Autorité
des marchés
financiers

July 2026

Financial Crime Risk Management

Overview of good practices observed within financial institutions

Table of contents

Preamble	3
Reminder of AMF Expectations	4
Theme 1: Governance	5
Theme 2: Integrated Risk Management	7
Theme 3: Reporting	9
Theme 4: Fraud Impacting Clients	10
Other Tools and Assistance Available from the AMF	12
Conclusion	13
Appendix 1 - Management of Information and Communications Technology Risks	14

Legal deposit – Bibliothèque et Archives nationales du Québec, 2026
ISBN 978-2-555-04485-2 (PDF)

Preamble

Financial institutions exist in an operational environment where financial crime risks are constantly evolving. The methods used to perpetrate these types of crimes are increasingly sophisticated and diverse, requiring institutions to continuously adjust their monitoring, detection and prevention mechanisms.

Financial crimes are generally grouped into three broad categories of practices that can impact clients:

- Fraud committed by a resource internal to the entity, such as an officer, director or employee, whether in collusion or not in collusion with an individual within or outside the institution (e.g. employee embezzlement).
- Fraud committed by a client or third party (e.g. forging a signature on a cheque or an insurance claim whose value has been intentionally overstated.
- Practices associated with money laundering and terrorist financing.

While responsibility for monitoring and investigating financial crimes lies primarily with specialized agencies such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the police, the Autorité des marchés financiers (AMF) plays an important role in supporting operational and financial resilience in the sector and protecting and assisting financial consumers.

During the 2025–2026 fiscal year, the AMF, as part of an ongoing effort to better understand industry practices and assess financial crime risk management, conducted a crosscutting supervisory review on a sampling of financial institutions authorized to carry on business in Quebec.

The supervisory review was based on a document review and statutory meetings or interviews held with institutions of various types and sizes. The aim was to develop a portrait of financial crime risk management practices, including practices associated with fraud that impacts clients.

Life and health insurers	**P&C insurers**
Deposit institutions	**Trust companies and savings companies**

The resulting findings and observations will serve as inputs for reflection in connection with updating the *Financial Crime Risk Management Guideline*, as will the opportunities for improvement submitted an individualized basis to institutions under the *Supervisory Framework for Financial Institutions and Credit Assessment Agents*.

The findings will also help the AMF direct and prioritize joint efforts undertaken with the industry to enhance existing frameworks with a view to reducing compliance burden.

The purpose of this document is not to provide a comprehensive portrait of observed practices or finalize the AMF's expectations but, rather, to share certain observations and good practices in order to support financial institutions in strengthening their financial crime risk management mechanisms and to promote a proactive, scalable approach to managing such risks.

It is the AMF's hope that the good practices described in this report will enable institutions to compare initiatives and will serve as a source of inspiration for the development and rollout of their financial crime risk management strategies.

Reminder of AMF Expectations

The good practices presented in this document are linked with the AMF expectations expressed in its guidelines.

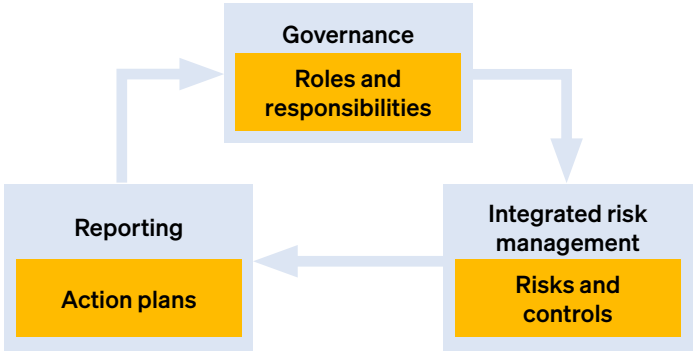
Practice framework: What is meant by "expectations"?

The AMF advocates a prudential approach primarily based on principles and good practices, rather than the enactment of detailed prescriptive rules. It therefore establishes guidelines, under the powers conferred on it by the laws it administers, to inform financial institutions of the measures that, in its opinion, can be taken to meet their obligations, based on the activities they are authorized to carry on.

It is the responsibility of each institution to adopt the principles and expectations set out in the AMF's guidelines and to implement them properly, following the principle of proportionality, based on the nature, size and complexity of its activities and its risk profile.

