DRAFT

AUTORITÉ DES MARCHÉS FINANCIERS

GUIDELINE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY RISK MANAGEMENT

January 2020

TABLE OF CONTENTS

Preamble

This guideline is an indication of what the *Autorité des marchés financiers* (the "AMF") expects of financial institutions in terms of their legal obligation to follow sound and prudent management practices. As such, it covers the interpretation, performance and application of this obligation.

In light of this, the AMF prefers a principles-based approach to a rules-based one. Its guidelines are therefore designed to be sufficiently flexible to enable financial institutions to establish their own strategies, policies and procedures for the implementation of sound management principles and to put in place sound practices commensurate with their nature, scale, complexity and risk profile. In this regard, the guideline demonstrates ways to meet the principles it contains.

AMF Note

The AMF believes that sound and prudent management and sound commercial practices of financial institutions, and thus the AMF's prudential framework, should rest on three pillars: governance, integrated risk management and compliance (GRC).

This guideline reflects this perspective and sets out the AMF's expectations for sound and prudent information and communications technology ("ICT") risk management practices.

Scope

This guideline is intended for authorized insurers, federations of mutual companies, financial services cooperatives and legal persons belonging to a cooperative group, authorized trust companies, savings companies and other deposit institutions governed by the following statutes:

- *Insurers Act*, CQLR, c. A-32.1;[1]
- *Act respecting financial services cooperatives*, CQLR, c. 67.3;[2]
- *Trust Companies and Savings Companies Act*, CQLR, c. S-29.02;[3]
- *Deposit Institutions and Deposit Protection Act*, CQLR, c. I-13.2.2.[4]

Solely for the purposes of this guideline, the generic terms “institution” and “financial institution” are used without distinction in referring to the entities covered by the guideline.

Lastly, this guideline applies to financial institutions operating independently as well as to financial institutions operating as members of a financial group.

The standards or policies adopted by a federation with respect to financial services cooperatives and mutual insurance associations that are members of the federation should be consistent, if not convergent, with the principles of sound and prudent management set down in legislation and clarified in this guideline.

1 Sections 463 and 464.

2 Sections 565.1 and 566.

3 Sections 254 and 255.

4 Sections 42.2 and 42.3.

Effective date and updating

The effective date of this *Guideline on Information and Communications Technology Risk Management* is January 23, 2020.

With respect to legal obligation imposed on the institutions to follow sound and prudent management practices, the AMF expects each institution to adopt the principles of this guideline by developing strategies, policies and procedures commensurate with its nature, scale, complexity and risk profile.

The AMF expects financial institutions to adopt and implement the expectations in this guideline by January 23, 2021.

This guideline will be updated to take into account developments in ICT risk management and reflect observations made by the AMF in the course of its supervisory activities in relation to the financial institutions concerned.

Introduction

While the rapid pace of technological innovations has helped to transform financial institution processes and business models, such innovations are introducing significant risks at a time when institutions are becoming more and more interconnected or dependent on legacy systems[5] and external suppliers to carry out their activities.

The adoption of technological innovations is also increasing the risk of data being lost, leaked, stolen, corrupted, or accessed without authorization. Institutions are exposed to an ever-greater risk of increasingly sophisticated, frequent and difficult-to-detect cyber attacks.

Information and communications technology (ICT) risks[6] can have adverse consequences, both financial and legal, for an institution's clients and reputation.

This guideline describes the AMF's expectations with respect to ICT risk. The ultimate goal of these expectations is to strengthen the financial sector's resilience in response to this risk. In particular, these expectations are intended to ensure the development of appropriate security hygiene through the implementation of measures[7] that will help prevent a major incident and limit its impact.

Each institution is responsible for clearly understanding all its ICT risks and ensuring that they are appropriately considered in light of the institution's nature, size, complexity and risk profile. The institution is also responsible for staying current on ICT risk management best practices and adopting them to the extent that they meet its needs.

5 A legacy system is a piece of hardware and/or software that continues to be used in an organization despite being superseded by more modern systems. It forms part of an organized assembly of resources enabling the collection, storage, processing and distribution of information.

6 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 cybersecurity), change, data integrity and outsourcing risk.

7 Such measures include both basic ICT governance practices and operational measures such as the timely deployment of software security updates, the detection of unauthorized traffic on network infrastructures, the management of information access rights, the strengthening of authentication mechanisms for access to critical systems and the monitoring of malware.

1. Types of ICT risks

The AMF expects financial institutions to put in place a taxonomy that catalogues all types of ICT risks.

