DRAFT

AUTORITÉ DES MARCHÉS FINANCIERS

GUIDELINE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY RISK MANAGEMENT

June 2019

TABLE OF CONTENTS

Preamble

The *Autorité des marchés financiers* (the "AMF") establishes guidelines setting out its expectations with respect to financial institutions' legal requirement to follow sound and prudent management practices. This guideline therefore covers the interpretation, execution and application of this requirement.

The AMF favours a principles-based approach rather than a specific rules-based approach. As such, guidelines provide financial institutions with the necessary latitude to determine the requisite strategies, policies and procedures for the implementation of principles and to apply them based on their nature, size, complexity and risk profile. In this regard, the guideline illustrates how to comply with the principles described.

AMF Note

The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for the sound and prudent management and sound commercial practices of financial institutions and, consequently, as the basis for the prudential framework provided by the AMF.

This guideline is part of this approach and sets out the AMF's expectations regarding the management of information and communications technology (ICT) risks.

Scope

This guideline is intended for insurers of persons (life and health insurers), damage (P&C) insurers, holding companies controlled by an insurer, financial services cooperatives, trust companies and savings companies governed by the following statutes:

- *Act respecting insurance*, CQLR, c. A-32;[1]
- *Act respecting financial services cooperatives*, CQLR, c. 67.3;[2]
- *Act respecting trust companies and savings companies*, CQLR, c. S-29.01.[3]

This guideline applies to financial institutions operating independently as well as to financial institutions operating as members of a financial group.

As regards financial services cooperatives and mutual insurance associations that are members of a federation, the standards or policies adopted by the federation should be consistent with—and even converge on—the principles of sound and prudent management as detailed in this guideline.

1 Section 325.0.1 and section 325.0.2, par.1(3) and par. 2, of the *Act respecting insurance*.

2 Sections 565.1 and 566 of the *Act respecting financial services cooperatives*.

3 Section 314.1, par.1(3) and par. 2, of the *Act respecting trust companies and savings companies*.

Coming into effect and updating

The *Guideline on Information and Communications Technology Risk Management* comes into effect on June 1, 2019.

With respect to the legal requirement of institutions to follow sound and prudent management practices, the AMF expects each institution to have developed strategies, policies and procedures based on its nature, size, complexity and risk profile.

The AMF expects the financial institution to assimilate the expectations set forth in this guideline and implement them by June 1, 2020. Where an institution has already implemented such a framework, the AMF may verify whether it enables the institution to satisfy the requirements prescribed by law.

This guideline will be updated based on developments in ICT risk management and observations noted during monitoring of the financial institutions covered.

Introduction

The rapid pace of technological innovations has contributed to transforming financial institutions' processes and business models. These innovations have, in turn, introduced considerable risks at a time when institutions are becoming increasingly interconnected and dependent on legacy systems[4] and external suppliers to fulfil their mandates.

The adoption of technological innovations has also exacerbated the risk of loss, theft, corruption and unauthorized access to data. Institutions are facing an ever-greater risk of cyber attacks, which are becoming increasingly sophisticated, frequent, targeted and difficult to detect. Cyber risks can have significant negative financial and legal impacts as well as impacts on clients and on the institution's reputation that should not be underestimated.

In this context, ICT risk management[5] should be thorough and robust and support key disciplines such as strategic planning, outsourcing, change management, information security (including cyber security), business continuity and data management.

This guideline specifies the AMF's expectations as regards ICT risk management. It presents the AMF's position, which will evolve as knowledge in this area comes to light through oversight activities and the development of international frameworks.

It is important to note that this guideline does not cover all aspects of ICT risk management. Rather, it focuses on those areas which the AMF deemed relevant when it prepared this document. Each institution is responsible for clearly understanding the risks it faces and for ensuring that those risks are given consideration commensurate with the institution's nature, size, complexity and risk profile.

[4] A legacy system is a piece of hardware or software that continues to be used in an organization despite being superseded by more modern systems. It forms part of an organized set of resources for collecting, storing, processing and distributing information.

[5] The AMF defines ICT risk as the business risk associated with the use, ownership, operation and adoption of ICT. This risk includes availability, continuity, security (including cyber security), change, data integrity and outsourcing risk.

1. Information and communications technology governance framework

The AMF expects financial institutions to identify, assess, control, mitigate and continuously monitor ICT risks. Institutions should establish and maintain a strategy and a management framework specific to these risks and adequately developed on the basis of recognized sources, recommendations and standards.

In addition to the AMF's general expectations set out in the Governance Guideline, the AMF has the following expectations as regards ICT governance.

The board of directors[6] must ensure the establishment and continued existence of an ICT governance framework and a clear definition of the roles and responsibilities required to achieve the institution's ICT governance objectives. As such, the board should, in particular:

- continually exchange information with stakeholders in order to document its understanding of needs and make judgments about the current and future design of ICT governance;
- ensure the implementation of the ICT governance framework in accordance with precepts[7] (section 1.5), decision-making models and agreed-upon authority levels;
- define the information required for informed decision-making (section 1.7);
- monitor the effectiveness and performance of ICT governance;
- assess to what extent ICT governance and the mechanisms put into place (including structures, framework design principles and processes) are operating efficiently and producing appropriate ICT monitoring.

In addition, it must ensure that risk appetite (section 2.2) and the level for ICT risk are understood, articulated and communicated, and that the risk of ICT use is identified and managed. As such, the board should, in particular:

- review and assess the current and future effect of using ICT within the institution;
- ensure the establishment of risk management to provide reasonable assurance that ICT risk management practices do not exceed the institution's risk appetite;
- track the key metrics and objectives of ICT risk management processes.

6 References to the board of directors may include a board committee established for example to examine specific issues.

7 Required conduct, rule (or set of rules) to be observed, generally formulated by an uncontested authority in a specific field.

The board must ensure that sufficient and adequate ICT resources (section 1.1) (individuals, processes and technologies) are available to support business objectives.