In general, the AMF expects financial institutions' financial crime risk management to:

- Be supported by effective **governance** and clearly defined roles and responsibilities;
- Be an integral part of financial institutions' **integrated risk management**; and
- Include a formal **reporting** framework.



By implementing risk management practices consistent with these expectations, financial institutions can prevent and detect activities associated with financial crime activities and mitigate the related risks for both the institution and its clients.

The good risk management practices identified during the review are grouped under four broad themes.

Theme 1: Governance

For most financial institutions consulted, sound management is underpinned by a **governance structure** that includes:

- The identification of key stakeholders in the operation of the institution;
- An **overall risk management policy that is** tailored to their situation and covers:
  - Stakeholders' roles and responsibilities;
  - Interrelationships with the risk management framework;
  - Mechanisms for managing and reporting information security incidents, including incidents of fraud;
  - Required reporting;
  - Expectations;
  - The culture;
  - Consequences for employees or third parties who are at fault; and
  - An organizational chart illustrating the governance structure.
- **Specific policies** that address money laundering, external and internal fraud, and other such matters.
- **Tools** enabling them to consider and manage situations faced by them and ensure that all business lines are made sufficiently aware of financial crime risks. The tools can be in the form of guides, quick references, communities of practice, sharing sessions, trend and root cause analyses and/or organizational coordination mechanisms.

Some examples of elements identified in the mechanisms and policies reviewed—which can differ depending on the institution, its size, and the complexity of its activities—are listed below for information purposes.

To keep their policies relevant, remain aligned with authorities' expectations, adapt to new risks and improve their practices, several institutions also perform **updates**:

- At regular, predetermined intervals (e.g. every two years).
- On an ad hoc or as needed basis (e.g. when deficiencies are identified in policies, procedures or controls, new schemes emerge, new products are launched, a new type of clientele is being developed, or a change is made to the distribution model, regulations or prudential framework.

Overall Risk Management Policy

Examples of elements considered:

- Governance and risk management framework (including a risk appetite statement)
- Committee mandates or charters
- Internal and external audits
- Reporting, dashboards and escalation

Specific frameworks and mechanisms for managing financial crime risks

Examples of elements considered:

- Information security
- Access management
- Incident management and register
- Third-party and outsourcing risk management
- Business continuity plan
- Use of artificial intelligence
- Fraud and loss prevention
- Case management and prevention measures
- Controlling and checking for fraud and potential issues
- Taxonomy
- Red flags and schemes
- Compliance guide
- “Know your client”
- Screening and treatment
- Classification and verification
- Reporting suspicious transactions
- Mandatory and ongoing training
- Communications
- Etc.

Specific ethics or conduct policy

Examples of elements considered:

- Codes for employees, directors, officers, and service providers
- Fight against corruption and collusion
- Disclosing conflicts of interest
- Ethics line
- Tip line (whistleblowing)
- Managing detected/reported cases
- Identifying sanctions and disciplinary measures
- Etc.

Theme 2: Integrated Risk Management

In addition to the governance framework, the AMF found that, depending on their size, institutions sometimes assign a specialized risk management team **specifically to the fight against financial crime and fraud**. In all cases, such responsibilities fall within the purview of a high hierarchical level within the institution (e.g. the second line of defence) and are carried out independently of supervised operations. The designated person therefore has direct access to the board of directors or a board committee.

The AMF also found that sound risk management involved **the input or collaboration of areas of the business** other than risk management, including:

- Legal affairs;
- Human Resources (e.g., in the case of consequences or disciplinary measures for employees);
- Compliance;
- Procurement (e.g., in the management of contracts or third parties);
- Chief Information Security Officer;
- Chief Technology Officer;
- Privacy Officer;
- Chief Data Officer;
- Fraud Manager;
- Internal Audit.

In best practices, financial crime risks are identified while taking into account **other risks** to which the institution is exposed (e.g. operational risks, information and communications technology (ICT) risks, and non-compliance risks) and the institution's vulnerability to **internal and external factors**.

Examples of Factors Considered when Identifying Risks

Internal factors	**External factors**
• Nature of activities • Product features • Development of new products • Distribution model • Clients' risk profiles • External business relationships • Information technology systems used • Geographic location • Employee experience • Etc.	• Economic and social context • Geopolitical context • Technological and regulatory changes • Methods used to commit financial crime-related acts • Historical record of external incidents • Etc.