The taxonomy should be forward-looking and capture the technology risks that are ever-present in all financial institution processes. The taxonomy should be developed in order to facilitate the aggregation and obtain a comprehensive picture of its ICT risks. It should therefore provide a comprehensive set of ICT risks so that those involved in risk identification may consider all types of risks that could affect the institution's objectives.

Technology risk should be assessed holistically, taking into consideration both common risks and the risks of not responding appropriately to technological changes or the arrival of new or emerging technologies in order to enhance the institution's agility and ability to respond to changes over time.

In addition to operational risks derived from technology-related risks, the following strategic risks[8] can impede the achievement of the institution's objectives and should be considered:

- Technology governance risk.[9]
- Technology positioning risk;[10]
- Technology implementation risk.[11]

To guard against a false sense of security or urgency and optimally define ICT risk tolerance, the institution should, among other things:

- use clear ICT terminology and a consistent taxonomy to describe risks;
- aggregate ICT risks[12] at the level of the institution so that they are considered in combination with all the other risks that must be managed.

8 These three groups of strategic risks can be described using other wording, according to the taxonomy established by the financial institution.

9 The risk that the board of directors fails to put in place the requisite elements to govern the development and implementation of its IT strategy.

10 The risk that, at the time the strategy is defined, the technology position aimed for in the industry is not adequately embedded in the business strategy, not viable or not feasible.

11 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.

12 ICT risks can be aggregated according to multiple dimensions (organizational units, types of ICT risks, processes, etc.).

In developing its risk taxonomy, the financial institution should aim for a reasonable number of categories so that risks may be properly aggregated without the discrete nature of the categories becoming eroded.

Some of the ICT risk categories that should be considered when developing the taxonomy are information security, crisis management, outsourcing, cloud computing, business continuity, program and project management,[13] change management, ICT operations, ethics, human resources and intellectual property.

If a financial institution has an existing risk taxonomy that is used within a particular functional area, such as internal audit, it could be considered in the development of an organization-wide risk taxonomy, as it may include categories that have been proven to be applicable to the organization. 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.

[13] For example, risks may result from the interdependence between various projects or from the dependence of several projects on the same resources and expertise.

2. ICT governance

The AMF expects financial institutions to implement ICT governance developed using accepted sources, recommendations and standards.[14]

ICT governance should reflect changes made over time. The quality of governance practices is an important factor in maintaining market confidence. ICT governance should therefore continuously take into account good practices recognized by existing professional and international bodies and should align with the institution's business goals.

The following, in particular, should be considered in establishing ICT governance:

- understanding and acceptance by individuals and groups within the institution of responsibilities related to ICT and data use;
- assessment of ICT and ICT activities, when plans and policies are reviewed, to ensure that they align with the institution's goals, reflect good practices and meet stakeholders' needs;
- evaluation of the institution's plans to ensure that ICT will support business processes with the required capacity;
- consideration of the data life cycle in defining responsibilities;
- the extent to which ICT satisfies regulatory, legal and contractual obligations and professional and international standards;
- the way individuals behave towards others (for all stakeholders) in ICT-related practices and decisions.

The various elements of the framework established by the financial institution (strategies, policies, etc.) should consider and align already existing provisions[15] that are inherent in and relevant to the management of technology risks.

14 E.g., OECD, G7, NIST, ISACA-Cubit and ISO.

15 These provisions may have been defined or documented separately over the years and could contain contradictions.

2.1 Roles and responsibilities

Board of directors

In accordance with certain expectations[16] already issued by the AMF, the board should ensure, in particular, that:

- senior management promotes a corporate culture based on ethical and secure organizational behaviour in the use of technology;
- ICT-related information is exchanged with internal and external stakeholders in order to document its understanding of needs and make judgments about the current and future design of ICT governance;
- the roles and responsibilities of the ICT function and the information security and business continuity management functions are clearly defined in establishing and maintaining ICT governance;
- support structures, roles and functions are regularly assessed to enable the development and continuous improvement of ICT governance.

In addition, the board of directors should ensure that the managers responsible for developing the ICT risk framework are competent and that the following individuals are assigned:

- an individual responsible[17] for the computer systems and information technology supporting the business's objectives;[18]
- a member of senior management, such as a chief information security officer (CISO) or another person in second line of defence, to oversee the deployment of the framework ensuring information security and the physical security of the institution's technology infrastructures;
- a member of senior management, such as a chief data officer (CDO) or another person in the second line of defence,[19] to oversee the approved framework for the collection, storage and use of data across the institution;
- members of senior management to be responsible for all of the various information assets and ICT risks present in the institution.