It must also ensure that assessment and reporting of ICT performance and compliance are transparent and that stakeholders approve the objectives, metrics and remedial measures. As such, the board should:

- review and assess current and future ICT usage needs for stakeholder communications and reporting;
- establish communication principles and ensure implementation of mechanisms for enhancing the quality and completeness of information (section 1.7).

1.1 Competencies

The AMF expects the board of directors to ensure that its members and decision-making bodies[8] have the required knowledge and understanding of ICT use, directions and trends, as well as the authority to fulfil their responsibilities.

Effective and efficient governance that includes information and communications technology and innovations related to ICT use requires an appropriate level of expertise, professional qualifications, knowledge or relevant experience.

These attributes should be initially assessed and subsequently maintained through a policy for evaluating members of the institution's decision-making bodies according to the applicable competency criteria. The policy should be periodically applied to individuals named, to strategic positions related, to ICT governance and risk management so as to ensure that the established criteria are met on an ongoing basis.

The appropriate level of board expertise, professional qualifications, knowledge or experience may be achieved collectively, i.e., through the complementary attributes of the individuals serving on the board.

Given the dynamic nature of ICT risk, the financial institution could consider a more frequent periodic update of the IT aptitude and knowledge grid it uses to assess the skills of members of the institution's decision-making bodies.

Financial institutions should therefore regularly take stock of all current internal ICT skills present within the institution and those needed to carry out strategies and reach goals.

ICT risk management stakeholders have a number of roles requiring distinct skill-sets and objectives tied to varying levels of education, qualifications, experience, knowledge, and technical and/or behavioural abilities. In addition, these skills evolve over differing life cycles.

[8] For ease of reading, the generic expression "decision-making bodies" will be used to refer to members of the board of directors, to senior management and to those in charge of supervision.

For an understanding of ICT system vulnerabilities and threats, a basic knowledge of an ICT system's components and how they are physically and logically interconnected is needed. Moreover, it is crucial to have expertise in threat sources, threat scenarios, vulnerability and the impact on business. This refers to the nature and basic components of ICT risk and the continuous improvement required to handle the ever-changing nature of threats, vulnerabilities and impacts.

To minimize the risk of board members and the chief executive officer lacking ICT experience, the board should develop a formal process for building skills in the area of ICT-related strategic issues.

Managing a financial institution implies an in-depth understanding of the institution, its operational environment, culture, sector or sectors of activity and risk profile. This knowledge may also encompass areas such as ICT-related implications, opportunities, threats and innovations. With this in mind, in order for the board of directors to be able to understand and influence compromises between flexibility, stability and the operational performance sought in developing ICT systems that support business architecture, it is essential that financial institutions propose formal mechanisms for creating and maintaining documentation regarding the ICT environment (section 1.6).

1.2 Roles and responsibilities

The AMF expects financial institutions to clearly establish and document the roles and responsibilities of ICT governance stakeholders so that the individuals accountable and responsible for the various tasks can be identified.

The documentation should also make it possible to identify the stakeholders who should be consulted and informed when ICT governance practices are developed and implemented, so as to promote transparency and cooperation within the corporate culture.

Board of directors

The AMF expects the board's mandate to specifically mention the roles and responsibilities of its members in respect of ICT and ICT-related innovations.

In connection with the roles and responsibilities usually attributed to the board, it should, in particular:

- ensure that the financial institution acts in accordance with applicable laws, regulations and standards, including the *Act respecting the protection of personal information in the private sector* and the *Act to establish a legal framework for information technology*;
- ensure that senior management promotes a corporate culture based on ethical organizational conduct. The use of massive amounts of data made possible as a result of new technologies may increase the risk of unethical conduct within organizations.

It is important for the board of directors to have a clear understanding of the strategic importance of ICT and the risks associated with the use of ICT and its data.

The board of directors should consider these specific actions pertaining to ICT risk management responsibilities:

- examine ICT frameworks, including reporting requirements, in order to evaluate their relevance and completeness;
- examine the hypotheses and analyses that help to identify key ICT risks;
- examine the types of ICT risks that the institution faces, the interrelationship between risks, their probability of occurring, their potential impact and any mitigation measures and action plans.

In terms of the institution's information security, the board of directors should ensure that:

- the institution maintains a level of security that is proportional to the magnitude and scope of the threats on its information assets and that allows it to function properly;
- the controls used to protect its information assets are proportional to the criticality and sensitivity of its assets;
- the institution undertakes systematic testing and obtains assurances regarding the effectiveness of its controls;
- the roles and responsibilities of decision-making bodies (including committees, working groups and forums) and other key individuals responsible for decision-making, approval, supervision and operation of information security functions are clearly defined.

The self-assessments performed routinely by the board regarding its overall mandate should also include a review of the board's knowledge and understanding of the ICT risks to which the institution is exposed.

The board of directors should regularly ensure the assessment of the institution's compliance[9] with its ICT governance framework. It should also ensure that the compliance function reports on the significant results of monitoring of ICT and on the national and international laws, draft laws and regulations governing ICT, and it should review any emerging compliance risks in connection with its activities.

The audit committee is expected to ensure the effectiveness of ICT-related governance, risk management and internal control processes.

[9] References to the compliance function can also include any other independent oversight function in the second line of defense.

Many ICT management tasks require positions and decisions to be taken by business sectors. Various aspects of ICT governance can be undertaken by management if it is assigned to the right responsibilities and authority by the board of directors.

Senior management

Members of senior management are responsible for achieving the institution's organizational strategic objectives. They are responsible for assessing ICT risks and implementing the appropriate internal control system. Senior management generally carry out all functions related to ICT management and to the operation of the institution in a manner consistent with its ICT strategy, risk appetite and tolerance, and board-approved policies.

