



January 2019 – final document

IT Risk

Discussion Paper

DRAFTED BY

Marc ANDRIES, David CARTEAU, Sylvie CORNAGGIA,
Pascale GINOLHAC, Cyril GRUFFAT, Corinne Le MAGUER

CONTRIBUTORS

Roméo FENSTERBANK, Thierry FRIGOUT,
Pierre HARGUINDEGUY, Christelle LACAZE



OVERVIEW OF THE PUBLIC CONSULTATION LAUNCHED IN MARCH 2018

The discussion paper on the IT risk was updated following the comments received after its publication on 31 March 2018 and at the ACPR conference on 18 September 2018, during which a roundtable on IT risk was held.

Seventeen French and foreign respondents (banking and insurance institutions, professional associations, and authorities) participated in this public consultation by answering the 12 questions and providing their general comments.

Its high quality was particularly emphasised, as well as the very strong interest in structuring the various elements of a risk definition and categorisation.

The updates that have been made include:

- **Clarification of the IT risk definition**, in order to highlight that it includes any inadequacy or failure that would affect one of the three macro-processes for the management of the information system. Several comments received pointed out that these risks were not limited to the information system implemented by the IT function, but could also relate to IT elements managed by the users themselves (shadow IT). The discussion paper has been revised to clearly mention these elements. Similarly, it is now specified that the risks associated with misuse by users are well included.
- **The definition of cyber security** has also been extended to indicate that these efforts to protect and respond also aim at avoiding negligence that may result in malicious IT activity.
- **Clarification on the organisation to implement IT risk control.** Thus, the document stressed the importance of an organisation in line with the three “lines of defence” model, which is advocated by international texts.¹ This organisation already applies to operational risk, but often imperfectly to IT risk, while it is part of it. According to this model, the IT function (whether it is entrusted to the IT department or shared with the business areas) is responsible for the operational implementation of the information and security system. It must thus identify its risks and define its policies and standards to control them, including security. Within the second line of defence, the risk management function is designed to determine the institution’s tolerance for IT risks, set the strategy and security policies to respect this tolerance, and to monitor the checks carried out by the first line of defence.

¹ Bank for International Settlements (2015): “Corporate Governance Principles for Banks”, July.

European Banking Authority (2013): “Guidelines on internal governance according to Directive 2013/36/EU”, including paragraphs 28 ff.

International Association of Insurance Supervisors (2017): “Application Paper on Supervision of Insurer Cybersecurity”, paragraphs 94 ff, September.

- **The role and positioning of the CISO is also specified.** Indeed, the responsibility for security should be adapted to the logic of the strongest organisation model, which is that of the three “lines of defence”. Institutions should have information systems security teams in the IT function (first line of defence), with the aim of identifying risks and defining security procedures and then verifying their implementation. But they should also have an information security team in the second line of defence, in the risk management function, in order to offer to the management body an acceptable level of tolerance to these risks for the institution, as well as a security strategy and policies to comply with this tolerance and to control the checks carried out by first line of defence. With the independence and ability to speak to the management body, the risk management officer should be able to alert them in case of exceptional risk situations.
- **Two risk factors have been added:**
 - “Default in risk analysis”: this risk factor complements those related to “risk management”, which may affect the “organisation of the information system” process. It enables to highlight the essential nature of the risk analyses to be conducted prior to new projects, new activities, when the information system involves or may have consequences for the information system.
 - “Default in software”: this risk factor complements those related to “Inadequate change management (projects, upgrades, fixes)” which may affect the “information system functioning” process. This addition allows specifying the requirements for the quality level of applications, including shadow IT.

The document revised following these interactions thus provides a more complete categorisation of IT risk to cover its different dimensions and to enable to handle it as a whole.

EXECUTIVE SUMMARY

The emergence of cyber-attacks in recent years has heightened concerns about IT risk. These concerns are not specific to the banking and insurance sectors, but they are of particular relevance to these sectors, which are essential components of a properly functioning economy and key actors in protecting public interests.

To address these concerns, the supervisory authorities have gradually ramped up their actions in this field. International bodies have developed new IT risk rules, and authorities, such as the ACPR, acting in particular within the framework of the European Single Supervisory Mechanism for the banking system, have strengthened their supervision.

This discussion paper emphasises that IT risk management is no longer a topic specific to IT teams, but must be part of an overall approach to risk control and risk management coordinated by the risk management function. Therefore, the operational risk management reference framework must be refined to more effectively include all aspects of IT risk within the recognised categories of operational risk. Under such an organisation, the management body must be directly involved in ensuring the alignment of its IT strategy with its risk appetite, but also in implementing and monitoring the risk management framework.

Based on their supervisory experience, the various departments of the ACPR have developed a definition and classification of IT risk that cover its various aspects and enable treating it globally. Institutions supervised by the ACPR can use this classification to develop or reinforce their own risk map. This classification covers the three main processes applicable to implementation and management of information systems, i.e. issues in relation to the organisation, proper functioning and security of information systems. For each of these major processes, this discussion paper describes a set of risk factors, which are examined on two levels to enable a fairly detailed analysis. For each risk factor, the main expected measures for mitigating and controlling risks are presented. These measures are optional and institutions can tailor them to their specific context. They illustrate the best practices usually observed by the ACPR and they aim to create a common ground for controlling IT risk management in the banking and insurance sectors.

CONTENTS

6	Introduction
8	IT risk and its inclusion in operational risk
8	1 Regulatory status at the international level
9	2 The ACPR's approach to defining and classifying IT risk
13	Organising the information system, including its security
14	1 Involvement of the management body
15	2 Alignment of IT strategy with the business strategy
16	3 Budget management
17	4 Roles and responsibilities of the IT and information security functions
18	5 Rationalisation of the information system
19	6 Control of outsourcing
21	7 Statutory and regulatory compliance
22	8 Risk management
25	Operating the information system ("build and run")
26	1 Operations management (systems and networks)
27	2 IT continuity management
30	3 Change management (projects, upgrades, fixes)
32	4 Data quality
34	Securing the information system
35	1 Physical protection of facilities
35	2 Identification of assets
36	3 Logical protection of assets
42	4 Detection of attacks
43	5 Response to attacks
45	Appendix: Classification of IT risk



Introduction

For several years, many international bodies have focused on the growing IT risk in the banking and insurance sectors. This emphasis is driven by two observations. Firstly, institutions' operations now rely entirely on automated information systems, including for customer relations,¹ and these environments have become complex to manage. Secondly, even when all precautions are taken, IT damage is a major risk for these institutions' operations. In particular, the capacity of cyber-attacks to cause harm has steadily increased in recent years. Whereas, initially, these attacks focused primarily on customer equipment and therefore were discrete events that caused little overall disruption, they now directly target institutions' IT environments and can have major consequences, including systemic impacts, due to the increasing interdependency between the various financial players.

In response, the bodies that develop international standards applicable to the banking and insurance sectors have begun to articulate their expectations vis-à-vis the industry. The European Banking Authority (EBA) has published several documents prescribing standards in relation to the IT risks to which the banking sector is exposed,

including guidelines to be followed by supervisory authorities for adopting a uniform approach to assessing institutions' IT risks.² The European Insurance and Occupational Pensions Authority (EIOPA³) has published an issues paper on cyber risk⁴ and has undertaken a review of this risk in conjunction with major players in the insurance sector.

Among the various IT risks, cybersecurity risks have been given particular attention by several authorities. The G7 has adopted high-level, non-binding principles intended to provide guidance and harmonise actions in this area,⁵ and continues these actions on several fronts to encourage the efforts of regulators in the sector. The Committee on Payments and Market Infrastructures (CPMI)⁶ of the Bank for International Settlements and the International Organisation of Securities Commissions (IOSCO)⁷ have published guidelines to improve the resilience of market infrastructures to cyber-attacks.⁸ The International Association of Insurance Supervisors (IAIS)⁹ has also published an issues paper on cyber risk for the insurance sector,¹⁰ which will be followed by an implementation document.

1 This is at times referred to as the "digitisation" of banking and insurance operations.

2 EBA (2017): "Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)", 11 May 2017.

3 In French *Autorité européenne des assurances et des pensions professionnelles* (AEAPP).

4 Drafted by its Insurance and Reinsurance Stakeholder Group (IRSG): "Cyber Risk – Some Strategic Issues" (April 2016).

5 G7 (2016): "Fundamental Elements of Cybersecurity for the Financial Sector", October and G7 (2017): "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector", October.

6 Committee on Payments and Market Infrastructures (CPMI).

7 International Organisation of Securities Commissions (IOSCO).

8 CPMHOSCO (2016): "Guidance on Cyber Resilience for Financial Market Infrastructures", June.

9 International Association of Insurance Supervisors (IAIS).

10 IAIS (2016): "Issues Paper on Cyber Risk to the Insurance Sector", August.

All of these documents explicitly or implicitly recognise IT risk as an operational risk, as documented and then regulated by the Basel Committee on Banking Supervision (BCBS) from 2003. However, the inclusion and treatment of IT risk within operational risk still needs to be clarified for the same treatment principles to apply thereto.

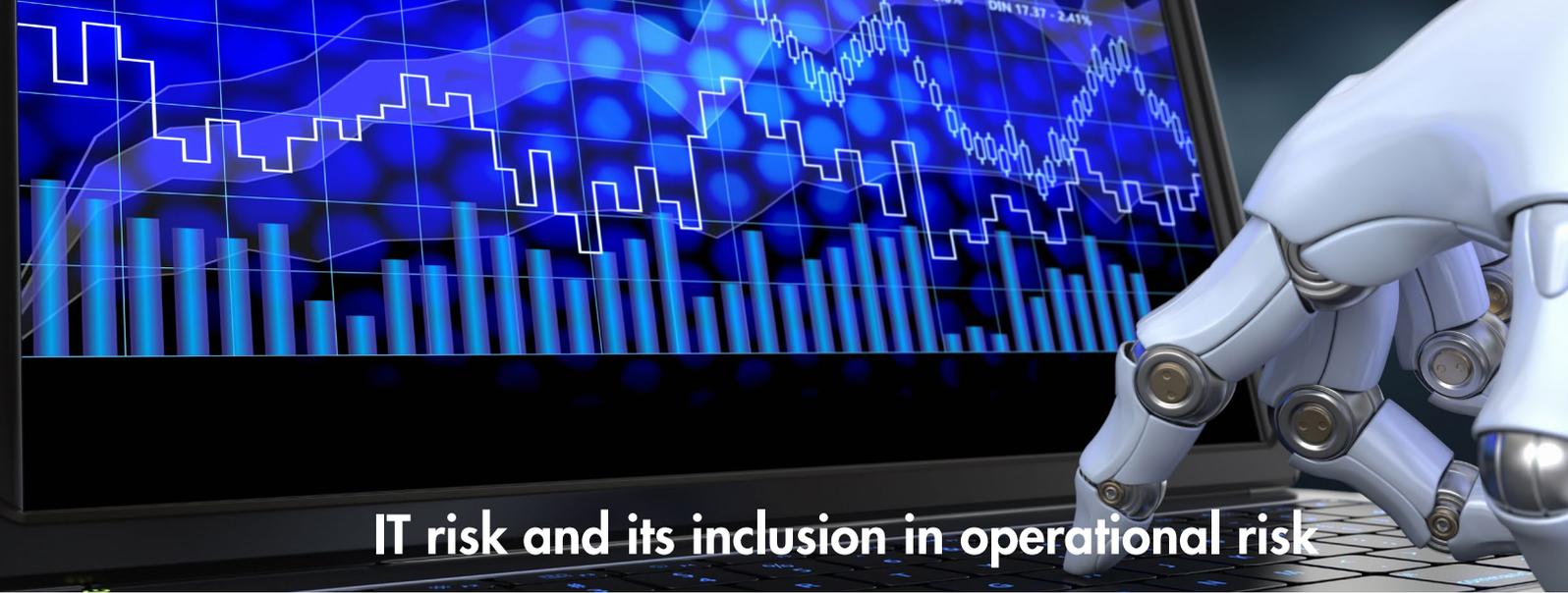
On their side, the supervisory authorities have also significantly ramped up their actions in the IT risk field. Starting in November 2014, when the European Central Bank (ECB) acquired direct supervisory powers over the largest banks of Euro-zone (“significant institutions”), assisted by national supervisory authorities comprising the Single Supervisory Mechanism (SSM), it immediately initiated several off-site supervisory actions and onsite inspections. Assessment questionnaires focusing on cybersecurity and IT outsourcing practices enabled a quick evaluation of the strengths and weaknesses of the sector, which led to corrective actions. Numerous onsite inspections, usually conducted by the national authorities, supplemented the process and provided precise information on actions to be carried out.