---

16 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

17 Such as a chief technology officer (CTO) or chief information officer (CIO).

18 This person is responsible for, among other things, execution of the ICT strategic plans, application of technology-related processes (operations, architecture, risk management, etc.) and development of the institution's technology infrastructures and also presents technology proposals and status reports on the implementation of ICT-related strategies and frameworks to the board.

19 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

The board of directors should obtain updates on the scenarios considered in developing and testing disaster recovery and business continuity plans so that it understands the objectives in maintaining the availability of critical ICT operations and systems. In addition, it should have a thorough understanding of the escalation procedures and processes for security breaches or incidents, including when it should be notified.

Senior management

In addition to the roles and responsibilities that normally devolve to it,[20] senior management should, in particular:

- establish an ICT function that operates under the supervision of a second-line-of-defence control function;
- clearly delineate the responsibilities of the information security function to ensure its independence and objectivity by, in particular, segregating it from ICT operational processes and implementing compensating controls where needed. This function should not be responsible for any internal audits;
- define roles and responsibilities for maintenance and dissemination, within the institution, of the documentation and information required for informed stakeholder decision-making regarding ICT;
- manage the relationship between the services provided by the ICT function and the business units in a formal and transparent manner while using a common language to ensure the achievement of strategic objectives;
- establish and maintain an enterprise architecture consisting of the processes, information, data and layers of application, technology and security architectures;
- identify the individuals responsible or accountable for ICT risk management and those who must be consulted or informed;
- working with the compliance and internal audit functions, regularly evaluate the control environment (self-evaluations, assurance reviews, identification of control deficiencies, compliance of ICT-backed processes with laws,[21] regulations and contractual obligations, etc.);
- periodically review non-compliance (including exceptions approved by the board of directors) with the frameworks established for ICT risk.[22]

In establishing the ICT strategy, senior management should, in particular:

---

20 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*. September 2016.

21 Particularly the *Act respecting the protection of personal information in the private sector* and *the Act to establish a legal framework for information technology*.

22 Exceptions should be reviewed periodically in light of the changing nature of ICT and inherent threats to ensure that they remain at an acceptable level and will be corrected in a timely manner.

- develop a holistic view of the business environments and the ICT environments (current and future) in order to identify the required transformation initiatives;
- define and document how the ICT, technology architecture, organizational structure and key dependencies with partners and suppliers will evolve in order to support its business strategy;
- properly align ICT strategic plans and business strategies on an ongoing basis while taking into account current and future ICT capacity;
- consider using technological innovations in strategic planning and enterprise architecture decisions;
- define objectives to maintain the institution's capacity to anticipate, detect and recover from ICT incidents[23] in order to ensure ICT system resilience.

Moreover, in terms of the institution's information security, the designated member of senior management should, in particular:

- develop, document and disseminate an information security policy that defines the principles and rules for safeguarding the confidentiality, integrity and availability of the information of the institution and its clients;
- define clear information security objectives for systems, ICT services, processes and people;
- apply the information security policy to all the institution's activities and include information handled by external stakeholders within the institution's scope;[24]
- deploy controls for information assets[25] that are proportional to the criticality and sensitivity of those assets;
- do systematic testing to ensure that the controls in place are effective;
- deploy information security training and awareness programs;
- produce security performance indicators covering areas such as the business impacts (for the benefit of non-technical personnel) and effectiveness of security controls.

23 An ICT, cyber or information security incident normally occurs when an unplanned disruption in the delivery of ICT services or a security breach in a system compromises the availability, integrity or confidentiality of ICT data or systems.

24 For external stakeholders, it is acceptable here to establish appropriate agreements regarding the secure treatment of information.

25 Information assets (data, hardware and software) are not limited to those held by the institution. They also include information assets entrusted or delivered by clients or third parties.

Senior management should report on the following, in particular:

- the objectives and indicators gathered in relation to ICT and its processes on a systematic and timely basis;
- the results of monitoring done with respect to ICT-related best practices and standards in development, at the national and international levels, and the potential impacts of such best practices and standards on the institution's activities;
- key ICT issues, including significant ICT projects, priorities and incidents, as well as regular reports on ICT risk.

Other roles

The institution's risk management function[26] should oversee its ICT function and assume responsibility for management of all ICT risks (i.e., both operational and strategic risks and risks derived from ICT-related innovations[27]). This function should also rigorously monitor material and emerging ICT risks.

The objective assurance expected from the internal audit function regarding the sufficiency and efficacy of ICT governance should cover, among other things, the efficiency and effectiveness of ICT operations, the safeguarding of information assets, and the reliability and integrity of their reporting processes.