In addition to the roles and responsibilities that normally devolve to it, senior management should, in particular:

- provide a holistic view of the ICT and business environment, as well a vision for the future and the initiatives needed to move in that direction (section 1.6);
- ensure that the institution has access to current, relevant and reliable knowledge to support its processes and facilitate decisions on ICT matters, and that such knowledge is identified, gathered, organized, maintained, used and evaluated to ensure it is up to date;
- gather and evaluate ICT and business indicators and objectives, ensure that processes are in line with the defined objectives and indicators and see to it that reports are produced systematically and on time;
- in cooperation with the compliance and internal audit[10] functions, monitor and evaluate the control environment on an ongoing basis through, for example, self-evaluations, assurance reviews, identification of control deficiencies, and measures to ensure compliance of ICT-backed processes with, among others, laws, regulations and contractual obligations;
- create an environment conducive to maintaining ICT awareness, identifying existing and emerging ICT opportunities and influencing strategic planning and enterprise architecture decisions;
- manage the relationship between IT services and business units in a formal and transparent manner, relying on common language to jointly meet strategic objectives;
- establish a vision of enterprise architecture that includes the processes, information, data, and tiers of architecture in applications and technologies;
- carry out ICT and business strategies by creating models and practices that outline current and target architectures.

[10] References to the internal audit function may also include any other independent assessment function in the third line of defense.

As part of ICT integrated risk management, senior management should, in particular:

- align its ICT risk management against the institution's objectives regarding the creation and preservation of value as well as the business processes or specific sectors in which such risks are most likely to materialize;
- assess and take into consideration the potential effects of the ICT risks identified on the financial institution's strategies and compliance as well as on the integrity of financial reporting.

The chief risk officer[11] is responsible for developing, implementing and coordinating the ICT risk management strategy. He must therefore be able to synthesize, put in plain language and communicate ICT-related information effectively.

1.3 Roles of lines of defense

Operational managers constitute the first line of defense responsible for day-to-day risk management. They must identify and report unusual risk exposures taking into account the financial institution's ICT risk appetite, risk tolerance levels and related policies, limits and controls.

ICT risk management function

The institution's risk management function should be responsible for the operational and strategic facets of risks associated with ICT and ICT-related innovations.

This function should monitor material risks and emerging risks in a rigorous and integrated manner and on an ongoing basis.

The precepts of ICT risk management are discussed in section 2.

Compliance function

The compliance function should establish compliance management policies and procedures to comply with legal, regulatory and normative requirements pertaining to the use, ownership, operation and adoption of ICT in all of the institution's activities and to ensure that they are regularly updated. The AMF considers that the framework and its principles should tie into the overall risk management framework.

Internal audit

The internal audit function should be able to provide objective assurance on the effectiveness of their ICT governance, ICT risk and compliance management processes and internal controls and their adequacy in view of the financial institutions' activities.

---

[11] If this function does not exist, responsibility should fall to a person with sufficient authorization to ensure his independence and who has the necessary powers and resources, commensurate with the institution's nature, size and complexity, to adequately accomplish his mandate, i.e., a member of senior management.

Pursuant to a risk-based approach, this standards-based assurance should cover principally the following: efficiency and effectiveness of ICT operations; safeguarding of informational assets; reliability and integrity of reporting processes; and compliance with laws, regulations, standards, procedures and contracts for the financial institution as a whole.

The institution's audit activities should include a review of the design and effectiveness of information security controls, including those carried out by external parties. Internal audit should also assess the assurance of information security controls when it is produced by an external party and has the potential of adversely affecting the institution, its clients or other stakeholders.

1.4 ICT governance structures

The AMF expects financial institutions to regularly evaluate their support structures, roles and functions, with a view to continuously developing and improving their ICT governance.

To this end, the financial institution should ensure that:

- ICT governance stakeholders and their roles and responsibilities (section 1.2) are reviewed and clearly identified;
- the authority, rights and boundaries of decision-making have been established and aligned among the various structures and chosen roles, and that escalation procedures have been put in place in the event that any decision-making problems arise;
- a board-level structure[12] is in place to focus adequately on all the institution's ICT-related issues;
- a member of senior management, such as chief technology officer, chief information officer or other officer, is assigned to present technology proposals to the board and report on the implementation of ICT-related strategies and frameworks;
- a member of senior management, such as a chief information security officer or other officer, oversees the deployment of the framework ensuring information security and physical security of the institution's technology infrastructures;
- a member of senior management, such as a chief data officer or other officer, oversees the framework approved by the board of directors for the collection, storage and use of data throughout the institution;
- an executive committee manages operational risks related to the implementation of the ICT strategies and frameworks approved by the board of directors;

[12] Without an equivalent function, the institution is exposed to significant strategic technological risks.

- certain members of management are assigned ownership of various ICT risks within the institution.

The financial institution should also ensure that:

- a committee, such as a risk management committee or executive technology committee,[13] comprised of senior executives, manages and oversees ICT strategic risks throughout the institution;
- a member of senior management is assigned to implement the ICT cost and benefit management framework;
- individuals from the institution's various sectors are assigned to identify, evaluate and report on ICT risks;
- managers are assigned to execute the change programs specified in the strategic plans;
- a bridge is built between the board of directors and senior management so as to establish a vision of enterprise architecture that includes the processes, information, data, and tiers of architecture in applications and technologies;
- an individual oversees development of the institution's technology architecture and its integration within the enterprise architecture.

The engineering and architecture roles, in developing information security adequate for the institution's ICT systems, should be supported by proper segregation of operational security and risk management.

Other roles throughout the institution can have an effect on ICT risk management and governance. They are not directly involved in ICT risks, but are stakeholders in this process. Examples include ICT and business process owners, the person in charge of business continuity and the person in charge of human resources or procurement.

The board of directors and senior management are best positioned to ensure that the lines of defense pertaining to ICT are properly represented in the risk management system and control processes. They are jointly responsible and accountable for establishing the institution's business objectives (including resulting ICT-related objectives). They are also responsible for defining strategies, establishing the structures required for the best ICT risk management and communicating the tone set by the institution's executive level, in particular, by advocating transparency and collaboration between stakeholders involved in ICT governance.

[13] This committee is sometimes referred to as the IT Steering Committee.