This approach was already well-established in France because, in 1996, the Commission bancaire (Banking Commission) had published a White paper on the security of information systems in credit institutions and, since 1995, it has had a unit dedicated to risks in relation to information systems within its onsite inspection teams. On the strength of this experience, the ACPR participated in the ECB’s actions by making its off-site supervisors available to the SSM’s joint

supervisory teams and by having onsite inspections performed by the Banque de France’s inspectors. In the areas in which it has direct authority, such as “less-significant institutions”, other banking sector entities (in particular, finance companies and payment service providers) and insurance, the ACPR also carries out numerous actions in connection with its ongoing supervision and onsite inspections. The constant increase in IT risks is an ongoing challenge that requires expanded resources and skills. To meet this challenge, the ACPR has continued its training actions and supplemented the dedicated onsite inspections teams with a network of around 20 IT risk experts. These experts represent the ACPR in various international bodies working on IT risk and cybersecurity issues.

This discussion paper was drafted by IT experts from the ACPR’s network. It aims to focus attention on IT risk issues deemed significant, both in terms of recognising and reducing such risks. It is a contribution to the discussion on how IT risk controls should be incorporated into the operational risk management framework. It may also contribute to work on improving the “operational resilience” of institutions, i.e. their ability to absorb operational disturbances of any kind.

Firstly, the paper proposes a definition of IT risk, which is viewed as part of operational risk. Secondly, this definition is supplemented by a proposal for classifying IT risk in a manner that covers all aspects in a coherent manner. For each factor included in this classification, the paper explains what it deems to constitute sound risk management.



IT risk and its inclusion in operational risk

11 BCBS (2003): "Sound Practices for the Management and Supervision of Operational Risk", Basel Committee Publications No. 96, February.

12 BCBS (2006): "International Convergence of Capital Measurement and Capital Standards", June 2006 (Basel Committee Publications No. 128).

13 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV Directive). Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (CRR, Article 4).

14 Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II). Article 13 (33) defines operational risk as the "risk of loss arising from inadequate or failed internal processes, personnel or systems or from external events".

15 Article 10 of the *Arrêté du 3 novembre 2014* on the internal control of companies operating in the banking, payment services and investment services sector subject to the supervision of the ACPR defines operational risk as "the risk of loss due to inadequate or failed internal processes, personnel and systems or external events, including legal risk. In particular, operational risk includes risks associated with events with a low probability of occurrence but significant impact, the risks of internal and external fraud defined in Article 324 of the aforementioned Regulation (EU) No. 575/2013, and model-related risks".

1 Regulatory status at the international level

The concept of operational risk, which was originally devised by the banking authorities, was then adopted by the insurance industry authorities. Since 2003, the Basel Committee for Banking Supervision has steadily expanded its recommendations on the management of operational risk.¹¹ It has also added capital requirements to enable institutions to deal with operational incidents they may experience.¹² To cover the multiple facets of operational risk, the Basel Committee has adopted a broad definition that includes internal failures and external events, and focuses on the risk of financial loss, whether direct or indirect. According to the Committee, operational risk covers any "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition, with slightly different wording, is now included in various legislative and regulatory frameworks, notably the European directives governing the banking sector¹³ and the insurance sector.¹⁴ It has also been incorporated into the French banking laws.¹⁵ This framework has been

intentionally designed to be broad and flexible so as to cover a wide variety of organisations and enable institutions to apply it in a manner that is proportionate to the breadth and complexity of their activities.

None of these documents explicitly addresses IT risk, although the various authorities are in agreement that it should be included under "process, personnel and system failures", for example in the case of IT system breakdowns or errors, or under "external events" in the case of cyber-attacks. This was due to the original reasoning of the standards-setting authorities, which considered IT tools, and information systems as a whole, to be components at the service of institutions' businesses, rather than an essential concern. Under this approach, the most important risks are those specifically related to business operations, such as credit, market or insurance risks. An IT failure is thus primarily viewed in terms of its consequence on the business of its user. The recognition of operational risk in the 2000s was a breakthrough insofar as a qualitative treatment (risk management and internal control), and later a quantitative treatment

(capital requirements), supplemented “business” risks and were extended to various events that could impact business support functions (including the IT function). The extensive and in-depth business continuity work carried out around 2005 also focused on more robust measures in this area to improve fault tolerance, but did not change the general operational risk framework. Apart from a broad all-encompassing definition, operational risk continues to be classified into seven (discretionary) categories, none of which, individually or combined, truly cover the varied aspects of IT risk.¹⁶

The recent work focusing on IT risk is therefore a significant development. There is a more explicit recognition of this risk due to its growing and cross-disciplinary importance for all businesses. Nevertheless, although all regulators classify it among operational risks, specific guidance on defining and handling IT risk has been slow to come. Accordingly, institutions have been given discretion in this area, but they must demonstrate that they deal with all aspects of IT risk in accordance with the provisions applicable to operational risk. This is not an easy task. Banking and insurance institutions, like all businesses, have long relied on sound IT management principles published by various international standards bodies, such as the International Organization for Standardization (ISO), to which some banking regulations themselves refer.¹⁷ However, these standards, which have been developed by IT professionals, do not share the conceptual framework established by banking and financial regulators. The concepts of risk management, although similar, are not exactly the same and, for example, are not based on an internal control system. Furthermore, these

standards are not necessarily pertinent to the corporate governance system that the banking and financial regulators require institutions to put in place. Supervisory authorities will ensure that institutions’ IT risk management framework is not entirely decided and deployed by the IT department, but require that this aspect be properly integrated into the general operational risk management framework. This should lead institutions to organise their IT risk management according to the “three lines of defence” model.¹⁸ With such a set-up, the IT function, in charge of the various operational processes related to the information system, is responsible as the “first line of defence” for implementing these processes with caution. It acts under the control of the “second line of defence”, which is generally the risk management function and in accordance with the risk management policies decided by the latter. Finally, the internal audit function acts as a “third line of defence” by controlling the actions of the first lines and assessing the effectiveness of the risk management framework.

2 The ACPR’s approach to defining and classifying IT risk

The ACPR General Secretariat has undertaken work to clarify the definition and treatment of IT risk. This cross-disciplinary work, aimed at both the banking and insurance sectors, was carried out by the ACPR’s network of IT experts. This work culminated in a definition and classification of IT risk intended to cover all aspects thereof. These elements are intended to contribute to the work of various international bodies, particularly in view of the Basel Committee’s revision of its Principles for the Sound Management of Operational Risk¹⁹ and the IAIS’s revision of its Insurance Core Principles.

¹⁶ CRR, Article 324: internal fraud; external fraud; employment practices and workplace safety; clients, products and business practices; damage to physical assets; business disruption and system failures; execution, delivery and process management.

¹⁷ EBA (2011): “Guidelines on Internal Governance (GL44)”, section E.30.2.2, September.

¹⁸ BCBS (2011): “Principles for the sound management of operational risk”, June, and EBA (2017): “Guidelines on internal governance under Directive 2013/36/EU”, September.

¹⁹ BCBS (2011): “Principles for the sound management of operational risk”, June.

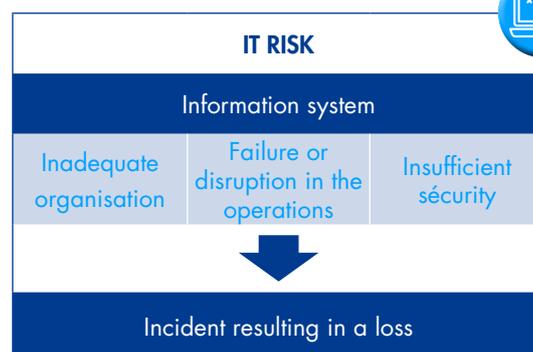


Definition of IT risk

At the outset, it seems important to have a clear definition of IT risk that is pertinent from the standpoint of IT activities, as well as with respect to customary operational risk analysis concepts. To date, there is no such definition in the regulations applicable to the banking and insurance sectors. The IAIS refers to a definition proposed by insurance sector professionals (The CRO Forum).²⁰ In 2014, the EBA included a definition in its guidelines on the Supervisory Review and Evaluation Process (SREP)²¹, which need to be supplemented in light of experience and knowledge acquired in this area.

To ensure its completeness, the definition developed in this document aims at covering the risk to all management processes of an institution's information system. These processes are grouped into three main elements: organisation and governance, proper functioning and quality, and security of the information system. IT risk is taken into account as a whole and the definition does not prejudge the organisation chosen by the institution, which may consist in entrusting the IT department with the entire responsibility for the information system, or in letting the business lines directly manage the part that concerns them. It is seen as an IT risk factor any kind of failure affecting the management processes of an institution's information system that would cause a direct or indirect loss.

The definition chosen by the ACPR aims to cover all aspects of risk, including aspects in relation to information system governance and organisation.