The institution's internal audit activities should include a review of the design and effectiveness of the information security controls, including the controls maintained by external parties. Internal audit should also review the assurances provided by an external party when they have the potential to adversely affect the institution, its clients or other stakeholders.

Other roles defined across the institution—such as the person in charge of business management and the person in charge of human resources—have an effect on ICT risk governance and management. Although not directly involved in ICT risk governance and management, they are nonetheless stakeholders and should be considered in defining roles and responsibilities.

[26] The chief risk officer (CRO) or a designated member of senior management must be able to synthesize, explain in plain language and communicate ICT-related information effectively to various audiences.

[27] For example, risks of bias or unethical use of big data technologies and artificial intelligence.

2.2 Integrity and competency

In accordance with the expectations[28] already issued by the AMF, effective and efficient governance, which includes information and communications technology, requires decision-making bodies to have an appropriate level of expertise, professional qualifications, knowledge or experience.

The members of the decision-making bodies and the established governance mechanisms (e.g., audit, risk management and ICT management committees) should a knowledge and understanding of ICT use, future trends and directions and have sufficient authority to fulfil their respective responsibilities.

When evaluating the competency of members of decision-making bodies, an aptitude and knowledge grid with ICT-related criteria should be developed, kept up to date and applied on a regular basis—or more frequently, if necessary—for individuals in strategic positions related to ICT governance and risk management.

The institution should therefore periodically take stock of all current ICT competencies within the institution and those needed to carry out strategies and achieve objectives.

To minimize the risk of having insufficient ICT expertise in key positions, a formal process for acquiring competencies pertaining to ICT-related strategic issues should be developed.

Similarly, a comprehensive ICT security awareness training program should be implemented for all personnel and should, at a minimum, take into account the current threat landscape (including cyber threats) and threat impacts, laws, regulations, the frameworks established by the institution and the responsibilities of personnel in safeguarding information assets.

The training program should be updated and renewed regularly for all of the institution's personnel and for any service provider with access to information assets.

Moreover, the institution should conduct regular security screening of human resources (including consultants, partners and suppliers) before they are hired, over the course of their employment and after their employment ends, where those human resources have access to ICT systems and data and may expose the institution to data theft, sabotage, fraud and other ICT risks.

2.3 ICT documentation

The institution's frameworks should clarify the roles and responsibilities of decision-making bodies and operating units in establishing, maintaining and securely consulting

[28] AUTORITÉ DES MARCHÉS FINANCIERS. *Guideline Governing Integrity and Competency Criteria*, June 2012.

documentation and information enabling stakeholders to make informed decisions about ICT.

While the documentation may be prepared and maintained by various components of the institution, the key elements should be overseen by senior management and approved by the board of directors.

This documentation should not be static but should, instead, evolve over time. As with the business, an institution's ICT constantly changes based on acquisitions, updates and external influences. The documentation should contain sufficient aggregated information to facilitate decision-making concerning the ICT strategy.

In particular, the documentation should consolidate information that reflects the status of its ICT strategy, current and target architecture, strategic ICT risks and objectives, ICT plans and current plan status, ICT risk impact statements and existing processes and structures for ICT risk management, development methodology and operation processes.

The strategic documents derived from best practices should include, in particular:

- a description of the situations faced by the institution and its business lines and support functions;
- the ICT strategy components, strategic plan and deployment status;
- a description of the impact of ICT risks on business strategies;
- the ICT risk register and ICT risk and control matrix;
- the current and target ICT strategic architecture;
- ICT operating models and processes.

3. ICT risk management

The AMF expects the financial institution to consider all activities, from recognized sources and standards, necessary to the preparation, treatment and monitoring required in managing ICT risks.

The development of strategies, policies and procedures enabling ICT risk identification, assessment, quantification, control and monitoring should take into account the preparation, treatment and monitoring activities that need to be carried out to lessen any harm that might occur in the first hours of an actual crisis. For example, all measures planned by the institution, including response and recovery measures, should be subjected to stress testing. In addition, the external stakeholders and specialists required by those measures should be prequalified and contractual terms and conditions should be pre-established.

In implementing robust ICT risk management practices across the institution, the latter should also take into account the participation of external stakeholders to ensure that accurate information relevant to risk management is distributed and used by everyone.

The ICT risk management framework should make it possible to establish and maintain a holistic view of ICT risks, including relationships and dependencies between people, end-to-end business processes, the institution's functions, ICT systems and assets supporting such processes and people. By taking stock of roles, processes and business functions, it should be possible to identify their relative importance and their interdependencies with the ICT risks.