1.5 Precepts and properties of the ICT governance framework

Precepts

The AMF expects financial institutions to identify the core precepts of sound ICT governance applicable to its environment and the actions required for developing and deploying all such precepts.

Sound ICT governance lies in defining and using core precepts that can help the board of directors understand, fulfil and communicate legal, regulatory and ethical obligations with respect to the use of ICT within the financial institution.

These core precepts of sound ICT management express the desired behaviours to guide decision-making. The statements of these precepts refer to what should be produced, without prescribing how or when this should occur. They should be drafted in a way that is easily assimilated by all targeted readers, including the board of directors and senior management.

The following core precepts should be considered for sound ICT governance:

- Responsibility: Individuals and groups within the institution understand and accept their responsibilities as they relate to ICT demand and use and to data use.

- Acquisition: ICT acquisition is justified and based on continuous relevant analyses as part of a clear and transparent decision-making process. Decisions are based on an appropriate balance between costs, benefits, opportunities, and short-, medium- and long-term risks.

- Performance: ICT is adapted to the institution's current and future support needs by providing the quality and level of service required.

- Compliance: ICT use is in compliance with legislation and regulations. Frameworks and practices are clearly defined, deployed and applied.

- Human behaviour: ICT frameworks, practices and decisions should demonstrate respect for human behaviours and how they change for all individuals involved in the activities.

Each financial institution is responsible for identifying the required actions for deploying these precepts, based on its nature and on analyses of ICT-related risks and opportunities. Many actions should also be considered for developing these precepts for ICT and data governance. In particular, the board of directors should:

- ensure that responsibilities cover the data life cycle;
- ensure that the qualifications of the key individuals responsible for making ICT decisions are assessed;

- assess ICT and related activities, when reviewing plans and policies, to ensure that they are in line with the institution's objectives, take good practices into account and meet the needs of key stakeholders;
- ensure that the institution and its suppliers develop a common understanding of the ICT acquisition process;
- evaluate the institution's plans to ensure that ICT will aptly support business processes;
- assess the extent to which ICT satisfy regulatory, legal and contractual obligations and professional and international standards.
- regularly assess the institution's compliance with its ICT governance framework, such as appropriate monitoring of frameworks governing data accuracy and ICT efficiency;
- evaluate ICT activities and ensure that human behaviours are identified and considered appropriately, that they remain relevant and that they are given due attention.

More specifically, the following core precepts also contribute to sound information security governance and should be taken into consideration:

- establish information security across all the institution's activities, including with respect to information treated by external parties within the institution's scope;
- adopt an approach based on the institution's risk appetite, including loss of competitiveness, compliance, operational interruptions, impact on reputation and financial losses;
- ensure compliance with internal and external requirements through independent security audits;
- cultivate an environment favourable to security by coordinating stakeholders' activities to obtain a cohesive direction for information security and to support delivery of security education, training and awareness programs;
- review how security is performing in terms of its impacts on the institution, not only with respect to the effectiveness of security controls.

Lastly, some additional precepts guiding the implementation of corporate architecture for ICT resource use within the institution should also be considered and defined. These precepts include agility for quick adaptation to changing needs and openness to the observance of international standards.

Properties

The institution is responsible for defining the shape of its ICT governance framework based on its nature, size, complexity and risk profile. However, some key points must be considered, including:

- the integration of current and future ICT capacity into business planning processes to ensure that ICT strategic plans are in line with business strategies;
- the implementation and recognition of mechanisms to ensure that individuals with responsibilities also have the duty to report on them.

A financial institution's governance framework should also reflect changes made over time. The quality of governance practices is important for maintaining market confidence. Thus, they should evolve in a manner which reflects new practices, including those involving technology and industry standards. The ICT governance framework should therefore take into account good practices recognized by existing professional and international[14] data governance and management frameworks as well as information security (including cyber security) governance frameworks, and should align with the institution's business goals.

The various ICT framework components should consider and align all inherent and useful provisions for technology risk management, in particular, those dealing with:

- ICT risk management;
- information security;
- crisis management;
- outsourcing;
- business continuity;
- program/project/change management;
- human resources;
- ethics;
- intellectual property;
- protection of personal information.

As well, due to the rapidly changing ICT operational and security environments, the institution should regularly review and update its framework and ensure that changes are implemented by the compliance processes, checking their application and closing any compliance gaps.

1.6 Documenting the ICT environment

The AMF expects financial institutions to continuously document their technological environment for consultation by ICT governance stakeholders.

[14] These include those established by NIST, Cobit, ITIL and ISO.

Documenting the environment would help to establish and maintain a clear understanding of the strategic importance and risks of the use of ICT and the institution's data and would contribute to decision-making.

As part of the documentation process, information could be compiled to reflect the status of the institution's ICT strategy, the current and target architecture, its strategic ICT risks and objectives, the ICT plans and the current status of its plans, its ICT risk impact statements and existing processes and structures for ICT risk management, its development methodology and its operation processes.

The AMF expects the financial institution to maintain knowledge of its systems, assets and data, their circulation in the institution and its capacities. The compiling, and especially the maintenance, of this documentation should contribute to optimal development of technology and business strategies. The inability to create a solid basis of information for strategic decision-making is in itself a strategic governance risk.

This documentation should never be static; it should change over time. Just like business, the institution's ICT are ever-changing and evolve with acquisitions, updates and external influences, such as cyber risks.

The documentation should contain sufficient aggregate information to facilitate decision-making concerning the ICT strategy.

The institution's frameworks should specify the roles and responsibilities of decision-making bodies and operating units in establishing, maintaining and consulting this documentation.

While the documentation may be prepared and maintained by experts at different levels of an institution, the key elements should be authorized by senior management and approved by the board of directors, and should constitute an authoritative source for decision-making, particularly strategic decision-making.

The strategic documents that draw on best practices could include:

- a description of the situations the institution, its business lines and its support functions faces;
- the ICT strategy components, its strategic plan and the status of that plan;
- a description of ICT risks on business strategies;
- the current and target ICT strategic architecture;
- ICT operating models and processes.