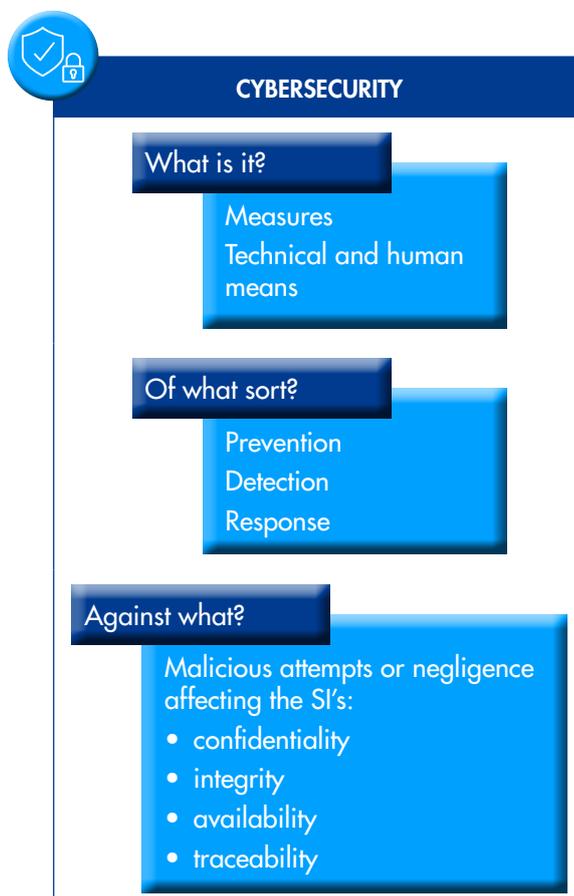
This definition is: **“IT risk” is the risk of loss arising from an inadequacy, or failure of organisational, operational or security processes of the information system, which includes all systems equipment, networks, software and data, and human resources contributing to processing the institution's information.** This definition is consistent with an operational risk approach because, if the risk is realised, it results in a loss (or near-miss, opportunity cost, undue gain or additional costs). It does not prejudge the causes, i.e. risk factors, a categorisation of which is given later in this document following the three information system management processes. It does not include reputation risk, which is not specific to it, but like any operational risk, IT risk may also worsen from reputation risk. Deliberately, the chosen definition is broad in scope and applies to the information system as a whole, i.e. its technical systems and organisation, as well as the human resources involved in data processing. It also applies regardless of the term used (information system risk, risk of “information and communication technologies – ICT” or IT risk). For reasons of convenience, the customary term “IT risk” has been chosen and covers these various other terms. In addition, the information system covered by the definition refers to what is being implemented by the IT department, but also to what is managed outside its control by user business and which is commonly referred to as “shadow IT”.

20 “Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments”.

21 EBA SREP GL (2014): “Information and communication technology (ICT) risk” means the current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability, integrity, accessibility and security of such infrastructures and of data.

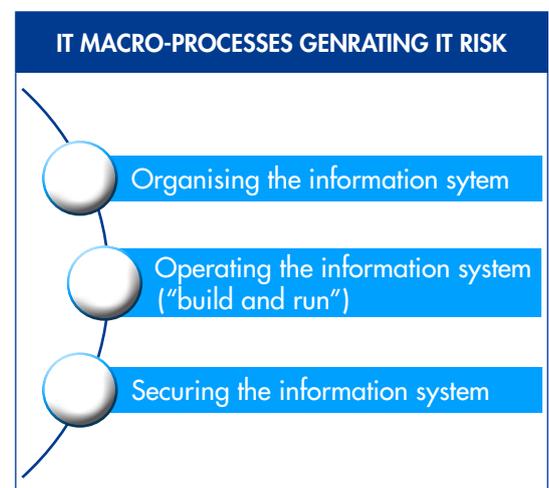
This definition includes cybersecurity, but is not limited to it. Cybersecurity refers to an approach designed to protect against and respond to attacks against all or part of the information system, and thus does not cover all IT risks. Therefore, cybersecurity should be included in the approach to treating IT risk and not the other way around. For its work, the ACPR uses the definition of cybersecurity adopted by the ECB.

According to this definition, **“cybersecurity is the set of controls and organisational measures, as well as the resources (human, technical, etc.) used to protect the components of the information system and communication networks against all logical attacks, whether carried out through physical or logical security breaches. These controls and measures include prevention, detection and response to any malicious IT activity or any negligence, which may affect the confidentiality, integrity or availability of systems and data, as well as the traceability of operations performed on this system and these networks”**.



Classification of IT risk

This proposed classification of IT risk categorises in an orderly manner all identified risk factors for the three IT macro processes, i.e. organising the information system (including its security), operating the information system (“build and run”), and securing the information system. Primary and secondary IT risk factors have been identified for each of these three macro processes. These factors may possibly cumulate.



Organisation-related risk factors include situations of inadequate decision-making and overall supervision, which can lead to poor IT management, inadequate support for business needs, and unsound management of IT risk in general.

Operation-related risk factors are considered in the broad sense of the term, i.e. including operations and projects, business continuity and data quality. They all focus on factors that may affect the proper functioning of the information system and thus impact the ability of an institution to conduct its business. In particular, the classification includes the risks of inadequate supervision of projects and changes, business continuity failures, and poor data quality (customer

data, reports to be submitted to regulators or reports specific to institutions not intended to be made public).

Lastly, security-related risk factors cover all malicious attacks that impact the availability, confidentiality and integrity of data and systems managed by the institution. These include risk factors such as inadequate identification and protection of IT assets, deficient detection systems and weak response capacity to attacks.

The proposed classification is set out in detail in the appendix hereto. It is more granular than the current classification of the Basel Committee on Operational Risk and is intended to complement it. Institutions are free to use their own classification or to use the one proposed by the ACPR. In all cases, the full range of risks identified should be covered, unless not justified by their organisation or business model. In this regard, it is worth noting that if all or part

of an institution's information system is outsourced, this does not mean that the institution is no longer exposed to these IT risks. It must therefore continue to identify and control these risks pursuant to its operational risk management framework and internal control system.

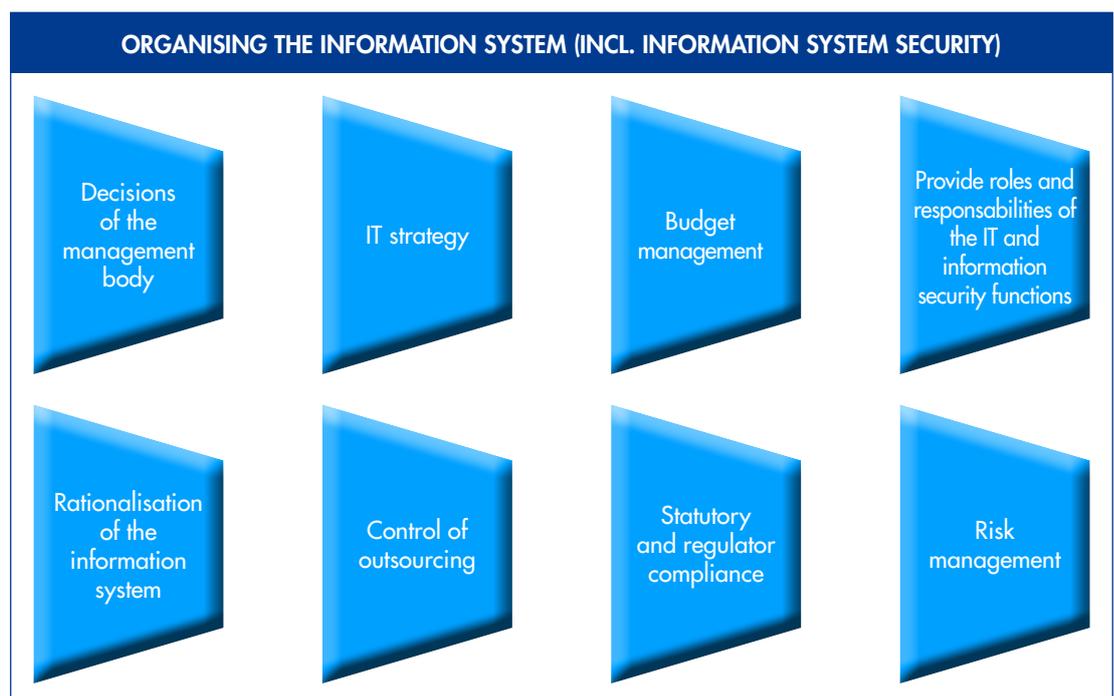
The sections that follow describe the risk factors included in the proposed classification and the measures deemed to be of use or necessary to control them. These risk factors are defined as events or situations that may increase the probability of IT risk. The measures to control these risk factors that are described in this paper are obviously not exhaustive or mandatory. The primary intent is to establish a common analysis framework for all institutions that will enable them to adopt sound practices for managing these risks. The ACPR may also use these measures as a basis for its contributions to the work of the various international bodies in which it participates.

Organising the information system, including its security

Information system organisation refers to the macro process covering all decision-making actions (sometimes referred to as “governance”), coordination (such as defining a “strategy” and allocating the corresponding resources), the allocation of responsibilities within the entity, as well as the policies and actions implemented to ensure proper management of the information system (for example by reducing its complexity), control of outsourced functions, and compliance of IT tools with the laws

applicable to the institution. Lastly, a sound and prudent organisation requires a risk management system that includes internal controls. These organisational actions are also important for the security of the information system.

The sections that follow explain the primary and secondary risk factors that may impact information system organisation and security, as well as the main measures to control these risks.



1 Involvement of the management body

Due to their technical nature, or for cultural reasons, the “management body” (which is the European regulatory reference to both senior executives and boards or equivalent²²) may be tempted to disregard IT issues and choose to rely entirely on IT managers.²³ However, if the IT managers do not have an accurate vision of the overall issues the company faces, or if they are not properly supervised, there is a risk that they may not be able to provide IT services that are adequate for the company’s business. It is therefore important that corporate governance principles, emphasising managerial responsibility and fostering clear and transparent decision-making processes, also be applied to IT activities. In other words, the management body, which is responsible for the proper functioning of the institution, must be involved in decisions relating to the information system and must ensure IT risks are controlled.

The ACPR’s IT experts have identified three risk factors generated by inadequate involvement of the management body.



INVOLVEMENT OF THE MANAGEMENT BODY



Inadequate understanding of issues



Inappropriate decisions



Insufficient monitoring

Inadequate understanding of issues

Maintaining and developing an information system requires anticipating the

future needs of the business lines and support or control functions, and ensuring they have the appropriate technological resources when needed. Information system quality and control must be included in strategic choices. If the management body inadequately understands these issues, there may be delays in adapting to change or situations where control over the information system is not maintained.

It is therefore essential that senior executives and independent directors understand the information system development and management issues relevant to the proper functioning of their institution. If they lack expertise in this area, they should, for example, schedule working meetings with internal and external specialists dedicated to these matters.

Inappropriate decisions

Appropriate involvement of the management body requires that it controls decisions relating to information system maintenance and upgrades. Otherwise, poor decisions may be taken, resulting in an inadequate information system.

Although it does not have to be involved in every decision, it is important that the management body sets the policies applicable to the information system. These policy choices should be based on a solid risk analysis in line with the risk management system and the risk appetite that has been approved. It is essential that major decisions relating to the information system, which involve the business lines or may generate significant risk, be taken by senior executives under the supervision of the board.

²² In this document, the words “the management body” refer both to senior executives (“*Direction générale*” in French) and to the supervisory body of the institution, like the Board (“*conseil d’administration*” or “*conseil de surveillance*” in French, or any similar body).

²³ Or, more broadly, on the Information Technology Department.

Insufficient monitoring

If the management body does not closely monitor the proper functioning and security of the institution's information system, it will be difficult to react quickly in the event of an operational or security incident.

Complete information on quality, performance, project schedules and security maintenance indicators is therefore essential to enable the management body to fulfil its responsibilities. These indicators should not be monitored solely by IT managers. The management body can of course focus on regularly monitoring certain key indicators that are deemed pertinent with respect to the defined strategy, risk control or oversight of a particular service.