3.1 Preparation

The selection of preparatory measures to manage ICT risks should, in particular, help to safeguard sensitive data (such as client information) against disclosure, leaks or unauthorized access. They should also contribute to ICT environment resilience. These measures should cover, among other things, access controls, authentication, data integrity and confidentiality, activity recording and security event monitoring.[29]

During preparations, the financial institution should understand the impact of technology risk on operations, including mission, functions or reputation, as well as on assets and individuals. Consequently, the integrated approach to managing ICT risk should be applied institution-wide and should enable the institution to, among other things:

[29] Sections 4.1 to 4.4 cover various additional measures to be considered and have proven useful in managing the risks related to information security, ICT operations, outsourcing and ICT transformation projects.

- align all risk assessment tools and scales used and ensure consistent, agreed-upon and transparent use;
- use a rigorous process to periodically identify information assets and their vulnerabilities in order to appropriately relate risks to assets in a holistic manner. The same applies to internal and external threats and potential likelihoods and business impacts in order to determine the level of risk and establish appropriate action plans. This asset management process should also cover data, personnel and the ICT systems (including the various hardware and software components of those systems) and the premises housing them.
- use a classification framework[30] enabling the criticality of data and information assets (including those managed by external stakeholders) to be defined, minimally, according to their availability, integrity and confidentiality requirements;
- use ICT incident management processes with appropriate resumption and recovery objectives to ensure proactive risk management;
- ensure proper and timely monitoring of activities to mitigate the risks recorded in the ICT risk register;
- monitor the effectiveness of mitigation measures, along with the number of reported incidents in order to correct them when necessary;
- consider financial, legal, regulatory, operational, client-related and reputational factors in assessing ICT risk.

In addition to assessing the ICT risk inherent in its activities, products or services (including, in particular, cyber risk), the financial institution should consider what this risk represents for its partners, suppliers and clients and also for other financial sector participants, when relevant.

The financial institution should assess ICT risks at planned intervals, when significant changes are expected or occur and when significant operational and security risks materialize, taking into account the established criteria. ICT risk assessment should be part of an ongoing systematic and cyclical process.

Furthermore, financial institutions should use methods enabling them to make the link between ICT risk scenarios and their potential impact on information assets and business processes so that all stakeholders[31] understand the effects of adverse events related to information and communications technology.

---

30 This classification should reflect the degree to which an information security incident affecting an information asset has the potential to adversely affect the institution and its clients or other stakeholders.

31 ICT risk assessments require the outcomes to be expressed in clear and unambiguous business terms. Effective ICT risk management also requires the business and technology areas to share a common understanding of the risks that should be managed and the underlying reasons for them. ICT risk management stakeholders should have the ability to understand and express how adverse events or incidents may affect the institution's business objectives.

The financial institution should:

- identify all potential individual points of failure in the ICT systems and network architectures to ensure that appropriate measures are taken to mitigate disruption risks;
- carry out end-to-end business impact analyses for critical business processes to ensure that disaster recovery and business continuity plans appropriately prioritize the institution's critical operations during ICT systems recovery;
- consider a plausible[32] set of disaster events and scenarios, including cybersecurity events, in recovery and continuity plan planning;
- include provisions for recovery within specified time frames and periodic testing in the data backup strategy to ensure procedure effectiveness.

Processes and procedures ensuring ICT system resilience should continually take into account rapidly evolving threats. Such processes and procedures should enable containment of the impacts of potential security incidents and help accelerate a return to normal operations. They include response and recovery plan planning, communications, analysis, mitigation and continuous improvement.

To avoid increased exposure to security and stability risks, the financial institution should establish plans for the timely replacement of its ICT hardware and software before the end-of-support dates indicated by their suppliers.

3.2 Treatment

In treating ICT risks, the financial institution should, in particular:

- determine all controls that are necessary to implement the treatment options for the identified risks;
- compare the controls so determined against existing best practices and verify that no required controls have been omitted;
- produce a statement containing the necessary controls and the justification for inclusions or exclusions of controls;
- maintain and use security frameworks and the processes and procedures arising from it to manage information systems and assets;

[32] The institution should consider, in particular, low-likelihood scenarios that have high financial or non-financial (reputation, compliance, etc.) impacts.

- maintain and repair ICT system components in accordance with the institution's established frameworks.