1.7 Information required for decision-making

Information is a governance tool that stakeholders use to fulfil their roles, perform their duties and interact. Different types of roles required for ICT governance consume, use, produce or protect information, both general and specific. This information can be physical, empirical, semantic, pragmatic or even social. Its use varies depending on the information

life cycle. The following are examples of information in support of sound governance and ICT risk management that the institution should factor into its practices:

- risk profile;
- risk taxonomy and register (or universe);
- risk and controls matrix (including risk scenarios and assessment);
- risk report;
- enterprise architecture defining the various viewpoints (or perspectives) so that the needs of various stakeholders can be met and documents describing its components (applications, technologies, infrastructure and so forth).

2. Identification and management of technology risks

The AMF expects financial institutions to identify, assess and mitigate ICT risks within established tolerance thresholds.

ICT risk management should form an integral part of an institution's integrated risk management.

In this regard, the institution should implement appropriate mechanisms to:

- collect relevant data for identifying, analyzing and reporting on ICT risks;
- develop useful information to support decision-making;
- maintain a register of known ICT risks and their attributes, and monitoring activities;
- produce information on current risk status for stakeholders in a timely manner;
- manage opportunities to reduce risk to an acceptable level like a portfolio;
- using efficient methods, provide a timely response to limit losses resulting from ICT-related events.

2.1 Types of technology risks

The AMF expects financial institutions to put in place a taxonomy[15] of their own to ensure that all types of ICT risks are considered, thus facilitating their aggregation and contributing to the establishment of a holistic view.

ICT risk is typically considered to be a component of operational risk. However, even strategic and reputation risks can entail an ICT component, particularly when ICT plays a part in the conduct of business. This is also the case for credit risk, where weak ICT security can lead to erroneous credit ratings.

Technology risk management should be forward-looking and take into consideration both the operational and the strategic aspects of technology risks that permeate all financial institution processes.

In particular, aside from technology-related operational risks, the following strategic risks should be considered, as they may hinder the achievement of corporate strategies by boards of directors:

- Technology positioning risk

[15] The AMF recognizes that there is no universal risk taxonomy, nor is there a definitive risk taxonomy in financial regulation other than the generic classification recommended by the Basel II Accord for deposit-taking institutions.

  - The risk that, when defining the strategy, the technology position aimed for in the industry is not adequately embedded in the business strategy, is not viable (in terms of the institution's business and technology models and strategic objectives) or is not feasible (in terms of its IT strategic implementation plan).

- Technology implementation risk

  - The risk that, when implementing its strategy and strategic plan, the board of directors fails to achieve the sought-after strategic IT objectives and related business goals.

- Technology governance risk

  - The risk that the board of directors fails to put in place the requisite elements (policies, processes and the like) to govern the development and implementation of its IT strategy.

The institution's taxonomy should be tailored to its situation in order to facilitate aggregation and contribute to creating a complete picture. This taxonomy should therefore be exhaustive in its coverage of ICT risks so that those responsible for identifying risks can consider all the types of risks likely to impact the institution's objectives.

To be more agile and increase its capacity to adapt to change over time, the institution should consider technology risk in a holistic manner by looking at not only common risks, but also the risk of not responding appropriately to technological changes or the introduction of new or emerging technology.

In developing its risk taxonomy, the institution should try to establish a reasonable number of categories that aggregate risks properly without diluting the particular nature of each category. Where an institution already has a risk taxonomy in a given functional sector (in internal audit, for example), it would be worth considering it in the development of an organizational risk taxonomy, because it may contain categories with proven institution-wide application. Once developed, this taxonomy should be communicated to the entire institution in order to ensure consistent use in identifying and aggregating ICT risks.

2.2 ICT risk tolerance

The AMF expects financial institutions to establish and maintain an overall statement qualitatively and quantitatively describing its ICT risk tolerance level. It also expects institutions to clearly define their tolerance levels for key material risks and embed them in their operations in keeping with their risk management policies and procedures.

Risk appetite is closely tied to the institution's business strategy. The risk appetite statement should contain qualitative information that makes it possible to situate the targeted ICT risks as well as the desired behaviour of the institution based on different scenarios. The statement should also contain a few quantitative objectives or limits, expressed on the basis of revenue, capital or any other metric deemed relevant.

As mentioned above, the board of directors and senior management are best positioned to disseminate the tone established at the top. They should regularly communicate the established ICT risk tolerance level so as to facilitate its integration into operations and encourage technological innovation.

The AMF expects the institution to assess the adequacy of resources in light of its risk appetite by means of stress tests for all material and probable risks, categorized by likelihood and impact (e.g., ICT risks, including cyber risks).

2.3 Attributes of the technology risk management framework

The AMF expects financial institutions to carry out ICT integrated risk management that is supported by a solid governance structure, strategies, policies and procedures that enable them to identify, assess, quantify, control, mitigate and carefully monitor material risks.

The AMF further believes that financial institutions should gravitate toward integrated ICT risk management rather than take an approach where risks are considered separately. Thus, risks considered less important but which could become significant when combined should also be considered. A holistic approach that captures the interrelationship and interdependence between risks would highlight the key aspects likely to influence the level of risk the institution will assume. For example, certain risks related to inadequate segregation of logical access to computer systems, and which result from information security governance deficiencies, appear more clearly when consolidated on an institution-wide level.

This approach also makes it possible to better take into account risks that are harder to quantify using traditional methods. Certain operational risks, strategic risks and reputation risks are good examples.

Moreover, an integrated risk management framework increases the effectiveness with which the cascading effects of risks with multiple consequences are handled. Risks associated with the use of technologies, given their multiple ramifications, are good examples: interrupted operations, loss of data, identity theft, cyber attacks, damage to

reputation, lawsuits, etc. With this in mind, strategies, resources, technologies and knowledge must be aligned to manage these risks adequately and comprehensively across the entire financial institution.