2 Alignment of IT strategy with the business strategy

Information technologies evolve constantly. These developments can provide institutions with new opportunities, but may also generate new risks. IT strategy, including with respect to security issues, is a component of institutions' overall strategy. Its objective is to meet the needs of the business lines and support functions, but it is also increasingly at the core of institutions' strategy to maintain or gain a competitive advantage through the use of technological developments. If the institution does not define an IT strategy, or if the strategy is not aligned with the needs of the business lines, the information system may ultimately fail to meet the institution's requirements, which could compromise its ability to achieve its commercial and financial objectives. The sections below discuss the risk factors that have been identified in this area.

Failure to anticipate business needs and technological upgrades/issues/uses

IT upgrades often take several years and must be properly anticipated. Unless based on a specific strategy that combines the variety of needs and foresees technological developments, upgrades to the information system may be erratic and unable to service the institution's requirements in a timely manner.

Therefore, it is important for IT managers, in conjunction with the business lines and with the approval of the management body, to formally adopt a genuine IT strategy in line with the institution's strategic objectives. To be pertinent, the IT strategy must anticipate medium-term needs and developments and set concrete objectives for managing them. Ordinarily, this should be the product of a formal process that includes consultations with the business lines and functions about their needs, and incorporates IT risk management (e.g. risks in relation to complexity, obsolescence and security). Thereafter, its implementation should be closely supervised to ensure objectives are achieved, anticipate difficulties and make necessary adjustments. It is also important to update the strategy annually to reflect new needs. If the institution is a member of a group, it is important that its strategy is consistent with that of its group.

Inadequate tools and service levels

If an institution has no IT strategy or if the strategy is not pertinent, there is a risk that the IT function will not appropriately take users' needs into account and that the institution will not be able to conduct its business optimally.

It is therefore important to include users' operational needs in strategic considerations, for example regarding the availability and security of environments. Obviously, the strategy document will not describe service levels with the same degree of detail as a service level agreement (SLA). Nevertheless, it is important to conduct a global analysis of the institution's operational needs, for itself and for its customers and partners, so as to avoid compromising its business.

3 Budget management

The budgetary process allocates the amounts required to implement the IT strategy that has been approved. These include expenses (equipment, licences, services, training, etc.) and human resources (internal or external resources, including project management services). The budgets allocated must then be monitored to make any necessary adjustments or to redefine them if required. If the budget allocation process is not clearly defined or if no such process exists, if the budget is not aligned with the strategy previously developed and/or if expenditures are not rigorously monitored, the financial resources available may not be used optimally for the purposes of planned IT changes.

Inadequate budget alignment with strategy

The IT budget must enable implementation of the IT strategy approved by the institution. If it is insufficient or allocated too late, the strategy may not be implemented or implementation may be delayed.

It is therefore advisable to make the two processes consistent so as not to generate discrepancies. Most frequently, the two

processes follow one another or are associated. Projects and maintenance should each receive a specific and well-identified budget allocation to avoid depriving either one of necessary funds. The resources made available should also correspond to the deployment stages set out in the IT strategy.

Non-existent or insufficiently clear budget allocation

Without the required resources, the IT function will be unable to properly manage the information system. A documented process, binding on all departments of the institution, including those concerned with information security, is essential to manage the process of preparing and allocating IT budgets.

This process includes identifying functional and technical requirements in relation to all applications, as well as those requirements in relation to the operation of the information system and data security. Given the life cycle of IT programs/projects,²⁴ it is important to combine: (i) a multi-year approach that allocates global budgets for large-scale programmes with (ii) an annual approach that defines the budget for the coming year, including the share of major programmes during the relevant year and smaller projects that are considered a priority. It is important that all stakeholders be involved in the process and that final decisions be taken by the management body.

Inappropriate oversight of expenditures

Monitoring and controlling IT costs are essential to maximise the institution's profitability, to report to the management body on the progress of projects and budget overruns and to make any necessary adjustments.

²⁴ In this paper, a programme refers to a set of projects that are coordinated in common due to their highly complementary nature, which does not exclude individual coordination of each project.

Budget control requires monitoring overall expenditures, which is ordinarily done by the financial function, as well as monitoring by programme and by project, both on an annual basis, against the allocation for the year, and on a multi-year basis, against the budget originally attributed, adjusted, if necessary, after the programme or project is launched. It is important that any budget overruns over a certain threshold be justified and approved by the management body, or that they be offset by management decisions. A clear and up-to-date procedural framework should provide for standardised procedures for managing expenditures, approving budget overruns, decision-making and informing senior executives and the board.

4 Roles and responsibilities of the IT and information security functions

Although senior executives have full responsibility for issues related to the information system and its security, they need to rely on IT managers and their teams, who are referred to in this document as the “IT function” and “information security function”. The information system will not be properly organised if these roles and responsibilities are not clearly defined and allocated, if the managers’ skills profiles are not appropriate or if insufficient resources are budgeted.

Poorly defined, allocated or communicated roles and responsibilities

A clear division of responsibilities between the managers will facilitate efficient management of activities and avoid blockages. As has been the case for other banking and insurance functions (risk, compliance), supervisors now increasingly expect to be

able to interact directly with IT managers who hold full and complete authority within their remits.

Therefore, the IT function should be in a position to globally manage an institution’s information system. Ordinarily, the IT department includes the application development and maintenance teams, as well as the staff responsible for operating system and network infrastructures. However, in some cases, the business lines and support functions have their own development and maintenance teams, and at times their own production teams, which may also be set up as IT departments. Accordingly, it is important that one person be in charge of the IT function broadly speaking, i.e. all teams, whether they are within the central IT department or the business lines or functions. This manager must have full authority over the strategic directions of the entire IT function, the overall budget, the standards and procedures for ensuring sound management and control of information system risks. The head of the IT function should be sufficiently senior in the hierarchy, ideally reporting directly to the management body, to ensure that IT issues are properly considered within the institution.

The information security function must also be clearly identified and granted full authority. This function, which is headed by the chief information security officer (CISO), originally focused on defining the information security policy, raising awareness of security issues among teams and contributing to risk control, for example by conducting security studies or performing level-2 controls. During its inspections, the ACPR has noted that this function was often incorporated into the IT function, whereas it is preferable that it be independent so as to enable it to give objective opinions on IT security, as well as to alert the

management body of high-risk situations. Similarly, ACPR's inspections have shown that the CISO does not always have a sufficiently high hierarchical position to give him sufficient authority and ability to be heard directly by the institution's management body. Yet, the intensification of cyber risks makes it crucial the alert of managers and the position should be placed high in the hierarchy. The ACPR considers that, rather than relying on a single responsibility, the information security function should be more structured along the lines of the three "lines of defence" model advocated by international texts.

Thereby, institutions should have information security teams in the IT function (1st line of defence), with the aim of identifying risks and defining security procedures and then monitoring their implementation. They should also have an information security team in the 2nd line of defence, within the risk management function, to offer the senior executives an acceptable level of tolerance to those risks for the institution, as well as a security strategy and policies to comply with this tolerance, and to control the checks carried out by the 1st line of defence. With independence and ability to speak to the management body, the risk management function should be able to alert them in case of exceptional risk situations. It should also be able to give independent opinions that prevail over those of the IT function and the business lines. These two lines of defence are subject to periodic control by the audit, with specialised teams acting as "3rd line of defence". Such an organisation would benefit from being applied to all IT risks as described in this document.

Inadequate or insufficient staffing

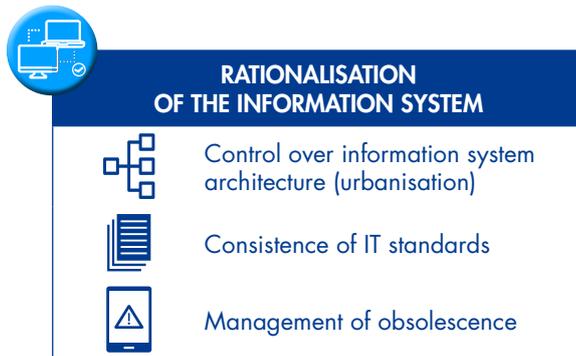
Senior executives' choice of the persons appointed to head the IT and IT security

functions is essential for the proper organisation of the information system. These functions must also have sufficient staff with the necessary skills and maintaining them updated through trainings, or they risk being unable to perform their duties, which would hamper the institution's proper operation and security.

It is important that the persons chosen to head the IT and IT security functions have the requisite experience and professional expertise because these positions require strong technical and managerial skills. These prerequisites also apply to all IT staff, and it is desirable to adopt a formal human resources management policy in this area that specifies the target distribution of internal and external staff, as well as the key functions for which it is necessary to maintain sufficient in-house expertise, including to supervise core functions that are outsourced. It can be supplemented by a skills management policy that defines staff training objectives, in particular obtaining professional certifications and providing additional training on technological and business developments.

5 Rationalisation of the information system

Over time, information systems undergo significant development as new tools are constantly added and old ones are retained, at times partially. The information systems of banking and insurance institutions are now vast sets of applications, systems and networks that may be difficult to map due to their complexity. Various factors create a risk of loss of control over the information system. These include a lack of control over the architecture of the information system, inconsistent IT standards and a failure to manage obsolescence.



Lack of control over information system architecture (urbanisation)

When an information system becomes highly developed, an architectural approach, sometimes called “urbanisation”, is needed to avoid chaotic uncontrollable growth. The principle is similar to that of the development of big cities. Applications and systems that work together are grouped together to simplify and better control their interactions. This work usually requires mapping and inventorying the components of the information system. Application and systems architects are responsible for ensuring that components are not added to the information system in a disorganised manner. They can identify areas of weakness and make recommendations on optimising and upgrading the information system.

Inconsistent IT standards

Uncontrolled development of an information system can occur if the actions of systems developers and engineers are insufficiently guided by design, development, production and security standards. The aim of these standards is to harmonise practices and prohibit the use of unapproved solutions within the institution. Different standards apply to different activities: applications development, production and commissioning

of network solutions. To be fully effective, these standards must be harmonised by the central IT function in order to avoid diverse or inconsistent practices within the various entities comprising the IT function (e.g. by the IT departments of the various subsidiaries of a group).

Failure to manage obsolescence

IT technologies evolve rapidly and must constantly be updated to avoid the risk that the information system will no longer be able to be maintained. This is a demanding task because it requires paying close attention to the frequent version changes of software and systems used, which involves, for example, particularly careful oversight of IT assets. More fundamentally, institutions should regularly replace applications that use old programming languages that are no longer used by developers. Security requirements may also justify regularly updating technologies used.

6 Control of outsourcing

Because institutions may need skills or a workforce they do not have in-house, IT activities are often outsourced to service providers, which may belong to the same group as the institution, or which may be third-party companies. Risks of insufficiently supervised outsourcing may arise if the contractual framework is poorly defined, if dependence on a vendor is not controlled, if the expected service levels are not rigorously monitored and if changes in vendors are not anticipated sufficiently in advance to activate contractual reversibility procedures.

Inadequate contractual framework

An inappropriate contractual framework, i.e. a non-existent, incomplete, invalid,

unbalanced or imprecise contractual framework, may mean that the institution will not obtain the expected service, which may be detrimental to the proper operation or security of its information system.

