Québec's AMF lays out its expectations for the use of AI

May 12, 2026

The Autorité des marchés financiers (AMF) has recently published its Guideline for the Use of Artificial Intelligence (the Guideline) aimed at the financial sector, which will come into force in about a year, on May 1, 2027.

This Guideline is the first to be issued by a provincial financial sector regulator on the use of artificial intelligence. It adds to the growing number of regulatory expectations from other financial sector regulators, including Guideline E-23 from the Office of the Superintendent of Financial Institutions and Staff Notice and Consultation 11-348 from the Canadian Securities Administrators (CSA).

The Guideline is primarily aimed at ensuring that financial institutions establish governance and risk management mechanisms for artificial intelligence systems (AISs) throughout their entire lifecycle.

Who does this Guideline apply to?

The Guideline applies to all financial institutions that use AISs and are subject to supervision and oversight by the AMF. This includes authorized insurers, financial services cooperatives, authorized trust companies and other authorized deposit institutions in Québec.

The Guideline defines an AIS as:

> a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

It also notes that "different AISs vary in their levels of autonomy and adaptiveness after deployment."

This definition is based on internationally recognized governance and risk management principles, and draws substantially on the definition developed by the OECD, as well as CSA Staff Notice and Consultation 11-348.

What are the AMF's key expectations?

Governance

Under the Guideline, the board of directors plays a crucial role in sound AI governance. The board is expected to proactively:

- ensure that senior management promotes a corporate culture focused on the responsible use of AI;
- be regularly apprised of trends, risks and changes arising from AISs that could alter the institution's risk profile; and
- ensure that the collective competency of the board is sufficient to understand the risks, particularly when the AISs are used to carry out critical operations.

Senior management, meanwhile, must ensure adequate oversight of AISs (including governance, risk management and control, AIS knowledge and validation adapted to the technologies in use).

The AMF also expects that a member of senior management will be accountable for all AISs within the institution. It further specifies that AISs must be under the responsibility of the model owners throughout their entire lifecycle. Model owners are the individuals or teams who select the model to be used and coordinate its development, implementation and deployment.

Risk management

The AMF expects financial institutions to rigorously manage material risks associated with AIS use across the institution so that it has a holistic view of such risks.

In this regard, the Model Risk Management Guideline also requires institutions to establish and maintain a centralized AIS inventory. AIS-related models must be subject to an overall risk assessment, the results of which must be reported periodically to key stakeholders, including model owners, managers of teams using or validating them, and senior management.

Risks to consider include non-compliance with personal information protection legislation when using client or employee information, bias or discrimination in automated decisions affecting clients' rights and obligations, and misalignment between the institution's ethical positions and AIS outcomes.

The Guideline also emphasizes that financial institutions must select and use AISs that provide significant support in meeting the financial institution's needs and produce reliable outputs suited to their intended use. This applies to the data, systems and technological tools used by financial institutions for support in meeting operational needs, making decisions or assessing risks.

Risk assessment

Financial institutions must manage AISs using a risk-based classification. Each AIS must be assigned a risk rating and updated regularly. The risk assessment process

described in the Guideline resembles the data risk matrix exercises that many institutions have conducted in recent years.

The Guideline sets out several factors to consider in the risk assessment, including an estimate of the potential operational impact, the level of the AIS's autonomy and the associated compliance risks. A provisional risk rating should be assigned during the initial assessment and may be revised once complete information is available.

This risk-based approach should allow for adjustments to validation and documentation activities, the requisite level of approval, the nature and frequency of monitoring activities, and the risk rating review schedule. Commensurate with the institution's risk appetite, risk ratings should also be used to adjust the constraints placed on AISs, the level of monitoring, and the controls and mitigating measures for managing residual risks.

That said, institutions retain discretion in determining risk ratings, which are intended to be an internal management tool.

AIS lifecycle

Financial institutions must establish governance mechanisms and documents, such as policies, processes, procedures and controls, to support the expectations for each stage of an AIS's lifecycle in a manner commensurate with the risk rating. In particular, they must:

- document their organizational needs and rationale for using an AIS (and reassess when the AIS needs to be revalidated);
- ensure the quality of the data used, both during training and while the AIS is in use (primary and secondary data, private and public data, real and synthetic data, and structured or unstructured data);
- include the AIS's risk rating and explainability requirements (and, where necessary, cybersecurity targets) in its selection criteria. These requirements may be adjusted based on the AIS's intended purpose, its level of autonomy, applicable regulatory requirements and potential impacts;
- conduct assessments tailored to the objectives and risk (e.g., output explainability, cybersecurity, timeliness of methods and review of third-party components);
- regulate the use of higher-risk AISs (or those for which the information is incomplete) through mitigating measures and restrictions commensurate with the institution's risk appetite;
- monitor integration, performance and use, and establish standards for risk level-based monitoring.

