AUTORITÉ
DES MARCHÉS
FINANCIERS

GUIDELINE APPLICABLE TO CREDIT ASSESSMENT AGENTS

February 2023

TABLE OF CONTENTS

Introduction

Credit assessment agents ("CAAs") collect, use, compile, produce and disclose consumer[1] data in accordance with applicable legislation.

Businesses such as financial institutions use the consumer credit data provided by CAAs in the course of their day-to-day operations.

Given the significant role played by CAAs in the financial ecosystem, the Autorité des marchés financiers (the "AMF") has been empowered under the *Credit Assessment Agents Act*[2] (the "Act") to supervise and control the commercial practices and management practices of CAAs and to issue expectations regarding such practices,[3] protection measures, the rights of persons concerned, remedies and complaints.[4]

The AMF prefers a principles-based approach to implementing these expectations and therefore provides CAAs with the latitude necessary to determine the requisite strategies, policies, procedures and processes and apply them based on the nature, size and complexity of their activities.

1. Governance

Sound governance is crucial and constitutes the cornerstone of appropriate management by a CAA that ensures that consumers' rights under the Act are respected.

With this in mind, the AMF wants to ensure that CAAs implement and follow appropriate management practices while instilling and promoting a business culture based on ethical organizational behaviour and decision-making body accountability.

By business culture, the AMF means the common values and standards that characterize a business and influence its mindset and conduct and the actions of its personnel. A good business culture is therefore essential to maintaining consumer confidence, while a deficient corporate culture can cause significant damage to a business's reputation and serious harm to both the business and its various stakeholders.

For a CAA to be governed effectively and efficiently, a formal operating, supervisory and accountability framework must be implemented through policies, procedures and information systems that help to organize and monitor the way the CAA is managed. Effective and efficient governance also requires risk management and control processes to be implemented across the organization using a rigorous, coordinated approach.

CAAs interact, in particular, with financial institutions and manage consumers' personal data. Given the sensitivity and importance of the data held by CAAs, the AMF believes it is essential that they draw on the three lines of defence model to

1 Referred to as a "person concerned" in the *Credit Assessment Agents Act*, a "consumer" in this guideline means the person who is the subject of the credit report or the representative of that person.

2 *Credit Assessment Agents Act* (S.Q. 2020, c.21)

3 See sections 53 and 54 of the Act.

4 See section 28 *et seq.* of the Act.

- promote careful coordination among the risk management and control functions
- structure management of the risks associated with their activities subject to the Act
- meet the same standards as their main commercial partners

Specifically, the AMF is issuing the following expectations for observance of the provisions of the Act in order that CAAs may ensure compliance with those provisions and guarantee that consumers are able to fully exercise their rights.

The outsourcing of the various functions identified below should be disclosed to the AMF upon request.[5]

First line of defence

The first line of defence is a CAA's operational management. It is responsible for managing risks on a day-to-day basis because controls are designed, pilot-tested and integrated into systems and processes under its guidance. Its responsibilities should include:

- identifying, assessing, managing and controlling the risks related to the requirements of the Act
- guiding the development and implementation of internal control procedures
- overseeing the application of those procedures by their employees
- ensuring that activities are consistent with goals and objectives
- ensuring that activities are carried out in compliance with the Act

Operational managers should also take corrective actions to address process and control deficiencies.

Internal control is also a key component of an effective governance structure because it enables the detection of functional deficiencies that could be major sources of risk for a CAA. As a result, the constituent controls should be designed and operated to ensure that the CAA's key policies and processes are effective in ensuring that consumers' rights under the Act are respected.

These controls should, in particular, cover the following:

- The appropriate segregation of duties, where necessary
- Decision approval policies
- The presence of controls adapted to each appropriate level of the organization
- Internal control training, particularly for employees with key responsibilities
- Consistency of internal control overall and for each individual control

[5] Refer to sections 50 and 51 of the Act.

- Verifications and tests by independent parties (internal or external auditors) to determine the effectiveness of existing controls

Since staff at all levels of a CAA are involved in internal control, they should be made aware of the importance of the constituent controls and receive clear communications from senior management for that purpose. It is therefore essential to identify and compile the relevant information and provide it to the individuals concerned in a form and within a timeframe that allows them to properly fulfill their responsibilities.