The management body should approve major outsourcing projects on the basis of the opinions expressed by the various control functions, including the IT security function. The contract and its associated documents should serve as the reference that defines the rights and obligations of the institution and the service provider. Such contract is required, even if services are outsourced within the same group. It is important for the contract to describe in detail the nature of the service, expected service levels, permanent controls to be executed, incident handling and business continuity procedures, IT security requirements, contractual reversibility conditions, the roles and responsibilities of the contracting parties, the contacts responsible for routine monitoring of the service, the bodies tasked with coordinating the relationship and the type of information to be regularly reported to the institution. The institution must be informed of chain outsourcing (sub-contractors), and it may require that such chain outsourcing be authorised in advance. In all cases, the institution must ensure that such outsourcing does not generate any additional risk. Moreover, the contract must include a right to audit the service, with possible onsite access, and it must describe the regulatory provisions applicable to the service provider. This right of audit must not be unduly limited by restrictive clauses (long notice periods, various limitations). The contract should also grant audit rights to the institution's supervisory authorities. It may be useful for the institution's legal department to approve standard clauses to ensure that all of the institution's

contracts comply with the laws and regulations on outsourcing and protect the institution's interests in a balanced manner.

Overdependence

If a service provider acquires a predominant position due to the scope of the IT activities it performs for an institution, the institution may find it difficult to impose its requirements, including if service deteriorates. Outsourcing to service providers abroad, especially outside Europe, may expose institutions to an inadequately supervised legal environment.

Developing an outsourcing policy that is approved by the management body provides a framework that defines the activities the institution is willing to outsource, and those that should be retained in-house due to their sensitive nature. Such policy should assess the legal risks associated with outsourcing to foreign jurisdictions, especially outside the European Union (for example, with respect to data protection rules). Controlling the risk of overdependence on one or more vendors requires consolidated oversight of contracts negotiated with vendors, as well as approval by the management body if outsourced activities exceed a dependence threshold to be defined. The outsourcing policy should also specify the conditions applicable to outsourcing (roles and responsibilities, the process for finding and selecting service providers, the contractual framework, and service oversight procedures).

Inadequate monitoring of service levels

Service levels are contractual commitments that a service provider makes to an institution about the quality and security of IT services. If no service levels are set, or if

the expected performance levels are too low, the institution will be unable to demand high-quality services.

It is therefore essential that service levels be contractually defined and that they be monitored on an ongoing basis by a dedicated team of the institution, both by analysing the dashboards set up in agreement with the vendor and by handling event occurrences, if necessary, by agreeing an action plan. This arrangement is most effective if a joint steering committee, comprising representatives of the institution and the vendor, is set up and tasked with monitoring service quality. The steering committee should be chaired by a manager whose hierarchical level is consistent with the sensitivity of the outsourced activity. For the most sensitive activities, it is advisable for the chair of this committee to be the head of the IT function or a senior executive. In addition, holding meetings of a technical committee, comprising members with the appropriate hierarchical level, may be a useful practice. Finally, a process should be set up for escalating degraded service quality or business relationship issues to the IT function or senior executives.

Inadequate reversibility procedure

Changing vendors in the IT field is relatively complex because it usually entails taking over an existing service, while guaranteeing users continuity of service with equivalent service levels, as well as recovering archives covering a long period.

Therefore, this process requires appropriate advance planning, taking into account budgetary constraints, respecting the timetable for activating the reversibility clause with the outgoing vendor, and precisely

defining the work to be performed. Some of this work will be taken over by a new service provider, or by the institution if the activity is brought in-house, whereas other work may require specific treatment, for example in the form of a project to be budgeted and planned.

7 Statutory and regulatory compliance

Like any undertaking, institutions must comply with the laws applicable to their business. Therefore, in terms of organisation, the IT solutions institutions use cannot be developed by IT engineers autonomously, without consideration for the legal obligations applicable to the institution. Otherwise, the institution risks breaching the laws governing its business, which is unacceptable and could also prove highly detrimental to its relations with customers. The information system may be non-compliant if the business lines' expression of needs is inconsistent with the applicable law, if IT developments do not follow the legal specifications set by the business lines, or if production standards or techniques are in violation of the applicable law.

Business needs not in compliance with applicable laws

Users are responsible for defining their information system needs. If they do not comply with the legal requirements applicable to their activity, the expression of their needs may include non-compliant requirements, which will then be incorporated into the information system and cause the institution to be in breach of the law.

Preventing such risk requires a project management methodology that includes a stage

at which it is determined that the business lines' expression of needs is in compliance with the legal requirements applicable to the institution, as well as with the institution's internal procedures, for example if they are stricter. Ordinarily, the legal department should be consulted and its agreement obtained with respect to the needs expressed.

Information system not in compliance with the business lines' legal instructions

The IT engineers should, in principle, comply with the user's requirements and, therefore, incorporate the legal provisions applicable to their activity if they have been properly formulated. If not, the institution will have a non-compliant information system. Moreover, legal requirements may change over time, thereby rendering the information system non-compliant.

It is therefore important that any modification in the information system include prior and ongoing checks of the compliance with the law applicable to the institution, and that potential violation be detected and remedied. This applies to both internal software or services and to those acquired or leased to external providers. If the applicable law is amended significantly, the users responsible for processing must submit change orders to be implemented by the IT engineers.

Incompatibility of IT standards with applicable laws

IT standards applicable to programming and operating rules may include provisions inconsistent with an institution's legal obligations, for example concerning personal data protection or data retention periods. These standards should not preclude compliance with the needs expressed by users.

They should be regularly updated to make them consistent with these obligations.

To prevent such situations, the institution must regularly verify that its standards are compliant with the law applicable to its business.

8 Risk management

The management body should be able to rely on an effective operational risk management system that covers all IT risks. In accordance with the law, this system must be based on a risk map and a regular risk assessment, and incorporate risk control and monitoring measures. These control measures should include internal controls at several independent levels to allow cross-checks. If the operational risk management system does not fully take IT risks into account, it will be incomplete and non-compliant with regulatory obligations. Moreover, it will not reflect all risks to which the institution is exposed, and the IT risk identification and control mechanisms will not be properly implemented. This may manifest itself as non-existent or partial mapping, an inadequate permanent control system, inadequate handling of incidents, or inadequate periodic controls.



Non-existent or partial risk mapping

Identifying and regularly assessing IT risks are prerequisites for adopting risk control measures. Otherwise, such measures may not be adopted or may be inappropriate, meaning institutions will be inadequately prepared and have a greater exposure to risk.

It is essential that the institution identifies and compiles a classification of its inherent and residual IT risks, both within business lines and support functions, including the IT department. This inventory should cover all physical assets (data centres, offices, agencies, etc.), logical assets (online or smartphone banking, cloud, etc.), activities (business lines and support functions), publics (employees, customers, service providers, partners) and tools (applications, networks, etc.), and should be consistent with the institution's risk appetite, as approved by the management body. It is important to include in this mapping the possible links with customers, providers and partners to take into account the contagion risks of a risk event. Mapping business processes and support functions is a prerequisite for identifying and updating these risks, and should be done at least annually. In addition to the mapping of processes and risks, which ideally should be computerised to facilitate its updating, consolidation and use, it is important to define risk reduction measures, whether organisational, technical or control-based. Furthermore, cross-disciplinary risks should be identified and included in the mapping for each activity. It is also essential to clearly define the responsibilities of the IT function and of other activities due to the fact that the business lines and support functions are exposed to certain IT risks that are managed by the IT function.

Failure in risk analysis

An analysis of IT risks, including security risks, should normally precede the adoption of new products, the undertaking of new businesses, any IT project, or the use of outsourced services. This is crucial to prevent the institution from engaging in an uncontrolled situation. This analysis contributes to the good information of senior management in order to inform their decision-making. Usually practiced on information systems security topics, risk analysis is intended to apply to all IT risk topics as recognised by the ACPR.

In addition to any analyses carried out the IT function, it is important that the risk management function formulates a prior opinion before the adoption, by users' businesses or by the IT function, of new products, projects or activities involving the information system. Acting in order to control IT risks, including those relating to the security of the information system, the risk management function delivers an independent opinion. It must have a sufficiently binding value to avoid the commitment in situations with a high level of risk for the institution, its customers or partners. An arbitration process by the management body should be able to be initiated in the event of a disagreement of the business or IT function on the opinion given by the control functions. The conditions laid down by these control functions shall be traced for monitoring and their removal shall take place through careful examination of the risk mitigation measures implemented.

Inadequate permanent control system

A permanent control system with two distinct levels of controls is necessary to avoid risk

situations. This permanent control system should encompass the various information system implementation and management processes to ensure that any failures are detected in a timely manner.

It is important that the permanent control of IT risks, including information security, be included in the institution's permanent control plan. This plan must cover all risks identified and be updated periodically. First-level controls should be performed by operational staff of the IT function constituting the "first line of defence". The level-2 controls should be performed by teams of the risk management function independent of the IT function, constituting the "second line of defence". The frequency of controls should be modulated depending on the risk level, but controls should be performed at least once a year. Action plans should be established to remedy any deficiencies discovered during the controls. A tool should catalogue the control plan and the results of controls as a means of informing the management body and facilitating their monitoring of controls.

Inadequate detection and management of operational risk incidents

Operational risk incidents should be monitored to measure an institution's losses and to take remedial measures. IT incidents are expected to be included in operational risk oversight if they meet the definition of operational risk.²⁵ If IT incidents, including security incidents, are not included in operational risk oversight, this risk will not be assessed completely, which could impact the quality of risk mitigation measures, and cause the

institution to hold insufficient capital to deal with such incidents.

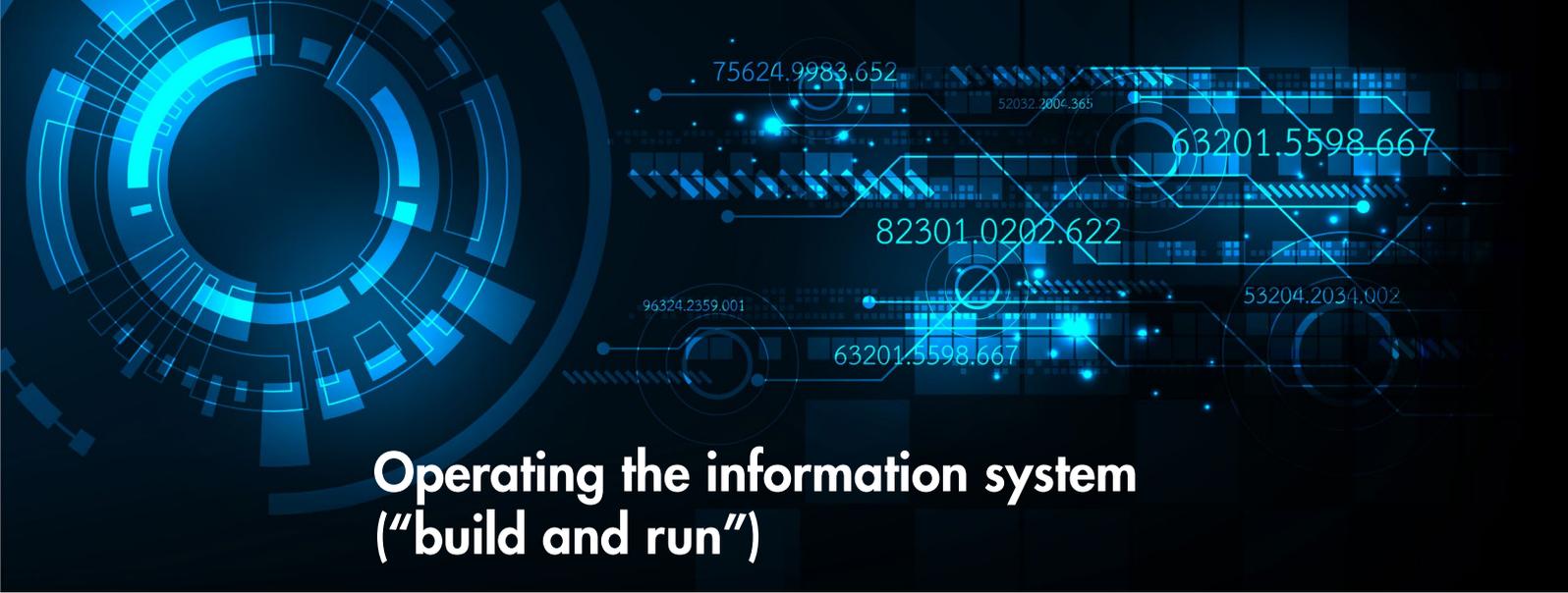
Therefore, it is expected that IT incidents that meet the criteria defined will be incorporated into the operational incidents database. If necessary, an incident reporting threshold can be established, but it should be set low enough to detect significant incidents. Aggregating multiple similar low-magnitude incidents is a good practice that enables detecting and correcting malfunctions before a major incident occurs. In addition, it is important that action plans be adopted in response to these incidents and that the management body be regularly informed about the most significant incidents and the associated action plans.