In addition, the financial institution should:

- continuously detect abnormal network infrastructure, ICT system and information asset activity in order to understand the evolution and potential impacts of undesirable events and verify the effectiveness of protection measures;
- test and maintain the aforementioned detection processes to ensure appropriate and timely knowledge of abnormal events;
- execute and maintain response and recovery processes and procedures in order to ensure a response to detected cybersecurity incidents and the restoration of systems or assets;
- receive, analyze and address the vulnerabilities identified by internal or external sources (in-house testing, bulletins or specialized security research);
- perform and review planned activities to prevent the expansion of an event to other ICT systems, mitigate its effects and resolve the incident.

Access to data retrieval and extraction tools[33] should also undergo a risk assessment and should, in order to protect against potential data leaks, be authorized only if there is an actual business.

The financial institution should demonstrate that it assesses the risks related to ongoing maintenance of its legacy systems and that adequate controls are in place to effectively manage the risks of these technologies. If the legacy systems support critical operations, the financial institution should have a strategy in place for managing ageing infrastructure.

Applications developed or acquired by end-users to automate their operations, including applications accessible via the Internet, should be approved by the relevant business areas and the institution's ICT function. Such applications should be taken into account in the information asset management and ICT risk management processes. The financial institution should ensure that appropriate safeguards against data loss or leaks and the exposure to malicious viruses linked to such applications are put in place. In addition, the financial institution should implement controls to monitor and detect the unauthorized use of such applications.[34]

---

[33] For example, the use of portable computer devices (tablets, cellphones, etc.), storage devices (USB keys, portable hard drives, etc.), e-mail, instant messaging and printed copies.

[34] The term **Shadow IT** (or sometimes **Rogue IT**) is also used to describe unapproved ICT systems implemented within organizations.

In risk and control assessment, protection mechanisms may include risk avoidance or elimination where the institution does not engage in a specific business activity. They may also include risk mitigation through controls or risk sharing or transfer.

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

As part of the regular maintenance of its register of known and potential ICT risks, the institution should clearly describe, in particular, their attributes and related control activities in sufficient detail. The ICT risk register should be updated on a forward-looking basis and the adequacy of controls should be regularly assessed.

3.3 Follow-up

In accordance with the expectations[35] already issued, the AMF expects the financial institution to implement the mechanisms need to promptly advise internal and external stakeholders, including the AMF, who may sustain serious harm due to a major operational incident (cyber incident, system failure, etc.).

The processes and procedures put in place by the financial institution for incident management should allow action to be taken and services to be resumed as quickly as possible when ICT-related incidents occur. In particular, they should:

- coordinate required responses and recovery activities after internal and external stakeholders have been notified;
- help minimize the impacts on clients;
- report incidents according to pre-determined criteria;
- share useful information contributing to enhanced information security;
- manage public relations and the impact on the institution's reputation.

In addition, the financial institution should conduct specific analyses following a major incident to improve its response and recovery plans. The institution should, in particular:

- explore the data gathered in its infrastructures by its detection systems;
- identify and measure the incident's impacts;
- mitigate or accept and document the risk for newly identified vulnerabilities;

---

35 AUTORITÉ DES MARCHÉS FINANCIERS. *Operational Risk Management Guideline,* December 2016.

- identify lessons learned when resolving the incident and communicate them to internal stakeholders;

- receive, analyze and respond to the vulnerabilities identified by internal or external sources (in-house testing, bulletins or specialized security research).

Based on lessons learned, observations and decisions made when managing ICT risks, the financial institution should review its strategies—particularly those developed during its preparatory activities (Section 3.1). The review should be guided by clear assessment objectives, established expectations and methodologies disseminated to stakeholders, and reports containing clear conclusions and tangible corrective actions.

4. Complementary standards to the AMF's guidelines

The AMF expects the implementation of sound and prudent management practices, set out in all its guidelines, to take into account tried and proven generally accepted practices specific to ICT.

ICT risk management depends on the financial institution adopting the expectations described in various AMF guidelines, including those on governance, integrated risk management and compliance. However, ICT risk management also depends on the expectations described in the previous sections of this guideline and the implementation of a number of ICT-specific practices.

In this perspective, the following practices[36] contribute to the establishment of a holistic approach. Applying them helps to prevent and mitigate ICT risks such as those related to the use and operation of ICT.

4.1 ICT security

The financial institution must implement robust security mechanisms enabling it to ensure the delivery of critical services and the identification of ICT incidents.

Mechanisms to consider include identity and access management, training and awareness, network segregation and protection of network integrity, data security, protection of endpoint devices, verification of software and microcode integrity, information protection processes and technological protection solutions contributing to system and information asset resilience.[37] Similarly, event and anomaly detection, continuous information system monitoring and detection process monitoring should be considered.

The financial institution should define a process to gather, secure, store, consolidate, treat and review ICT event logs to facilitate security monitoring operations. The latter should include firewall, application, operating system and authentication event logs.