The exercise of identifying, compiling and communicating information should help to ensure that internal controls adequately meet the objectives intended to ensure compliance with the Act, including the obligation to adhere to sound commercial practices. Specifically, the assessment of the effectiveness of internal controls should include the following:

- The control strategy adopted
- The control reference framework
- Completion status of the implementation or update
- Information regarding the resources needed to ensure internal control operating effectiveness
- A description of identified issues and deficiencies

Second line of defence

The risk management and compliance functions serve to ensure that internal controls are properly designed, effective and operating as intended and that the applicable laws, regulations and standards are complied with.

In order to be effective and properly fulfill their role in the second line of defence, the risk management and compliance functions should have sufficient authority, be appropriately positioned in the hierarchy, be independent from operational management, have the necessary resources to exercise their roles, and have unrestricted access to the decision-making bodies.

An effective risk management function in the second line of defence is independent from the risk-taking operational level and closely monitors material and emerging risks.

A compliance function[6] that is independent from the activities it oversees is one of the key components of a CAA's second line of defence and an essential foundation for appropriate management practices as it ensures that consumers' rights under the Act are respected.

[6] A compliance function is not necessarily a specific unit within the CAA. The staff responsible for compliance may be involved in operational units and report to the management team responsible for the activity involved. However, where appropriate, it is important for those units to be able to report to the chief compliance officer or the individual responsible for that function, who should be independent from operational management.

Third line of defence

An effective and efficient independent internal audit function constitutes the third line of defence of the governance framework, providing the CAA, using a risk-based approach, with independent, objective assurance and consulting services designed to add value and improve the organization's operations.

With respect to appropriate management practices and sound commercial practices, internal audit must assess the design, adequacy and operational effectiveness of processes and make appropriate recommendations to improve them. The goal is to provide the decision-making bodies with objective assurance that the processes are properly designed, operate as intended and achieve, in particular, the objectives of:

- promoting ethical organizational behaviour that reflects the fair treatment of consumers
- monitoring and reporting organizational performance
- communicating risk and control information to the appropriate areas of the CAA
- coordinating the activities of, and communicating information among, the decision-making bodies, the external auditors and the internal auditors[7]

Internal audit should also evaluate the effectiveness and relevance of risk management and compliance processes and internal controls and promote their continuous improvement, including the achievement of the organization's risk management, compliance and internal control objectives by the functions in the first and second lines of defence.

To effectively fulfil its role as the third line of defence, it is preferable that internal audit have direct and unrestricted access to the decision-making bodies in order to assert its independence and reinforce its objectivity within the CAA.

The three lines of defence model could, however, be adjusted to reflect how roles and responsibilities are allocated within the corporate group to which the CAA belongs, without limiting the CAA's responsibility in this regard and while satisfying the AMF's expectations set out in the section on outsourcing risk management.

[7] The Institute of Internal Auditors. Standard 2110.

2. Sound commercial practices

CAAs have a legal obligation to adhere to sound commercial practices.

The commercial practices, or conduct of business, of CAAs reflect their behaviour in their relationships with consumers—behaviour that should result in the fair treatment of consumers (FTC).

FTC draws on guidance issued by various international bodies.[8] It encompasses concepts such as ethical behaviour, acting in good faith and the prohibition of abusive practices. FTC involves, among other things:

- Offering services relating to consumers' rights under the Act in a way that pays due regard to the interests and needs of consumers
- Providing consumers with accurate, clear and sufficient information allowing them to make informed decisions
- Protecting the privacy of consumer information
- Processing consumer complaints in a fair and diligent manner
- Making sufficient resources available to consumers, including staff, to facilitate the timely exercise of their rights

Therefore, the AMF expects FTC to be an integral part of a CAA's business culture. Establishing an FTC culture would, among other things, help place consumers' interest at the centre of decisions and the conduct of business and ensure that all staff act ethically and with integrity in their dealings with consumers.

a. Communicating with consumers

CAAs should communicate information to consumers orally or in writing, in plain, simple and precise language, regardless of the means of communication. Such communications should be in French or English, according to each consumer's language preference. Moreover, CAAs should ensure that they have a sufficient number of employees who are properly trained to answer consumers' requests and questions.

For example, if a code or rating system is used in provided materials or technical terms are employed to communicate information, the AMF expects CAAs to explain what they mean in accordance with the good practices set out in this subsection.