The financial institutions consulted conduct a **review of the risks and environment** to which they are exposed:

- On a periodic basis, adhering to a predefined frequency (e.g., every two to three years). or on an ad hoc basis where circumstances warrant;
- Quarterly for institutions that operate in a constantly evolving risk environment;
- Targeting specific activities or products when required;
- Considering the **activities carried out by the third parties** with whom they do business; and
- Using their own **risk taxonomy** to ensure that all types of risks are inventoried. Those risks differ depending on the institution's area of activity, size, and business environment.

The ICT and controls risks associated with specific scenarios are illustrated in Appendix 1 in order to clarify the issues and the means by which the institutions address these types of risks.

Some institutions group risks into risk families, which facilitates the identification of similar causes so that a range of measures can be implemented, including some, like controls, that are common to a set of risks.

The **means used to counter financial crime risks** include, but are not limited to, applying effective controls, leveraging data to detect threats, and using technologies that enable an effective response.

As for **cybersecurity**, using a multi-layered approach ensures that if a control is compromised, another control can take over to protect information.

Here are some examples of controls and more specific means used by financial institutions.

Examples of Controls	
Segregation of duties	Transaction approval thresholds by employee level
Dual approval of large/sensitive transactions	Information matching
Data analysis	Background checks (employees, business partners and service providers)
Multi-factor authentication	**Other Means**
Access controls and managing system privileges	Code of ethics and professional conduct
Logging accesses	Mandatory training at the time of hire and on a recurring basis

Theme 3: Reporting

Reporting to the appropriate governance bodies is a key step in sound governance. The AMF found that those responsible for managing financial crime risks report to the **board of directors or a board committee** such as the audit committee or the risk management committee, which also considers ICT risks, so that the board or committee members:

- Are given an overall picture of the institution's situation with respect to financial crime risk management, providing them with assurance that the institution is in compliance with the applicable laws, regulations and guidelines.;
- Are able to identify controls to be corrected or implemented;
- Are able to track trends;
- Are made aware of and able to assess the magnitude of exceptional events that could increase certain risks; and
- Can monitor evolving risks.

The topics of such reports include, without being limited to:

- Emerging risk monitoring;
- Certain higher-risk occurrences, which are also the subject of specific and direct communication to the board of directors or the audit and risk management committees, either in the context of such reports or on a more frequent basis if necessary;
- Trends;
- Main causes;
- Checks performed for higher-risk issues; and
- Ongoing remediation work or requested actions to address more significant risks.

More detailed information is also shared, with the necessary modifications, across all hierarchical levels via operational risk dashboards displaying data as ratios or trends, for example.

The following figure presents **fraud-specific indicators** that are tracked by the institutions and may be included in this type of reporting.

The reports usually also provide information on preventative measures, including the number of training sessions given, the tests performed on various controls, and frameworks that are in the process of being updated.

Fraud-specific indicators
Number of fraud cases by quarter, product and sector
Fraud amounts (on average, by minimum/maximum), ratios/trends
Total losses related to fraud, overall, by sector and fraud type, ratios/trends
Effectiveness of existing controls
Comparability with other institutions of the same size in the same sector
Root cause identification rate by fraud type

Theme 4: Fraud Impacting Clients

In addition to the activities carried out to identify governance and risk management practices, the cross-cutting supervisory review included work focused specifically on fraud impacting clients. In connection with this, meetings were held with selected institutions to identify good practices in preventing fraud, assisting clients who are fraud victims, and protecting vulnerable clients.

With respect to good **prevention** practices, the AMF found that some financial institutions:

- Are active participants in **information sharing communities** that strive to keep community members informed of the latest fraud trends, share information on fraudsters' modus operandi, and strengthen collective vigilance in the industry. Such communities can be comprised of groups internal to an organization, various entities of the same financial group, or a number of provincial, national or international financial institutions.
- Maintain a **training program** for teams, officers and third parties that includes certain mandatory training activities. These programs are intended to teach first-line stakeholders how to recognize fraud schemes that impact clients and act quickly to reduce the risk for clients. Such training is dispensed at the time of hire and then on an ongoing basis (e.g. annually or when warranted by new circumstances).
- Have an anonymous **reporting line** so that clients and employees can report situations potentially related to fraud attempts. Reporting lines help create a safer environment and encourage the proactive detection of suspicious behaviours. Reports are handled confidentially and anonymously by an independent entity such as the internal audit function or a specialized outside firm. When circumstances warrant, reports are submitted to a committee such as the compliance and ethics committee so that appropriate action may be taken.