The financial institution should ensure that physical and logical access[38] to information assets and associated resources is limited to authorized users, processes and devices and to activities authorized in accordance with a rigorous and predefined process.

Access rights should be granted on a "need to know," "never alone, "least privilege" or "segregation of duties" basis, only to authorized personnel and in such a manner as to

---

36 The topics discussed in this section are drawn from best practices recommended by national or international organizations, including the NIST, Cobit, the G7 and the ISO.

37 E.g., firewalls, network access controls, intrusion detection and prevention tools, anti-virus software, encryption and log monitoring and analysis tools.

38 This includes both regular or high-privilege user access and remote access.

prevent large data sets from being improperly accessed and security controls from being bypassed.

The financial institution should limit the use of generic or shared access accounts and ensure that ICT system users can be identified. Exceptions should be justified, compiled and documented.

The financial institution should subject its information security controls to various types of periodic independent assessments, tests and reviews as well as penetration testing[39] and red team exercises.[40]

In assessing information security risks, the financial institution should, among other things:

- identify information security risks related to the loss of confidentiality, integrity and availability of information, and name the persons responsible for the risks;

establish and maintain information security risk criteria, including risk acceptance criteria and criteria for assessing information security risks. The financial institution should actively maintain the security of its information while taking into account threats and vulnerabilities, including those resulting from changes to its information assets, the stage they are at in their life cycle[41] and its business environment.

There should be adequate segregation between operational security and risk management duties within the engineering and architecture roles in developing appropriate ICT information security for the financial institution's ICT systems.

4.2 ICT operations

Technological innovations, such as cloud computing, the Internet of things and metadata, have a significant impact on the ICT function (particularly at the level of the processes that must be adapted, including capacity management and security management, and knowledge that should be enhanced to fit new ICT systems).

In this context, it is important for ICT operations personnel to have the information and tools they need to detect any potential problems in processing centre operations, networks, IT security infrastructures and user support. Such tools and information should, among other things, assist in:

---

39 Penetration testing and vulnerability assessments produce an image of a computer system in a specific state and at a specific time. This image is limited to the portions of the system that are tested during penetration attempts. In this perspective, penetration testing and vulnerability assessments are not substitutes for an ICT risk assessment.

40 Red team exercises simulate targeted attacks to test the institution's detection and response capabilities. The institution's control processes for people and technology are reviewed throughout the exercise by simulating the objectives and actions of an attacker.

41 This refers to the process from information asset planning and design through to decommissioning and disposal.

- preparing an exhaustive inventory of information processing hardware, resources, locations, etc.;
- prioritizing ICT risk mitigation efforts;
- identifying mitigation controls such as policies and procedures for physical and logical security; data, personnel and change management; information distribution and transmission; backups; and user support;
- performance, capacity planning and control self-assessment monitoring and reporting.

The financial institution should implement a process for managing the configurations of the hardware and software components of its information systems so as to have visibility and effective and secure control of its systems.

The financial institution should minimize business disruption risk by establishing appropriate processes to manage changes affecting ICT equipment (hardware and software) and procedures involved in the development, delivery, support and maintenance of ICT production systems. These processes should provide for, among other things:

- pre-implementation security risk and impact assessments (particularly in relation to other information assets);
- sufficient testing for the new ICT and planned upgrades and patches to the existing systems prior to rollout;
- requirements and approval levels needed for the change rollout;
- clearly defined procedures for evaluating, approving and implementing urgent changes, including approvers, in order to reduce production environment security and stability risks;
- strict segregation of duties in the software updating process in order to restrict the ability of a single person to develop and compile software code and deploy it from a development environment to a production environment;
- activation of activity recording in the audit and security logs.

To reduce business interruption risk from the exploitation of software bugs or vulnerabilities, the institution should establish a framework of secure practices and standards for programming, source code reviews and application security testing for its ICT systems. Any information and ICT system availability, integrity and confidentiality issues identified in applying such practices should be compiled, monitored and corrected.

The financial institution should ensure that processes are deployed to assess and manage all operational risks associated with the use, ownership, operation and adoption of ICT. The institution should, in particular:

- implement an appropriate ICT operational structure to support the institution's business activities;
- review and understand how the existing systems support the related business processes;
- support an appropriate control environment through the identification, assessment, management and monitoring of ICT 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.

4.3 Outsourcing and cloud computing

Outsourcing does not reduce the risks inherent in ITC. It can expose the institution to increased security, operational performance and business continuity risks if poorly managed. Responsibility for properly managing those risks continues to rest with the institution. The institution should therefore identify the ICT strategic risks involved in outsourcing initiatives, implement an effective risk program for managing such risks, and monitor the risks stemming from any outsourcing arrangement.