A CAA should make means of communication available to consumers that enable them to contact the CAA quickly and efficiently. Such means of communication should be varied (telephone numbers, e-mail addresses, instant messaging, etc.) and easy to locate on all of the CAA's platforms (website, social networks).

[8] Including the principles on financial consumer protection developed jointly by the Organisation for Economic Co-operation and Development and the Financial Stability Board.

CAAs should also take appropriate measures to ascertain the identities of consumers they interact with. CAAs should not disclose a credit report if they are unable to properly ascertain a consumer's identity.

The AMF expects product and service advertising materials to be accurate, clear and not misleading.

b. Managing information in a credit report

CAAs should have a clear, up-to-date policy for managing information contained in a credit report.

Given the sensitive nature of such information, CAAs should have stringent information security standards in place for any data they receive, use and share. CAAs should also have effective processes for periodically reviewing the management of such information.

In addition, the AMF expects a CAA's privacy policy and procedures to draw on best practices and enable it to discharge its privacy obligations, including those under the *Act respecting the protection of personal information in the private sector*.[9]

CAAs should establish and apply an operating method that ensures that the information they communicate is up to date and accurate. To that end, CAAs should ensure that evaluations and reviews are conducted regularly to determine whether the agreements entered into with external providers are being complied with and, if necessary, to address any suspected or observed breaches of the terms of those agreements.

CAAs should have a robust process for validating any changes made to consumers' personal information (e.g., mailing address, telephone number).

c. Processing complaints

The AMF expects complaints to be processed fairly and diligently, following a process that is simple and readily accessible for consumers.

The complaints received by a CAA and the handling of those complaints are, among other things, key elements to consider in assessing the CAA's FTC performance.

The Act requires CAAs to do such things as keep a complaints register and adopt a complaint processing and dispute resolution policy.[10]

The AMF expects:

- the complaint process to take into account consumers' interests and ensure that complaints are handled in an objective and consistent manner
- the CAA to designate a complaints officer who has the authority and competence to perform the function and ensures, among other things, that the complaint processing

[9] *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1

[10] *Credit Assessment Agents Act*, s. 35.

and dispute resolution policy is implemented, disseminated and complied with within the CAA

- staff responsible for processing complaints to have the necessary competencies to process the complaints assigned to them
- consumers to receive proper assistance throughout the processing of their complaint and be informed in a timely manner of the status of their complaint
- consumers not to be faced with constraints or administrative barriers and any need the institution has for additional information not to hinder or delay the complaint process
- the CAA to develop an overall picture of the complaints received in order to identify common causes and the issues to be resolved to ensure FTC

3. Operational risk management

The AMF expects a CAA to adequately manage operational risk related to its business model and the management strategy for such risk. Such management should take into account exposure to operational risks inherent in people, processes, systems or external events, as well as stakeholders' exposure to such risks.

Operational risk management should also identify situations where activities, processes or systems do not ensure FTC. For example, an information security breach caused by the accidental disclosure of consumers' personal information or a deliberate leak of confidential information could negatively affect FTC, which could ultimately harm a CAA's reputation.

Moreover, when a consumer reports that he or she has been, or believes he or she is, the victim of fraud or a related crime, including identity theft, a CAA should, after properly ascertaining the consumer's identity, demonstrate diligence and take appropriate action.

In terms of operational risk, the establishment of a culture that promotes sound risk management must necessarily emanate from the decision-making bodies and be adapted to reflect the extent of exposure to operational risks and, consequently, the requisite commitment of all levels of the organization to properly manage such risks.

Awareness-raising should also extend to external stakeholders, including service providers under material outsourcing arrangements,[11] since outsourcing exposes an organization to operational risks (e.g., exposure to cyber risk).

[11] An outsourcing arrangement that could have a significant impact on an institution's financial condition, its operations and, ultimately, its reputation is considered material.

4. Information and communications technology (ICT) risk management

CAAs should implement an ICT risk management approach that is robust and relies on sources, recommendations and standards emanating from recognized organizations such as the OECD, the G7, NIST, ISACA (COBIT) and ISO. In addition, CAAs should, among other things, ensure that the decision-making bodies promote a business culture based on ethical and secure conduct in using technology.

To that end, CAAs should have an appropriate risk-based framework ensuring information security and the physical security of all their technological infrastructures and information assets.