Several institutions have formally defined the concept of a **vulnerable person**. This good practice typically draws on the definition proposed by the AMF in its guide entitled *Protecting vulnerable clients: A practical guide for the financial services industry*.

This guide has also inspired other good practices for **protecting vulnerable clients**, including:

- Identifying a trusted contact person when creating or updating records;
- Documenting the client's written authorization to contact the trusted contact person, indicating the situations in which the trusted contact person may be contacted and the type of information that may be disclosed to that person;
- Defining signs of vulnerability and financial mistreatment to look for (e.g. unusual transactions, sudden changes in behaviour, interference by a relative);
- Offering clients the possibility of being assisted by a person they trust;
- Implementing a graduated response process if mistreatment is suspected;
- Designating an internal resource person for situations involving vulnerability or mistreatment;
- Training employees and representatives on identifying high-risk situations, the role of the trusted contact person, and the documentation expected in the file.

Certain financial institutions expressed reservations related to the **operational limitations** they face. Though warnings are issued to them, clients are free to perform whichever transactions they want. This creates a gap between the intended objective of prevention and the actual ability to prevent certain situations, especially where a client exercises full decision-making autonomy despite the risks that are identified or made know to the person by the institution.

When it comes to **assisting clients who are fraud victims**, institutions reported that they typically follow the good practices below when an incident occurs:

- Designating a contact person to provide ongoing follow-up on the situation;
- Developing criteria to determine the causes of the fraud and support decision making regarding possible client compensation.

Other Tools and Assistance Available from the AMF

The AMF has published content on its website to help empower financial institution stakeholders, including:

- Protection of data and personal information (in French only)
- Application of the United Nations Resolution to Suppress Terrorism
- Information Security Incident Management

Other content is available to provide clients with the awareness and tools needed to protect themselves against different types of fraud and fraud scams.

Financial sector clients and stakeholders can also contact the AMF Information Centre for information or assistance at 1-877-525-0337.

The AMF's expectations are outlined in the following guidelines and regulation:

- *Financial Crime Risk Management Guideline*
- *Governance Guideline*
- *Guideline on Information and Communications Technology Risk Management*
- *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents*

Conclusion

It can be concluded from the review forming the basis of this report that institutions are cognizant of growing financial crime risks, particularly as they pertain to information and communications technologies, and of the impact that financial crime can have on their activities.

The review also allowed the AMF to identify opportunities for improvement and aspects that require clarification. For example, the AMF found that there is a need to further formalize its expectations regarding assistance offered by financial institutions to clients who are fraud victims. The AMF will be exploring various options to address this need in order to support the industry.

As stated in the AMF's *2026-2027 Annual Statement of Priorities* (in French only), changes to national and international regulations are bearing out the need to update the *Financial Crime Risk Management Guideline*. The AMF will work toward this in 2026–2027, drawing on the findings of this review, with the aim of helping to ensure that clients who are fraud victims are treated more fairly.

Until the guideline has been updated, financial institutions are encouraged to draw on the good practices outlined in this document and integrate them into their activities in a manner proportionate to their risk profile.

Appendix 1 - Management of Information and Communications Technology Risks

Access management

Fictitious scenario[1]

An employee transferred to another area of the institution continues to hold the privileges assigned to them in their previous role, including transactional authorizations allowing them to modify or approve certain client records.

Risks

This situation can generate several risks, including:

- Risk of data error or manipulation, whether intentional or otherwise;
- Risk of internal fraud due to transactional access privileges that persist needlessly;
- Risk of conflict of interest due to the change in roles;
- Risk of non-compliance and segregation of duties breach;
- Information integrity risk if undetected actions are carried out.

Examples of identified mitigation measures and good practices

Rigorous management of the access lifecycle is crucial. It may include the following processes:

- Revocation of rights and privileges;
- Regular review or certification of access rights and privileges (formal mechanisms to ensure that a change in roles triggers the timely review and revocation of rights and privileges that are no longer required);
- Application of the principle of least privilege (aligned with current employee responsibilities and periodically reviewed, especially for high-privilege accesses);
- Alignment between an employee's current role and the authorizations associated with that role;
- Segregation of duties between operational roles and monitoring roles, such as compliance and risk management, to prevent conflicts of interest and reduce the risk of internal fraud;
- Activity logging, traceability and monitoring.