Inadequate periodic control system

The institution's periodic control system provides a third level of controls of all processes implemented. If it does not cover all information system processes, the management body may not be provided with independent information on the risk status and corrective measures taken in this area.

It is therefore essential that IT risks, including information security risks, be included in the institution's audit plan and that they be reviewed by specially trained auditors, either as part of general audits or pursuant to specific assignments. Furthermore, the findings should prompt recommendations and action plans, the most critical of which should be approved and monitored by the executive managers. The management body must receive sufficient, regularly updated information on the IT risks assessed by the periodic control system.

²⁵ Generating a financial gain or loss, whether or not realised (lost profits, near-miss), or a non-financial gain or loss (e.g. man-days devoted to re-establishing service after an IT breakdown).



Operating the information system ("build and run")

This section deals with risks related to the "information system operation" macro process, which includes all actions in relation to the use and operation of the existing system, as well as actions to develop new services or equipment (projects), or simply actions to make corrections or moderate changes (corrective and upgrade maintenance). The operational management of existing services is sometimes called "run" and the delivery of new services (application projects, installation of infrastructures) is sometimes called "change" or "build".

The aim of all of these actions is to ensure the proper operation of the information

system installed, i.e. providing the service expected by users, especially in terms of quality, reliability and availability. The same issues apply to "change" actions, where the risk is that they will be unable to properly provide the expected services. In recent years, particular attention has also been paid to data quality.

The following sections explain the primary and secondary risk factors that may disrupt operating processes, continuity management, change management, and data quality. The main measures for controlling these risks are also described.



OPERATING THE INFORMATION SYSTEM ("BUILD AND RUN")

Operations management
(systems and networks)

Continuity management

Change management
(projects, upgrades, fixes)

Data quality management

1 Operations management (systems and networks)

IT operations, also called “production”, consist of running the computers on which applications are installed. These computers, as well as their connecting equipments, are called systems and network environments. Improper operations management of these systems and networks may result in more or less serious disruptions that can impact the quality of service provided to users.

The ACPR’s IT experts have identified several risk factors that may lead to unsound operations management. These may include deficiencies in the means of production, in the process for detecting errors and anomalies, or in the process for resolving incidents and problems. This also includes the risk that service levels expected by users will not be met.

Inadequate means of production

The means of production provide the resources necessary for proper operation of the information system. If they are not properly resourced, for example with equipment that is sufficient in number and with adequate power, the information system may not be able to operate properly, in particular at peak times. Furthermore, if the configurations of this equipment are not up to date or are inappropriate for the institution’s needs, disruptions may occur or security may be impaired.

It is therefore important that the choice of equipment that will comprise the operating environment is properly assessed before new solutions are released. The technical characteristics, in particular the power of the equipment, must be appropriate to the operational needs imposed by the service levels expected by users. In addition, the capacity of resources

used must be monitored to allow sufficient time for expansion without compromising increased use of the information system (e.g. number of users able to connect to the system, computing power, storage space).

Sound management of the means of production requires up-to-date inventories. Inventory management consists of referencing and centralising all information system hardware and software, in order to have a complete picture and to be able to verify that the equipment installed is adequate for the needs identified. The characteristics of each piece of equipment should be recorded, such as version numbers, licences installed and the technical specificities of the various components. This will facilitate compliance with technical standards, and the obsolescence management of ageing components will be optimised.

Inadequate process for detecting errors and anomalies

Processing errors and anomalies disrupt proper operation of the information system by reducing availability (delays, interruptions) or data quality. Therefore, promptly detecting them is crucial.

Detection is one of the primary tasks of the operations staff who monitor production. They can increasingly rely on detection tools, listing for example anomalies already encountered, that automate monitoring. Specialised teams can also be tasked with these actions to improve response capacity. It is advisable to install error detection tools at various levels of the information system in order to identify various types of technical malfunctions, even before an incident occurs. For example, detecting abnormally long response times may enable anticipating an interruption of the information system. The

detection tools should cover all equipment to facilitate comprehensive oversight.

Inadequate management of incidents and problems

When detected, incidents²⁶ should be managed so as to restore proper operation of the information system as quickly as possible and minimise downtime. Problem²⁷ management, which complements incident management, consists of diagnosing the cause of repetitive or difficult to resolve incidents, putting in place measures to prevent them from reoccurring, and mitigating the impact of problems that cannot be avoided. Therefore, it is essential for these two processes to be effective in order to minimise service degradation and loss of user confidence.

It is advisable that these processes be formally expressed as operational procedures. The various incident and problem handling stages, from detection to resolution, should be performed by specialised teams, whose actions must be documented to ensure they are properly completed. Scaling based on sensitivity levels enables prioritising. Problem management is closely related to incident management, and uses similar tools, classification criteria and priorities. Resolution is generally easier if facilities, information flows and critical services have been mapped and inventoried. The resolution of incidents and problems should be monitored by the committees tasked with monitoring service quality. Succinct reports should be submitted to the management body to enable them to mobilise the appropriate teams and allocate sufficient resources.

Non-compliance with service levels

Service levels define users’ expectations with respect to the operation of the

information system (e.g. availability periods, possible interruption periods, data backup frequency, switchover to backup systems). Service levels are agreed for operating conditions and, more broadly, for overall performance of the service. Regardless of any incident, problem or improper hardware configuration, unsound operations management may make it impossible for the systems and network administrators to keep commitments to users.

Systems and network operating processes are ordinarily set out in formal operational procedures that enable their administrators to rigorously monitor the various operations in normal service and degraded service situations. In addition, it is important that service levels be formally set out in service agreements with end users. These agreements should specify the monitoring criteria and expected satisfaction levels for these services, with respect to service quality and availability. Documenting expected service levels in contracts is useful for measuring whether users’ needs have been met. Indicators should be used to monitor commitments and take necessary corrective actions.

2 IT continuity management

IT continuity refers to the measures and resources implemented to ensure the availability of the information system in accordance with the needs expressed by users in terms of “business continuity”. Services generally operate in accordance with availability periods that vary depending on the nature of the activities, except in certain cases where no interruption is tolerated. In any case, the systems and networks must be fully available during the availability periods to enable applications to function with adequate response times. Otherwise, the system will be

²⁶ The Information Technology Infrastructure Library (ITIL) defines an incident as “an unplanned interruption to an information technology (IT) service or reduction in quality of an IT service”.

²⁷ ITIL defines a problem as the cause of an incident.

unavailable or experience slowdowns, thereby disrupting user activity.

The information system may risk unavailability if the institution does not have an adequate organisation in place to manage its service continuity system, or if it has not correctly identified the various unavailability scenarios, or if the means of production or backup systems are inadequately protected against accidents, or if its IT continuity system is inadequate, does not correspond to the system planned for users, or has not been tested sufficiently.

Inadequate continuity organisation

Institutions must set up an organisation to manage their service continuity framework, in accordance with regulatory requirements. This framework is twofold with a component specific to the continuity of users’ activities (fall back premises) and an IT backup component (switchover to a backup site). This system should describe the actions to be taken to ensure the continuity of the business processes deemed essential, and the necessary resources to be implemented in the event of a crisis. This reduces the risk of business interruption or information system malfunctions to an acceptable level for the institution. If the organisation set up is inadequate, the institution may not have available backup resources in the event of a failure of its main equipment.

It is therefore important that the organisation set up to manage business continuity be based on formal coordination, supervision and decision-making policies and procedures. This requires that the roles and responsibilities in crisis management situations be clearly defined. The involvement and approval of the management body is

necessary to ensure that the continuity system is aligned with the institution’s strategy, that sufficient budgetary and human resources are allocated, and that employees and their managers are committed to the process. Ordinarily, a methodology, an effective crisis management structure and an appropriate communication policy complete the system. The institution should have a business continuity plan that includes an IT backup plan.

Inadequate identification of unavailability scenarios

The continuity plans are customarily based on loss of assets scenarios, including systems and networks malfunctions of varying durations. The IT backup plan should describe the procedures for activating backup resources under these various scenarios. If the scenarios defined do not identify all possible disturbances or miscalculate the consequences, the continuity management system may not adequately respond to an unforeseen breakdown, which will prevent users from continuing their activities.

To prevent such situations, it is necessary to perform impact assessments for users’ businesses (in particular, at the regulatory, legal, commercial, financial and reputational levels) based on the various scenarios of unavailability of premises, information systems, staff, energy, telecommunications and key vendors. These impact assessments allow the definition of the “maximum tolerable period of disruption” (MTPD) and the “maximum allowable data loss” (MADT). On this basis, objectives are set to production teams in terms of maximum recovery time (“recovery time objective” – RTO) and the maximum allowable period between an incident and the date of the most recent data backup (“recovery point objective” – RPO).

Non-alignment of IT continuity with business continuity

The IT backup plan describes the continuity arrangements for IT production. It should be part of the institution’s overall business continuity plan, which also describes the backup resources available to users. The IT backup plan must therefore be consistent with the business continuity plan; otherwise, there is a risk that it will be inadequate to enable continuity of essential or critical applications.

To avoid any discrepancy resulting in inadequate IT backup resources, the IT backup plan must be based on impact assessments for users’ businesses and their corresponding service recovery times (expressed as RTO and RPO). Any discrepancies that may result from a known deficiency of backup resources must be brought to the attention of the management body for a decision on user needs or the allocation of additional resources.

Inadequate protection of means of production and backup resources against accidents

Data centres are particularly vulnerable to accidents and damage that may affect hardware and thus disrupt the proper operation of the information system. These sites are dependent on electricity to power equipment and water for air conditioning. A wide variety of accidents and natural disasters may severely impact them (fires, floods, earthquakes, plane crashes, chemical pollution, electromagnetic pollution, etc.).