CAAs should implement their own taxonomies so that all types of ICT risks are identified. ICT risk categories that should be considered include information security, outsourcing, cloud computing, business continuity, crisis management, human resources, ICT operations and ethics. Once developed, this taxonomy should be communicated to those directly involved in risk assessment and control activities so that it may be used consistently in the identification and aggregation of ICT risks.

CAAs should clearly delineate the responsibilities of the information security function to ensure its independence and objectivity by, in particular, segregating it from ICT operational processes or implementing compensating controls where needed. This function should not be responsible for internal audit work.

CAAs should ensure that the following individuals are assigned:

- a member of senior management, such as a chief information security officer, to oversee the deployment of the framework ensuring information security and the physical security of the organization’s technology infrastructures
- a member of senior management, such as a chief data officer, to oversee the approved framework for the collection, storage and use of data across the organisation

CAAs should maintain adequate capacity to anticipate, detect and recover from ICT-related operational incidents, including information security incidents.

Regarding consumers’ rights under the Act, CAAs should, in particular:

- Define in their information security policy principles and rules for safeguarding the confidentiality, integrity and availability of consumers’ information
- Define clear information security objectives for systems, ICT services, processes and people
- Apply the information security policy to all their activities while ensuring that the policy also covers information handled by external stakeholders within the CAA’s scope
- Deploy controls for information assets (data, hardware and software) that are proportional to the criticality and sensitivity of those assets
- Conduct systematic testing to ensure that the controls in place are effective

The preparatory activities considered by CAAs for the management of ICT risks should, in particular, help to safeguard sensitive consumer data against disclosure, leaks or unauthorized access. They should also contribute to ICT environment resilience. These activities should cover, among other things, access controls, authentication, data integrity and confidentiality, activity recording and security event monitoring.

CAAs should take into account the preparation, processing and monitoring activities that need to be carried out to quickly mitigate negative impacts for consumers in the event of an incident or an actual crisis.

CAAs should use a rigorous process to periodically identify information assets and their vulnerabilities in order to appropriately associate risks with them.

CAAs should use a classification framework enabling the criticality of data and information assets (including those managed by external stakeholders) to be defined, as a minimum, according to their availability, integrity and confidentiality requirements. This classification framework should reflect the degree to which an information security incident affecting an information asset has the potential to adversely affect the CAA and consumers or other stakeholders.

CAAs should use ICT incident management processes with adequate resumption and recovery objectives, ensure appropriate and timely monitoring of activities to mitigate the risks recorded in the ICT risk register, and monitor the effectiveness of mitigation measures, along with the number of reported incidents in order to correct them when necessary. CAAs should also conduct specific analyses following a major incident to improve their response and recovery plans.

CAAs should also establish and maintain documentation and information enabling informed stakeholder decision-making regarding ICT risks. The documentation should include, in particular, a register, a description of the impact of ICT risks, a risk and control matrix and existing processes and structures for ICT risk management.

Moreover, CAAs should implement robust mechanisms enabling them to ensure that consumers' rights under the Act are respected. Activities to consider include identity and access management, training and awareness, network segregation and protection of network integrity, data security, protection of endpoint devices (e.g., laptops, tablets, smart phones), verification of software and microcode integrity, and technological protection solutions contributing to system and information asset resilience. Similarly, event and anomaly detection and logging, continuous information system monitoring and detection process monitoring should be considered.

CAAs should ensure that physical and logical access to information assets is restricted to users, processes, devices and activities authorized under their established security policies. Access rights should be granted based on such generally recognized principles as "need to know," "least privilege" or "segregation of duties" and only to authorized personnel and in such a manner as to prevent large data sets from being improperly accessed and security controls from being bypassed.

CAAs should subject their information security controls to various types of periodic independent assessments, tests and reviews as well as penetration testing.

CAAs should implement procedures and processes for reporting information security incidents to concerned parties, including the AMF and consumers, in accordance with existing requirements.

5. Outsourcing risk management

CAAs should identify the various risks related to outsourcing arrangements, particularly ICT risks, in order to be able to adequately assess and manage them.