The institution should understand the impact of technology risk on operations, including its mission, functions or reputation, as well as on assets and individuals. Consequently, the institution should have an integrated approach to identify, assess, control and manage technology risk. This approach should be applied institution-wide and should enable the institution to:

- ensure proper and timely monitoring of risk mitigation activities shown in the ICT risk register. This register, updated prospectively, on a regular basis, could, for example, contain a list of known and potential ICT risk attributes likely to affect the institution and provide timely information that is useful for reducing risks for all stakeholders;
- align all the risk assessment tools used so as not to impede a holistic view of ICT risks across the institution;
- use an exhaustive information asset[16] management process to associate risks in a holistic manner;
- use a framework for the classification[17] of data and information assets, including those managed externally, and established and deployed procedures to provide a holistic view of key systems;
- use incident management processes with appropriate resumption and recovery objectives that allow for proactivity in risk management.

The institution should assess ICT risks at planned intervals or when significant changes are expected or are taking place, bearing in mind the established criteria. ICT risk assessment should be part of an ongoing, systematic and cyclical process.[18]

The institution should demonstrate that it has assessed the risks associated with the ongoing maintenance of its legacy systems and that adequate controls are deployed to effectively manage the risks of these technologies. If these legacy systems support critical operations, the institution should have a strategy in place for managing ageing infrastructure that comprises an evaluation of additional investments or the transition to new-generation technology over time.

All of the institution's ICT model hardware and software components have a useful life cycle, and the board of directors should be aware of the risks of failing to update these systems within a reasonable time frame.

---

16 The institution's asset vulnerabilities should be identified and documented. The same applies to internal and external threats as well as likelihood and potential business impacts in order to determine the risk level and establish appropriate action plans. Also, these activities should be conducted in ways that make use of all available information, particularly existing intelligence on cyber threats.

17 This classification should reflect the extent to which an information security incident affecting an information asset could adversely affecting its clients or other stakeholders.

18 Organisation for Economic Cooperation and Development. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, 2015.

The institution should also notify the AMF when it becomes aware that an ICT-related incident could have a significant and harmful impact on its ability to provide its clients with adequate services, its reputation or its financial position.

In addition to assessing the technology risk inherent to its activities, products and services (including, in particular, cyber risk assessment), the institution should consider the impact that this risk will have on its partners, suppliers, clients or even other financial sector participants.

The financial institution's management practices should include the submission of institutional controls to periodic independent review and, depending on its nature, size and complexity, the performance of penetration testing.[19] The effectiveness of controls for information security should be tested through a systematic program proportional to the pace of change in threats and vulnerabilities, to the criticality and sensitivity of the information assets, to the impact of an information security incident and to the materiality and frequency of changes to the institution's information assets.

Details of key findings from reviews should be reported to the board of directors. Any shortcomings identified should be corrected within a reasonable amount of time.

In assessing information security risks, the institution should, in particular:

- identify information security risks related to the loss of confidentiality, integrity and availability of information, and name the risk owners;

- establish and update information security risk criteria, including risk acceptance criteria and criteria for assessing information security risks.

In addition, in treating information security risks, the institution should, in particular:

- determine all measures necessary for the implementation of the information security risk treatment options chosen;
- compare the measures determined against existing best practices and verify that no required measure was omitted;
- produce a Statement of Applicability containing the necessary measures and a rationale for their inclusion, a mention as to whether or not they are to be implemented, and a rationale for excluding measures.

The financial institution should actively maintain the security of its information based on changes in threats and vulnerabilities, including those resulting from changes in its

[19] Penetration testing and vulnerability assessments only produce an image of a computer system in one state and at one particular time. This image is limited to the portions of the system that are tested during the penetration testing. Penetration testing and vulnerability assessments are not substitutes for an ICT risk assessment.

information assets, the stage at which they are in their life cycle[20] and its business environment.

The institution should keep documented information on information security risk assessment and treatment processes.

In risk and control assessment, protection mechanisms may include risk avoidance or elimination whereby the institution does not engage in an identified activity. They may also include risk mitigation through controls or risk sharing or transfer. In particular, the institution could consider taking out insurance for various risks, including recovery and resumption costs.

The institution should also evaluate the ICT risk management framework on an ongoing basis against clear evaluation objectives, established expectations and methodologies disseminated to stakeholders, and reports comprising clear conclusions and concrete corrective action. This also involves documenting, in an aggregated and synthesized manner, findings and decisions (sections 1.6 and 1.7) stemming from the application of the ICT risk management framework and stress testing exercises (e.g., adjustments made to the ICT risk appetite statement and strategic plan). The AMF may, if it deems it appropriate, provide more specific expectations concerning the documentation required to support the ICT risk management framework.

2.4 Technology risk aggregation

ICT risk management can only achieve its full potential when risk is managed across the institution. An aggregate view of ICT risks, beyond technical issues, is crucial for preventing a false sense of security or urgency and for accurately defining ICT risk tolerance.

To contribute to a sound ICT risk aggregation, the institution should:

- ensure that clear and consistent ICT terminology is used throughout the institution;
- use qualitative and quantitative data as well as compatible scales to assess risk frequency and impact;
- determine dependencies among identified, compiled and reported risks in order to prevent more significant risks;
- ensure the use of harmonized, consistent and agreed approaches that have been communicated to all stakeholders in order to assess the frequency and impact of ICT risk scenarios;
- use a consistent taxonomy to describe risks (section 2.1).

[20] This refers to the process of planning and designing information assets until their decommissioning and disposal.

ICT risks can be aggregated according to multiple dimensions (organizational units, types of ICT risks, processes, etc.). They should be aggregated at the institutional level to be considered in combination with all the other risks that must be managed.

2.5 Business impact of technology risks

The AMF expects financial institutions to use methods through which they can establish a link between ICT risk scenarios and their potential impacts on business so that all stakeholders understand the effects of adverse events associated with ICT.

The AMF does not prescribe any methods for putting ICT risks in appropriate business terms. The institution should choose the methods based on appropriate notions of finance, confidentiality, integrity, clientele, competitive edge and reputation.