It is therefore important for institutions to rigorously select the locations for their data centres, avoiding areas exposed to natural

hazards (e.g. flooding or seismic areas) or neighbouring risks (airports, chemical sites, etc.). They should also equip their data centres with devices to detect accidents and minimise potential damage, in particular fire (detection, extinction) and water leaks from the air conditioning system. These devices must be properly resourced, regularly tested and kept in good working order. These protective devices are not only necessary on the premises housing the hardware, but also in the rooms housing electrical equipment and telecommunication servers. It is also advisable to develop a comprehensive safety policy, for example, prohibiting the storage of flammable materials, such as cardboard, in machinery rooms or nearby premises.

Inadequate continuity systems

In accordance with the IT backup plan, the institution must be able to switch operation of its information system over to a backup infrastructure if its main system becomes unavailable. If it has poorly resourced its backup equipment, it may not be able to run the applications it needs. If its backups are not recent enough, it may lose significant quantities of important data.

Therefore, the backup infrastructure equipment must be properly resourced to be able to run the applications and functionalities identified as essential and critical in the continuity plan. These infrastructures must be operational in order to quickly switch production over to them in accordance with users’ requirements (RTO and RPO). Data backups must be sufficiently frequent and well-protected. Switchovers may be triggered for the entire information system, or for certain components or applications. If the operation is spread over at least two sites operating on a

load-shared basis ("active-active" mode), it is important that each site can support the total operating load in the event of the unavailability of one or more sites. In addition, the possibility of regional disasters must be taken into account, in particular by locating the production environment sufficiently far away from the backup environment. Moreover, it is particularly important that the backup site have a power supply from a different power generation source than that supplying the main site, and that it not be exposed to the same natural hazards as the main site (river flooding, proximity to the same airport or industrial or chemical site, etc.). If this is the case, a third site will be needed in order to actually retain production capacity in all unavailability scenarios.

Inadequate testing

The effectiveness and pertinence of business continuity plans and IT backup plans depend on sufficiently regular implementation testing. The testing of technical and organisational systems makes it possible to assess the robustness of the planned solutions, in accordance with the service levels approved by users.

It is important for continuity plans to be tested comprehensively using a proven methodology, so as to obtain reasonable assurance of the plans' quality and effectiveness, including compliance with user requirements. Backup tests are truly pertinent only if they include a switchover of production from the main environment to the backup environment. Therefore, the backup environment should be used in actual situations by the business line teams for a sufficiently long period of time and on a range of matters that is representative of their critical activities (in particular, to enable

conducting end-of-period work, such as at the end of a week or month). Backup environments should allow alternate production on at least one of the backup sites. The results should be monitored at the appropriate level and necessary corrective measures should be taken.

3 Change management (projects, upgrades, fixes)

IT "change" (a.k.a. "build") refer to all modifications made to a system, either to fix it or upgrade it (maintenance), or to change or supplement it (project). Changes may concern software and hardware. These are obviously delicate processes because they are carried out on existing production. Mismanaged changes will cause malfunctions. In this area, the risk factors to be considered are inappropriate change management standards, poorly organized or incompetently managed changes or projects, functional and technical requirements not adequately taken into account, insufficient testing of new components, and improperly implemented changes.

Inadequately defined or applied change management standards

Because it is a tricky process, change management is usually governed by operational policies and procedures. Such policies provide, for example, that releases should be grouped in batches rather than implemented individually. A release for which proper guidelines have not been adopted has greater exposure to the risk of erroneous operations.

Therefore, complete and appropriate policies and procedures are recommended. They should be implemented by specialised teams

trained for this purpose within the entities. The different types of changes should be defined, including standard changes and urgent changes to correct serious malfunctions. The description of treatments should distinguish the various phases, including recording, impact assessment, classification, prioritisation, validation stages, planning, testing and regression conditions. Management of versions (releases) should also be included in these processes.

Poor project management organisation

Successful change management, and especially project management, depends to a large extent on setting up a solid organisation and on the expertise of the teams in charge. Applying a work methodology also helps to guide the process. Failure to control the work can cause delays and generate additional costs, or may result in a deterioration in expected functionalities.

In particular, the roles and responsibilities of each participant should be clearly defined in order to ensure a solid organisation. Committees that monitor the work and coordinate the various parties can provide oversight of deadlines, costs and quality, and facilitate decision-making. Major projects should be monitored by a sponsor responsible for ensuring they progress smoothly. A communication system for the various parties involved will reduce misunderstandings that can be a source of errors or delays. Applying a project management methodology is advisable because it ensures proper sequencing of the various performance stages after the quality of deliverables has been verified. Finally, the choice of staff is crucial, and it is necessary to verify that they have the expertise required to perform the various tasks.

Functional and technical requirements not adequately taken into account

Applications and software have to respond to users' needs. These have therefore to be formally expressed to be correctly taken into account. In addition, technical standards will also impose technical requirements with respect to security, production and network operation. It is also possible that users and IT developers work together in a close and interactive way to adequately capture needs (ex: "agile" development method). This also applies to IT developments that could be managed by the users ("shadow IT"), especially when they are used to produce important management information.

A methodology shared by all stakeholders should be followed to collect and approve the users' functional requirements. Technical requirements that restrict the possibility of meeting functional needs must be made known to and be accepted by users. Technical requirements specific to the operation of the systems and networks must be taken into account by the technical administrators at the earliest stages in the design and development of new equipment.

Failure in software

Of course, the software used by the institution should not suffer from operational flaws that would undermine the reliability of the information produced, or would slow down and complicate the process management. This is also applicable to applications specifically developed for the institution and to market software. This also applies to IT developments that could be carried out by the users ("shadow IT"), especially when they are used to produce important management information.

Functional and technical acceptances verify that applications and software are adequate. It is important that they be comprehensive and formalised, as well as the results thereof are documented in reports shared with all stakeholders. Corrective actions should be taken if significant anomalies are discovered. Minor anomalies can be considered non-fatal for commissioning and be fixed later.

Inadequate testing

Testing is a mechanism for ensuring that changes meet the needs approved, both functionally and technically.

Non-regression testing should be performed systematically in case of changes to avoid unwanted side effects. A pre-production environment as similar as possible to the production environment will enable verifying the adequacy of new components (functionalities, performance).

Improperly implemented changes

Releasing changes is particularly delicate because if it not correctly carried out, it can create disruptions to the system in place, with potentially very damaging consequences if rollback is difficult.

It is therefore important to follow a very rigorous release process. Planned software and hardware deployments should follow formal procedures that aim to ensure a satisfactory level of availability. These procedures should include rollback methods in the event of a defect. Customarily, a change timetable is adopted in order to group changes and implement them at times when experienced staff are present and outside normal service periods (e.g. on weekends).

If necessary, qualified experts should be on call and managers should be reachable in the event of an anomaly.

4 Data quality

One of the most important requirements for an information system is that its data be accurate, i.e. it corresponds to the data inputs expected and/or changes thereto as a result of processing performed by the information system do not generate errors. This is particularly important for the information systems of banking and insurance institutions, which hold personal data and financial assets. This requirement is also important for risk calculation data, which is used by the management body to manage the business and by supervisors to supervise it. Therefore, poor quality data can be particularly detrimental, both for conducting business if the institution does not use reliable data, and for monitoring risks if the indicators used are erroneous. Data may be of poor quality if data standardisation and definitions are inadequate, or if the information system uses or generates erroneous data. Inadequate controls may also explain a data quality problem.

Inadequate data standardisation

The information systems of banks and insurance institutions often comprise multiple applications. If they were designed at different times and for new needs on each occasion, the concepts they use (e.g. “borrower”, “insured”) may not always be defined in the same way, making it difficult to compare or aggregate data. Ordinarily, the most commonly used terms should be managed by establishing unique “glossaries”, which are to be used throughout the institution. Similarly, data “standardisation” means homogenising, and unifying if possible, the definitions of

similar concepts used throughout the information system. If the institution does not use glossaries for its most commonly shared data, or if it has not undertaken a standardisation process, the various components of its information system may use non-comparable data or data that cannot be aggregated, thereby depriving it of a consolidated picture of its business and risks.

For this reason, glossaries should be created for the concepts most commonly used by the institution. The various applications using this data will thus have a single and reliable source. A function or business line should be given responsibility for these glossaries and tasked with updating them and ensuring the data definitions are pertinent. Similarly, to increase uniformity among the various applications that use similar data, and thereby facilitate data aggregation, it is in the institution's interest to undertake a data standardisation process. This process should involve business lines and functions, as owners of the information system, as well as the IT function, which is responsible for the consistency of the information system as a whole. This standardisation process can usefully be supported by data dictionaries that set out data definitions and syntax, and that apply to all user entities.

The information system uses or generates erroneous data

If the information system uses inaccurate input data, it is likely that it will generate inaccurate output data. Moreover, regardless of the quality of the source data, if there are processing errors in the system, the data generated will be erroneous. Data errors

are not due solely to accuracy issues; they may also be the result of inappropriate or incomplete data, or data that is unavailable at the time of processing. The risk of errors also increases if an automated process is reprocessed manually.

Users should test data suitability before it is released and, thereafter, should check it regularly. Audit trails will enable reconstruction of processing and the steps taken to make changes, thereby providing a history of changes made to information from its original form to its final form. Manual treatments should be limited as much as possible and should be thoroughly and regularly verified. Production incidents should be analysed to assess their impact on the quality of the data generated. Risk indicators produced for the management body and supervisors should be based, to the extent possible, on automatically calculated indicators rather than approximate values. Lastly, it is important that the available data be sufficiently detailed and aggregated in accordance with the criteria requested, in order to meet all significant users' needs.

Inadequate data quality controls

Data quality must be regularly and thoroughly checked by users and control functions. Otherwise, the institution may not detect situations in which erroneous data is used or generated.

Therefore, the verification of data generated throughout their life cycle and risk monitoring reports should be based on automated and manual controls that enable detecting any anomalies and setting up action plans to fix them.

Securing the information system

This section discusses the risks that may affect the “information system security” macro process, which includes the various prevention and response actions that may be taken to thwart security breaches. Customarily, these breaches are described in terms of their impact on the availability, integrity, confidentiality, and evidence or traceability of data and operations.

The issue of information system security has become increasingly important due to cyber threats, but is in fact not a new concern. Originally, it encompassed both accidents (breakdowns, natural disasters) and malicious threats. Today, accidental threats are more commonly dealt with under the “information system operation” macro process, as was done above, and the “information system security” macro process focuses on preventing and responding to malicious

attacks, including when they take advantage of negligence.

Security-related recommendations should not be read in isolation from those set out above regarding organisation and governance.

The sections below describe the main risk factors that can impact the security of the information system as a whole (production, development, test and back-up) and, for each one, will suggest risk reduction measures that can be implemented. The risk factors discussed are due to inadequate physical protection of facilities that enable intrusions, inadequate identification of IT assets (i.e. the various assets that comprise the information system, such as hardware, software and data), inadequate protection of these assets, inadequate detection of attacks, and inadequate response to attacks.



SECURING THE INFORMATION SYSTEM

Physical protection of facilities

Identification of assets

Logical protection of assets

Detection of attacks

Response to attacks

1 Physical protection of facilities

The protection of buildings against malicious intrusion has become increasingly important in recent years to deal with new types of attacks, whether violent or surreptitious. An intrusion onto the premises can result in the theft and destruction of physical assets, and may facilitate a logical intrusion into the information system if malware is installed that can spy on, sabotage or replace the information of the institution, its customers or its partners. Such intrusions are possible if the measures taken to protect buildings or access to IT equipment are inadequate.