Outsourcing is defined as delegating to a service provider, over a defined period, the performance and management of a function, activity or process that is or could be undertaken by the CAA itself. Any outsourcing arrangement entered into with a service provider operating outside Canada or that processes, stores or transfers data outside Canada is considered to be offshoring. Outsourcing or offshoring arrangements relating to consumers' rights under the Act must be disclosed to the AMF upon request.[12]

It is essential before entering into an outsourcing arrangement involving the protection measures and consumers' rights set out in the Act that CAAs assess the risks that could result from the use of outsourcing. This assessment should also cover the service provider's ability to provide quality service through components relating to financial, operational and reputational aspects.

The AMF expects CAAs' outsourcing arrangements to be drafted to include the terms governing the relationship, functions, obligations and responsibilities of the parties to the arrangement.

CAAs should monitor their outsourcing arrangements to ensure that commitments are met. In the AMF's view, ultimate responsibility for outsourcing arrangement compliance with the legal and regulatory requirements applicable to the outsourced activities remains with the CAAs even where those activities are performed and managed by service providers.

The AMF also expects CAAs to adequately manage the risks related to any material outsourcing arrangements entered into with the members of its group, if applicable.

Lastly, a CAA's reliance on service providers should not jeopardize its business continuity management.

In the context of outsourcing and cloud computing, CAAs should, in particular:

- Contractually secure their right to audit and their right to access the premises of the cloud computing service provider
- Mitigate supply chain outsourcing risks when suppliers outsource certain activities to other suppliers
- Ensure supplier compliance with security objectives and measures and performance expectations

[12] See sections 50 and 51 of the Act.

While using the services of certain stakeholders may not constitute a form of outsourcing, many of those services are delivered using ICT or involve information that is potentially confidential. Such stakeholders may also be exposed to security incidents. CAAs should assess and appropriately manage the confidentiality breach, integrity breach and availability breach risks associated with the information processed by such third parties.

6. Business continuity

CAAs should adopt a strategy to ensure the continuity of critical business operations and the resumption of disrupted or interrupted business operations within reasonable time limits.

With this in mind, CAAs should assess the impact of operational incidents on their resources, operations and environment and determine the measures to be taken in light of this assessment.

It is therefore essential that CAAs develop a business continuity plan ("BCP") outlining the actions to be taken in the event of an operational incident that has an impact on critical operations. The BCP should, for example, define the procedures and systems required to restore the CAA's operations should its critical operations be disrupted. The BCP should be clear, easy to use, tested and updated regularly. It should also be accompanied by a communications plan. CAAs should notify the AMF as soon as possible when they activate their BCPs and also notify any other interested party that is likely to be affected by the situation.

CAAs should also identify their critical operations and major operational incidents that could disrupt, slow or interrupt them. They should also assess the extent to which critical operations are concentrated at a single site, their interdependence, and their reliance on the same resources, particularly with respect to staff, systems and service providers.

CAAs should consider a set of plausible events and scenarios, including cybersecurity events, in planning and testing disaster recovery and continuity plans.

CAAs should identify all potential individual points of failure in the ICT systems and the architecture of networks supporting consumers' rights under the Act in order to ensure that appropriate measures are taken to mitigate disruption risks.

CAAs should minimize business disruption risk by establishing appropriate processes to manage changes affecting ICT equipment (hardware and software) and procedures involved in ICT system development, delivery, support and maintenance.

To reduce business interruption risk stemming, for example, from the malevolent exploitation of software vulnerabilities, CAAs should establish a framework of secure practices and standards for programming, source code reviews and application security testing for their ICT systems supporting the application of consumers' rights under the Act. Any information and ICT system availability, integrity and confidentiality issues identified in applying such practices should be compiled, monitored and corrected.

The AMF expects a CAA to periodically verify the reliability of its BCP. The business continuity management process should be a dynamic one that takes into account any changes affecting the CAA, its stakeholders and its environment. The CAA should ensure that its service providers have robust BCPs aligned with the objectives of its own plan and do not introduce new unidentified risks for the CAA.

7. Supervision of appropriate management practices and sound commercial practices

In line with its wish to promote the establishment of appropriate management practices and sound commercial practices within CAAs, the AMF, in performing its supervisory activities, intends to assess the extent to which the principles in this guideline are being observed.

Consequently, the effectiveness and appropriateness of implemented strategies, policies and procedures and the quality of oversight and control exercised by the decision-making bodies will be assessed.

The management practices and commercial practices addressed in this guideline are constantly evolving. The AMF expects decision-making bodies of CAAs to inquire into best practices and apply them to the extent that they address their needs.