ICT risk assessments require the results generated to be expressed in clear, unambiguous business terms. Effective ICT risk management also requires a mutual understanding between the business and technology sectors of the risks that should be managed, and the underlying reasons. ICT risk management stakeholders should have the ability to understand and express the manner in which unfavourable events or incidents could affect the institution’s business goals.

3. Technology risk management practices

The AMF expects financial institutions to factor in all demonstrated ICT risk management practices when establishing ICT governance and risk management.

All practices covered in this section draw on best practices. They contribute to establishing a holistic approach to ICT governance and to developing an organizational understanding of systems, information assets, data and the required capacities for ICT risk management. They could also facilitate the institution's ICT risk management efforts with respect to protection, detection, response and recovery.

Institutions implementing robust risk management practices at every level should also take external stakeholder participation into account to ensure that accurate, relevant risk management information is being distributed and used, before any security incidents occur.

3.1 Identification practices

The AMF expects financial institutions to implement mechanisms that provide them with a better understanding of their business context, the resources that support critical functions and ICT risks, so they can identify and prioritize efforts based on business needs and risk management strategies.

These mechanisms include asset management, the business environment, ICT governance, ICT risk assessment and the ICT risk management strategy.

The institution should ensure that data, staff, ICT systems (including hardware and software) and the premises that contribute to achieving business objectives are identified and managed in keeping with their relative importance to the institution's business objectives and risk strategies.

Roles, responsibilities and ICT risk management by all stakeholders should take into account the institution's mission, objectives, priorities and activities (including their interdependencies, critical functions and resilience needs for purposes of delivering critical services).

The governance established for managing all risks (strategic, legal, regulatory, operational, etc.), the impact of ICT risk on the institution's operations, image or reputation and the strategy (priorities, constraints, tolerance levels and assumptions) should be understood and factored into the institution's ICT risk management.

3.2 Protection practices

The AMF expects financial institutions to implement protection mechanisms to ensure delivery of critical services.

These mechanisms include identity and access management, training and awareness-raising, data security, information protection processes and procedures and protection technologies.

The institution should ensure that physical and logical access to information assets and associated facilities is limited to authorized users, processes, devices, activities and transactions. The institution should also ensure that:

- the organization's personnel and partners are provided information security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with established frameworks;
- information and records (data) are managed in keeping with the organization's risk strategy to protect the confidentiality, integrity, and availability of information;
- security frameworks (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), and the processes and procedures arising therefrom, are maintained and used to manage protection of information systems and assets;
- maintenance and repairs of ICT system components are performed in keeping with established frameworks and procedures;
- technical security solutions are managed to ensure the security and resilience of systems and assets, in keeping with related frameworks, procedures and agreements.

3.3 Detection practices

The AMF expects financial institutions to implement activities to identify potential ICT risk events.

These activities facilitate timely discovery of any potentially adverse events. They include detection of anomalies and events, continuous security monitoring and testing of the detection processes.

The institution should ensure, in particular, that:

- anomalous activity is detected in a timely manner and the potential impact of events is understood;
- ICT systems and information assets are monitored at regular intervals to identify cyber security events and verify the effectiveness of protective measures;

- detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

3.4 Incident response and recovery practices

The AMF expects financial institutions to implement appropriate activities to respond to detected cyber security incidents, maintain plans ensuring resilience and restore the services affected by a cyber security incident.

These activities support the institution's capacity to contain the impacts of a potential security incident and accelerate the return to normal operations. They include plans for response and recovery, communications, analysis, mitigation and continuous improvement.

The institution should ensure, in particular, that:

- response and recovery processes and procedures are executed and maintained, to ensure a response to detected cyber security incidents and the restoration of systems or assets;
- response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies);
- restoration activities are coordinated with internal and external parties (e.g., coordinating centres, Internet Service Providers, victims and vendors);
- an analysis is conducted to ensure adequate response and support recovery activities;
- activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident;
- organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities;
- recovery planning and processes are improved by incorporating lessons learned into future activities.

3.5 Other practices

Technology-related operations

Technological innovations, such as cloud computing, the Internet of things and megadata, have a significant impact on the ICT operations function, particularly in terms of processes that must be adapted, like capacity management and security management, and in terms of knowledge that should be enhanced to fit new ICT systems.

In this context, it is important for the board of directors to recognize the key role that ICT operations play in the success of the ICT strategic plan, and for ICT operations staff to

have the information and tools they need to detect any problems that may arise in the operations of processing centres, networks, IT security infrastructures and user support.

These tools and information should contribute to:

- risk identification (inventory of information processing equipment, resources, locations, etc.);
- risk assessment (prioritization of ICT risk mitigation activities);
- the deployment of mitigation controls (policies, guidance, standards, procedures, controls, physical and logical security, management of data, personnel and change, information distribution and transmission, backups, user support, etc.);
- risk monitoring and reporting (performance monitoring, capacity planning, self-evaluation of controls).

Although harnessing technological innovations and the complexities they entail may be facilitated by using several sources of information, the board of directors should be aware that such innovations must be carefully managed to avoid creating unnecessary risk that could affect implementation of the strategic plan.

Therefore, in collaboration with senior management, the board should ensure that processes are deployed to assess and manage all operational risks associated with the use, ownership, operation and adoption of ICT within the institution. It should, in particular:

- implement an appropriate ICT operational structure to support the institution's business activities;
- document existing systems and understand how they support related business processes;
- establish and support an appropriate control environment through the identification, assessment, management and monitoring of ICT-related operational risks based on precepts similar to those set out in the *Operational Risk Management Guideline*;
- create a secure physical and logical operational environment;
- provide for operational continuity and resilience;
- provide for appropriate selection, staffing, replacement and training of ICT personnel.