In accordance with the expectations[42] issued by the AMF, the financial institution remains responsible for recovering its operations after a disaster affecting its suppliers when its ICT strategy is outsourced with cloud computing. It should also consider ICT risk, particularly cyber risk, when assessing the level of experience and expertise required to perform the outsourced activity and manage the outsourcing relationship.

The financial institution should ensure the effectiveness of its ICT risk management framework when outsourcing agreements are entered into with external service providers or members of its group.

The increasing use by financial institutions of cloud computing services[43] carries many advantages (economies of scale, access to good practices, agility, etc.). The distributed nature of such services may also enhance resilience to disasters or service disruptions. The AMF considers cloud computing services to be a form of outsourcing. Financial institutions should therefore refer to the AMF's expectations in its *Outsourcing Risk Management Guideline*.

---

42 AUTORITÉ DES MARCHÉS FINANCIERS. *Outsourcing Risk Management Guideline,* 2010.

43 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.).

The financial institution should have a clear understanding of the typical characteristics of cloud computing services, including colocation, data amalgamation and a strong propensity for computer processing to be performed at multiple or distributed sites. The institution should consider taking actions to identify and manage the risks associated with data access, confidentiality, integrity, sovereignty, regulatory compliance and auditing. In particular, the financial institution should satisfy itself that the service provider has the ability to identify and segregate client data through robust physical and logical controls. The financial institution should also keep all information relevant to the management of its data-related risks (e.g., nature, sensitivity and location(s) of data processing, storage and traffic) in its centralized list of material outsourcing arrangements.

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

- contractually secure its right to audit (and the right to audit of the relevant authorities, if applicable) and its right to access the premises of the cloud computing supplier;
- ensure that data and the location of computer processing are secure through the use of appropriate controls[44] (established using a risk-based approach) such as encryption technologies for data in transit, in memory and at rest;
- mitigate supply chain outsourcing risks when suppliers outsource certain activities to other suppliers;
- develop appropriate contingency plans and exit strategies enabling the institution to terminate any contractual agreement without any disruption in service delivery or any impact on regulatory compliance or the continuity and quality of ICT services provided to clients.
- monitor the development of potential concentration risk if the delivery of critical services depends on a small number of service providers;
- monitor and obtain assurance of supplier compliance with security objectives and measures and performance expectations.

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. Cybersecurity should not be considered only at the level of major suppliers or critical service providers but also at the level of the links deemed weakest.

While using the services of certain third parties may not constitute a form of outsourcing, many of those services are delivered using ICT or involve information that is potentially

[44] When establishing contractual and service level agreements, the institution should, among other things, consider using information security objectives and measures, applying its own definition of the data life cycle and determining its security monitoring and data encryption needs.

confidential. Such third parties may also be exposed to security breaches. The financial institution should assess and appropriately manage the confidentiality breach, integrity breach and availability breach risks associated with the information processed by such third parties.

4.4 Change projects and programs

The implementation of any ICT strategy requires a formal start-up of technology change management programs. Such programs require resources and need to be properly managed and monitored. They also introduce new risks that have to be mitigated. These risks include, among other things, client service disruptions, loss of competitive advantages, negative reputational impact and delays in implementing critical and strategic products or processes.

The financial institutions should establish a project management framework that will ensure the ongoing use of management practices to deliver results that meet business and security needs and objectives. Risk management under the framework should allow the related risks to be identified, assessed, managed and monitored throughout a project's life cycle.

This management framework should cover the practices needed to manage a project's entire life cycle. It should also enable the development of the comprehensive ICT project plans required to implement the strategies. These project plans should clearly define the project scope, cost-benefit and feasibility analyses, activities, deliverables and key milestones, and the roles and responsibilities of the resources needed for each project phase.

When projects relate specifically to the acquisition, development or modification of new or existing ICT systems, the financial institution should ensure that the processes, procedures and controls in its framework adhere to the security-by-design principle to ensure that a reliable, attack-resilient ICT system is implemented.

The financial institution should standardize its project management methodology and support it with tools. It should clearly define the ICT system development life cycle, which consists of various steps—including the identification of information security needs—that must be completed in sequence so that business needs can be translated into systems or applications and those systems and applications can be properly maintained.

In addition, the institution should manage project-generated structure- and process-level changes, including informal and intangible aspects (e.g., perceived impact and changes to work habits), communications, organizational readiness (e.g., resistance to change), training and post-launch support.