1 The scenarios in this appendix have been developed to illustrate potential risks and share good practices implemented to mitigate them. They are not actual cases.

Phishing

Fictitious scenario

An employee receives an email that appears to be from the institution's IT security team. It states that an urgent update of the authentication system is required and provides a link to a page made to look like the internal login portal.

The employee clicks on the link and enters their login information, which is then used by fraudsters to attempt to access the institution's internal systems.

Risks

This situation can generate several risks, including:

- Risk of privacy breach (critical), abuse and fraud:
  - Potential exposure of personal, confidential and financial data;
  - Targeted fraud, identity theft and phishing;
  - Possible ransomware attacks;
  - Integrity breach;
  - Compromised systems/lateral movement activity.
- Regulatory risk (e.g., disclosure obligation);
- Reputational risk.

Examples of identified mitigation measures and good practices

Examples of good practices include:

- Information security training and awareness initiatives for all users;
- Phishing tests for all employees, including senior management and the board of directors;
- Detection and verification of phishing e-mails;
- Verification of internet accesses to filter out malicious sites;
- Deployment of an endpoint security system to detect and rapidly respond in the event a system is compromised;
- Inclusion of a banner on e-mails from outside the organization;
- Multi-factor authentication (MFA) or the use of passkeys for any access from outside the organization.

Internal theft/fraud

Fictitious scenario

A malicious employee uses their privileged access to discreetly manipulate data in several claims in order to redirect payments to fraudulent accounts that the employee controls.

Risks

This situation can generate several risks, including:

- Risk of abuse and fraud:
  - Stolen data used to attempt to access accounts or conduct fraudulent financial transactions;
  - Financial losses;
  - Reputational risk.

Examples of mitigation measures and good practices

Examples of good practices include:

- Increased monitoring of access privileges (modification of more sensitive fields such as client contact and banking information) and how the privileges are used;
- Identity and access management (IAM):
  - Segregation of duties and application of the principle of least privilege;
  - Ticketing system for authorizing privileged accesses;
  - Vault that assigns single-use passwords for this type of access, which are logged.
- Active fraud monitoring: Bolstering rules, increasing checks at the contact point, behaviour detection, e-mail confirmations/warnings when client contact information is changed;
- Pre-hire inquiries.

Third party

Fictitious scenario

An external cloud service provider in charge of managing a financial institution's client records is the victim of a targeted intrusion. The perpetrators are able to extract a dataset that includes personal information and sensitive financial information.

Risks

This situation can generate several risks, including:

- Risk of privacy breach (critical):
  - Exposure of personal and financial data.
- Heightened risk: Fraud, identity theft, targeted phishing attacks;
- Regulatory risk (e.g. disclosure requirements, risk of sanctions or non-compliance);
- Reputational risk;
- Operational risk resulting in:
  - Activation of an incident response: analyses, communications, coordination of legal resources;
  - Disruption of operations if the service provider is unavailable.
- Third-party risks arising from:
  - Control deficiencies at the service provider;
  - Potentially inadequate contractual clauses (notification, audits and responsibilities).

Examples of mitigation measures and good practices

Examples of good practices include:

- Prior assessment of third-party risk and requiring the third party to comply with security practices and/or hold security certification such as SOC 2 Type 2 or a certification specific to the area of business;
- Bolstering access controls associated with the server provider (immediate rotation of keys, tokens, accounts, and multi-factor authentication);
- Active fraud monitoring: Bolstering rules, increasing checks at the contact point, behaviour detection;
- Flow and permission limits on the service provider (segmentation, minimum amount of access, suspension of non-essential exchanges);
- Timely notification (institution's managers/officers and decision-making bodies; the Commission d'accès à l'information; the AMF; and clients) and activation of a clear and transparent communications plan to reduce reputational risk;
- Requiring the supplier to provide a control remediation and improvement plan and proof that deficiencies have been addressed, and conducting a contractual review (inclusion of audit rights and notification timeframes).

Toll fee: 1-877-525-0337
lautorite.qc.ca

Québec City
418-525-0337
Place de la Cité, tour PwC
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Montréal
514-395-0337
800, rue du Square-Victoria, bureau 2200
Montréal (Québec) H3C 0B4