Business continuity

Continuity management[21] is its own discipline and extends beyond the scope of this guideline. There are many standards in this area, which defines continuity as the strategic and tactical ability of organizations to prepare for and respond to incidents and business

[21] The *Business Continuity Management Guideline* sets out other management principles recommended by the AMF.

interruptions so that operations can continue at an acceptable pre-defined level. However, it is important to bear in mind the following:

- Strategic governance and operations risks related to ICT can arise when a financial institution does not have adequate structures and policies in place to protect it from the consequences of a disaster.
- Changing[22] an institution's ICT, in connection with new business strategies, requires an evaluation of the impact this has on business continuity planning.
- While business and ICT strategies are in progress, operational environments will be in a state of continuous change and new and different continuity needs will emerge. This could expose the financial institution to significant risk in terms of strategic implementation, particularly when the strategy spans a number of years.
- Although business continuity can be outsourced when the ICT strategy involves cloud computing, the institution remains responsible for recovery when a disaster affects its suppliers.
- ICT continuity and resilience should be sufficiently robust and proven in order to ensure timely recovery from operational disruptions.

Outsourcing and cloud computing

The increasing adoption by financial institutions of cloud computing services[23] provides numerous advantages (economies of scale, access to sound practices, agility, etc.). The distributed nature of these services can also enhance resilience in the event of disasters or service interruptions.

The AMF considers these cloud computing services to be a form of outsourcing. Institutions should therefore refer to the AMF's expectations in the *Outsourcing Risk Management Guideline.*

The institution should fully understand the typical characteristics of cloud computing services, including colocation, data amalgamation and a strong propensity for computer processing in multiple or distributed sites. The institution should consider actions to identify and manage risks associated with data access, confidentiality, integrity, sovereignty, regulatory compliance and audit. In particular, the institution should satisfy itself that the service provider has the ability to identify and segregate client data through robust physical and logical controls.

In the specific context of outsourcing and cloud computing, the financial institution should:

---

22 For example, technological innovations (cloud computing, the Internet of things, megadata, etc.) and their significant impact on the ICT operations function (section 3.5 "Other practices").

23 Cloud computing services are a combination of business and delivery models, available in public, private or hybrid operating mode, that allow on-demand access to a shared group of resources (applications, servers, storage, networks, security, etc.). They are generally delivered as Software as a Service ("Saas"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

- secure in a contract its right to audit (and that of the appropriate authorities, if applicable) and its right to access the premises of the cloud computing supplier;
- ensure the security of the data and the location of computer processing through appropriate controls (established through a risk-based approach), such as encryption technologies for data in transit, data in memory and data at rest;
- mitigate supply chain outsourcing risks when suppliers outsource certain activities to other suppliers;
- develop solid contingency plans and exit strategies enabling the institution to quickly pull out of any contractual agreement without service delivery interruption, adverse effects on regulatory compliance or impact on the continuity and quality of ICT services provided to customers.

As part of its due diligence, the institution could also consider whether the supplier adheres to relevant international standards for the delivery of ICT services. Assurances resulting from these international standards will probably be insufficient, but will contribute to decreasing risks and should be considered.

In addition to the AMF's expectations pertaining to outsourcing risk management,[24] the financial institution should consider ICT risk, particularly cyber risk, when assessing the level of experience and expertise required for the outsourced activity and for management of the outsourcing relationship. The financial institution should also keep, in its centralized list of material outsourcing arrangements, all useful data risk management information (nature, sensitivity, location(s) of data processing, of storage and of traffic, etc.).

Given the number of suppliers and the variety of potential impacts that outsourcing and cloud computing can have on financial institutions, strict controls should be put into place. The institution therefore should identify the ICT-related strategic risks involved in outsourcing initiatives, implement an effective risk program for managing such risks, and monitor the risks stemming from any outsourcing arrangement.

Transformation projects and programs

When identifying the risks involved in transformation projects, the institution should consider, in particular, disruption of client services, loss of competitive advantages, the negative impact on its reputation and delays in implementing critical and strategic products or processes.

Such risks can arise from a combination of technical, business and project management decisions. This could, for example, include the institution's inability to recognize changes in the business and technology landscapes that are likely to influence its strategies, inability to integrate sectors and business and ICT plans, and failure to involve business users, suppliers and technologies to understand needs and allow for delivery of ICT strategic plans.

[24] AUTORITÉ DES MARCHÉS FINANCIERS. *Outsourcing Risk Management Guideline*, December 2010.

Although the orientations of the *Integrated Risk Management Guideline* apply to all types of risk, operational risk inherent in ICT solicits the commitment of those in charge of the financial institution's activities, processes and systems. The effectiveness of such management should be validated and verified regularly, based in particular on a variation attributable to factors such as the changes resulting from organizational transformations affecting systems. Such changes could require a review of ICT-related operational risk tolerance levels.[25]

In this situation, the financial institution should:

- involve senior management to ensure consistency with the strategy and receive financial support as well as assistance in conflict resolution;
- ensure that the vision, objectives and information systems are properly understood and cohesive and that the transformation project is consistent with its strategy;
- understand project portfolio management, project management and its own practices, terminology and standards as well as the methodology that it has adopted;
- standardize and support its project management methodology;
- define the development life cycle, which includes various steps to be completed in sequence so that business needs can give rise to systems or applications and their maintenance can be handled;
- manage changes to structures and processes, including informal and intangible aspects (e.g., perceptions of impact and changes to work habits), communication, organizational readiness (e.g., resistance to change), training and post-launch support.

[25] Autorité des marchés financiers. *Operational Risk Management Guideline*, December 2016.

4. Supervision of sound and prudent practices

In seeking to promote sound and prudent management practices within financial institutions, the AMF, acting within the scope of its supervisory activities, intends to assess the degree of compliance with the principles set forth in this guideline in light of the specific attributes of each institution. Consequently, it will examine the effectiveness and relevance of the strategies, policies and procedures adopted by financial institutions as well as the quality of oversight and control exercised by their board of directors and senior management.

Given that IT and communications risk management practices are constantly evolving, the AMF expects decision makers at financial institutions to remain current with best practices and to adopt them, to the extent that they address their needs.