERVICES EN LIGNE DE L'AUTORITÉ
Accueil
Dossier client
Qualification
Certification
Divulgations
Institutions financières et agents de crédit
Autres de
Accéder en tant que client
Coordonnées individu
Coordonnées entreprise
Suivi des demandes
État de compte
Rapports
Gestion des liens d'affaires
Inspection
Signalement des incidents de sécurité
Bien
l'Aut
e de
rs.
Cet envir
électroniq
nous de n
pouvez m
transactions administratives liées à l'obtention, aux obligations
ou au maintien de votre droit d'exercice
Bonjour

If an Organization has any doubts concerning the materiality of a reportable Incident, it can consult the person responsible for its file at the AMF or contact the AMF.