Finally, when an AIS involves the processing of personal information, the institution must conduct a privacy impact assessment (PIA) in accordance with the requirements of the *Act respecting the protection of personal information in the private sector* (the Private Sector Act). See our recent publication, Québec's Private Sector Act: Compliance guide for organizations, for more information.

Fair treatment of clients

The Guideline also addresses fair treatment of clients by reference to the AMF's Fair Consumer Practices Guideline, and sets out additional expectations tailored to the use of AISs.

In this regard, it emphasizes the importance of identifying and mitigating risks of discrimination and bias. Institutions should develop a list of factors and surrogate variables that may not be used because they would be discriminatory given the intended use of each AIS. They should also communicate such lists to stakeholders in a timely manner.

Transparency

With respect to client communication, institutions should inform clients when they enter into any dynamic method of communication (whether written, audio, video or other) with an AIS and advise them that they can request to speak with an individual acting on behalf of the institution. For example, this requirement could apply to the use of a voice chatbot in a call centre that interacts with clients, answers their questions or handles their requests.

Any content generated with the help of an AIS should be accompanied by a notice to that effect. Finally, where clients are subject to a decision made or recommended by an AIS, the institution should explain the decision in clear and easy-to-understand language.

What are the first steps to ensure compliance?

BLG's attorneys have prepared a checklist of practical steps to help you meet the AMF's expectations.

1) AIS inventory

- Establish a centralized inventory of all AIS (in production, testing/piloting or development) and keep it updated.
- Identify "critical operations" and use cases where an AIS may influence decisions, recommendations or content with significant impact.

2) Governance and accountability

- Designate a member of senior management to be accountable for all AISs.
- Designate model owners (per AIS) who cover the entire lifecycle.
- Ensure that the board of directors is regularly apprised of evolving trends, risks and material changes resulting from the use of AISs that could potentially alter the financial institution's risk profile.
- Identify training needs for the board of directors and senior management regarding the AISs in use and their associated risks, especially when the AIS supports critical operations.

3) Risk management and classification

- Identify, document and update the significant risks associated with AISs on an institution-wide basis.
- Establish a consistent methodology for assigning a risk rating to each AIS (including a provisional risk rating when information is incomplete).
- Schedule periodic reviews of risk ratings and mitigation measures.
- Communicate the results of comprehensive risk assessments periodically to key stakeholders (AIS owners, managers and senior management).

4) AIS lifecycle

- Document organizational needs and the rationale for using an AIS.
- Implement data quality requirements during training and in use (accuracy, bias, relevance, etc.).
- Include explainability requirements (and, where necessary, cybersecurity targets) into selection and procurement criteria.
- Tailor assessments to the objectives and risk level of each AIS (e.g., output explainability, cybersecurity, timeliness of methods, review of third-party components).
- Regulate the use of higher-risk AISs (or those for which the information is incomplete) through mitigating measures and restrictions commensurate with the institution's risk appetite.

5) Personal information and privacy

- Conduct a privacy impact assessment (PIA) when an AIS involves processing personal information, in accordance with applicable regulations.
- Regulate access to, retention of, traceability of and deletion of data used by AISs.

What changes were made to the final version of the AMF's Guideline?

For those familiar with the draft Guideline, the BLG team has identified the most significant changes made in the final version and compiled them in a Q&A format.

Does the Guideline apply to all uses of AISs?

- Yes. The AMF's new Guideline explicitly states that it now applies to any use of AISs, including situations that do not involve the handling of client records.

What expectations have been removed compared to the draft Guideline?

- Risk management function: The AMF previously stated that it expected the risk management function to play a role in AIS validation, the development of a risk taxonomy and the management of sources of risk. In the final version, however, the AMF does not assign a specific role to this function.
- Internal audit: The AMF no longer refers to internal audit in the final version of the Guideline.

- Web scraping: The previous version stated that secondary data obtained through web scraping had to adversely affect an AIS's risk rating. However, all references to web scraping have been removed from the Guideline.
- Ongoing monitoring: While maintaining the general expectation of ongoing monitoring, the AMF has removed the list of specific elements that should be subject to ongoing AIS monitoring.

What new expectations were added?

- Monitoring standards: The AMF states that it now expects standards for risk level-based monitoring of AISs to be established. These monitoring standards will serve as guideposts for the monitoring of AISs with features that present unique challenges, such as autonomous AISs or AISs with dynamically adjusted models.

What expectations were modified?

- Validation process: The AMF now recommends conducting different assessments for the AIS validation process, including an explainability assessment, an analysis of the timeliness of AIS-related processes and a review of AIS components sourced from a third party. Assessments of bias analysis and correction, as well as discrimination analysis, have been removed.

The authors would like to thank Marianne Bellavance, student-at-law, for her contributions to this article.

By

Frédéric Wilson, Guillaume Talbot-Lachance

Expertise

Banking & Financial Services, Artificial Intelligence (AI), Technology, Financial Services, Financial Services Regulatory

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749