Inadequate protection against intrusion into buildings

Protective measures are crucial for premises in which systems and network infrastructures are housed (data centres). They may also be necessary for commercial or administrative premises which, although not as critical, nevertheless contain the institution's workstations, network accesses and documentation.

It is advisable not to identify data centres with signs that describe the use and ownership of the premises. Access thereto should be restricted to a small group of persons in order to reduce risks. Strict procedures should regulate access to facilities, including for service providers appointed to maintain equipment. These procedures should grant access only to persons who have been properly scheduled, identified and accredited. In general, premises should be protected by perimeter security barriers (fences, gates, security doors, badge controls, etc.) and intrusion detection systems (video surveillance, alarms, etc.). This equipment must be regularly tested and maintained in

good working order. Access control measures differentiated by zone should supplement the security system within the premises by restricting access to various areas according to the recognised need of staff, called "need to know". The security systems should be synchronised to enable correlating events. The event logs of the various components of the security system should be kept for the time periods required to complete all necessary investigations.

Inadequate protection of IT equipment

Hardware safeguards should complement anti-intrusion systems. Critical physical assets, such as servers, administration consoles, network hardware, electrical equipment, keys, etc., require enhanced protection using additional and specific security devices (e.g. cages around servers, locked bays, and specific video surveillance).

2 Identification of assets

An inadequate inventory of IT assets may be detrimental to information system security management because homogeneous and appropriate security measures may not be taken pre-emptively or the response to an attack may be deficient. The relevant risk factors are an incomplete inventory or classification of assets.

Incomplete asset inventory

An inventory of IT assets is necessary to identify the most critical assets for users and the assets that are most exposed to cyber-attacks. This inventory should include "business line" assets (e.g. applications, data) and "support" assets (e.g. premises, hardware), and should be kept up to date.

It should include all information necessary to identify assets, and should describe the location, function and ownership of each asset. The inventory should also associate interrelated assets to make it possible to quickly identify interactions and interdependencies, which would be useful for crisis management purposes.

Incomplete asset classification

Classification consists of defining the level of sensitivity of assets, which is used to determine the protective measures to be implemented and to quickly identify the assets to be isolated and safeguarded in the event of an attack. The primary focus of this classification should be data and their associated applications. The classification serves as the basis for assigning sensitivity levels to the systems and network equipment used for these applications, as well as to the sites where such equipment is installed, thereby providing a global picture, both logically and physically, enabling the institution to prioritise the protection of assets.

For the classification to be complete and pertinent, it must include all logical assets as well as all physical assets supporting them. It should result from a formal analysis process approved by the owners of the relevant assets, and be reviewed periodically. The asset classification is made according to their sensitivity regarding criteria of availability, integrity, confidentiality, traceability and legal or regulatory obligations. Financial and reputational impacts may also help to this assessment.

3 Logical protection of assets

Asset security relies primarily on a set of IT protection measures (“logical” measures)

intended to prevent any breach of the information system. Cyber-attackers have varied motives, such as realising a direct gain (fraud, theft, ransom, espionage) or causing harm (disrupting normal operations, sabotage, reputational damage). Regardless of the motives, these attacks may impact the system’s availability (e.g. blocking a system), integrity (manipulation of an asset), confidentiality (e.g. viewing or stealing data) or traceability (e.g. deleting access rights changes). Protective measures must therefore cover these various types of disruptions and be adapted to the sensitivity of each asset. These measures can no longer be designed individually. Current best practice is to replicate them at the various levels of the information system (e.g. by filtering communications not only upon entry but also at other points in the system) in order to slow the progress of an attacker. This is known as the “defence-in-depth” concept. If the logical protection of assets is inadequate, there is a risk that an attacker may enter the information system and compromise it. This may be due to inadequate perimeter security systems, inadequate protection against malware, inadequate identity and access rights management, inadequate employee authentication, inadequate protection of systems and data integrity and confidentiality, inadequate protection of systems and data availability, inadequate management of security patches, inadequate security reviews, inadequately secured outsourced solutions, or inadequate information systems security awareness.

Inadequate perimeter security systems

Perimeter security consists of protecting the information system from external intrusion or of isolating internal zones. Due to the significant number of communications with external parties, perimeter security includes

channelling communication flows to a limited number of obligatory passage points, then filtering and reviewing the content of incoming and outgoing communications. In recent years, this protection has been criticised on the grounds that it has become nearly impossible to implement due to the multiplicity of communication channels and flows. Nevertheless, perimeter security continues to be a key tool for effectively protecting the information system, although it should be supplemented by other measures, including detection measures within the system.

It is therefore expected that systems providing perimeter security for the information system will be set up to prevent any unauthorised attempt to access the information system, or at least the applications and data identified as sensitive. Devices for filtering network traffic (e.g. firewalls), comprising monitoring and blocking rules, should be deployed, and the most sensitive assets should be logically isolated within the information system or cut off therefrom. The effectiveness of perimeter security systems should be regularly reassessed and such systems should be adapted as necessary.

Inadequate protection against malware

Malware is the most frequent vector for cyber-attacks. It can be used to collect information that may facilitate future intrusion (technical, organisational or procedural information), compromise the integrity of systems or data (website defacement, data encryption followed by a ransom request), disrupt the availability of applications (sabotage) or, more directly, may be used to steal confidential information (espionage). If an institution does not install safeguards against malware, the security of its information system may be severely compromised.

It is therefore important to deploy anti-malware devices on all hardware and software: messaging gateways (scanning attachments, detecting executable files), Internet access gateways, network access points for partners, etc. These devices must be activated and kept up to date. Any exceptions must follow formal guidelines and be approved. Protective devices must themselves be protected against any attempt by users to disable or uninstall them. The use of several separate security suites within the information system prevents the exploitation of a weakness or vulnerability of a particular tool.

Inadequate identity and access rights management

Access rights to the information system should normally be granted to users on a “need-to-know” basis. They protect legitimate use of the system and are components of user identification management. Access rights should be granted by the institution on the basis of its employees’ status and duties. Therefore, access rights should be updated whenever employees are hired, leave or change position. Similar principles should apply to information system components managed by external providers. If this is not done, or if the rights granted are too broad or incorrectly updated, attackers may be able to more easily spoof them and hack into the information system.

To enable all actions on the information system to be attributed to a given person, internal and external staff must be identified by name or unique identifier. The use of generic accounts to access servers, applications and data must be restricted and formally supervised. Employees with privileged accounts (e.g. administrators) should

also have regular accounts to perform everyday tasks (access to corporate e-mail, web browsing, etc.). Effective access rights management requires the use of profiles (business line and technical profiles) to standardise and facilitate the granting of individual rights. Any additional individual access rights, inconsistent with the user's profile, must be justified, formally granted and approved. In general, access rights to an asset should be approved by the owner of that asset, either directly or by a delegate. It is important that access rights be consistent at all times with the positions users hold. In particular, accreditations granted should be promptly deleted when an employee is transferred or leaves the company. Best practice in this area is to synchronise access rights management systems with human resource management systems (or service contracts if applicable). Rights granted should be reviewed regularly to ensure they continue to be justified. The frequency of these reviews is adapted to the sensitivity of rights granted. Similarly, the definition of profiles should be reviewed periodically to determine if they remain pertinent.

Inadequate employee authentication systems

Authentication consists of providing proof of identity, for example to access a piece of hardware or an application. In computing, the most common tool is a password but it must be sufficiently secure to prevent spoofing.

It is therefore important to set up authentication systems adapted to the sensitivity of the assets to be accessed. Dual factor and/or dynamic authentication means should be implemented for access to the most critical assets. If necessary, the rules governing the

complexity of confidential authentication means chosen by employees should be standardised and adapted to their duties. Compliance with these rules should be regularly monitored. Granting temporary authentication credentials should be closely supervised and secured (e.g. password changed at the time of the first connection). If static, authentication credentials (passwords, tokens, etc.) must be renewed periodically. Any off-site access to the information system should require enhanced authentication procedures (for employees and external service providers). Authentication secret elements need to be appropriately protected.

Inadequate protection of the integrity of systems and data

System and data integrity safeguards are needed to prevent attackers from making changes to information system components that may affect its proper operation (including its reliability) or security. Such actions may include changes to the system's configurations or access rights in order to carry out an attack, or altering data for the benefit of the attacker, or an encryption with the view of asking a ransom.

To enhance the security of systems and to enable detection of any configuration change, whether by adding a programme or changing the parameters of systems or applications, best practice dictates strictly limiting the right to run software on equipment (servers and workstations) and fingerprinting the servers' "key" files. Another way to reduce the risk of compromising hardware is to reduce to a bare minimum the software installed thereon and its features. This technique, called "hardening", mechanically reduces the number of software vulnerabilities that could be exploited

by an attacker. Data and their associated applications can be protected against attempted alteration in several different ways. It is advisable for applications to be designed securely by including automatic controls for creating, modifying, and deleting sensitive data. Moreover, applications can be configured to require dual validation (“four eyes” principle) for important operations (e.g. approving a payment). When data is transported and stored, its integrity can be protected by “sealing” tools and applications that can be used to verify that data has not been altered. Usually, the seal is calculated by a function called “hashing”, possibly after adding a “salt”, to prevent “dictionary” attacks (“rainbow tables”). However, to be fully effective and secure, these tools should comply with the current recommendations of the *Agence Nationale pour la Sécurité des Systèmes d’Information* (“ANSSI” – National Information Systems Security Agency).²⁸ Lastly, and specifically for web services offered by institutions, protections can be applied to websites against the risk of website defacement.

Inadequate protection of the confidentiality of data

Measures to protect the confidentiality of data, whether in relation to applications (e.g. customer databases) or hardware (e.g. configuration data), aim to prevent unauthorised access (reading) or theft (copying). In either case, the legal (breach of regulatory obligations), financial (compensation for losses, sanctions) and reputational consequences may be disastrous for an institution.

To prevent data disclosures or theft, production data should be protected and the transfer thereof to other environments should be

restricted. Production environments should be logically segregated or isolated from other environments to reduce uncontrolled access from a development or testing environment that is typically less secure. Furthermore, the data accessible from testing or development environments can be anonymised; better yet, such data could be entirely fictitious to avoid the risk of disclosing real data. To reduce the risk that data may be accessed by unauthorised third parties, the right to view or manipulate production data must be supervised and access records kept. This measure particularly applies to service providers such as web hosts, managed service providers and software solution publishers, which may have extensive rights over production environments without the institution knowing precisely who has access to its data. In addition, the most sensitive data should be protected throughout its life cycle: when it is input and displayed (e.g. partially or totally hidden), as well as during storage and transport (encryption). It may also be advisable to encrypt network communications end-to-end, i.e. both on public networks and internal networks (between applications). In all cases, to be fully effective and secure, these cryptographic tools should also comply with the current recommendations of the ANSSI.

The hardware that hosts data or allows access to data must also be protected. This is particularly true for mobile devices (phones, laptops, tablets), to which specific measures can be applied to prevent unauthorised access to the device or its contents, such as the encryption of internal storage media or, if possible, requiring a password to start the equipment. More generally, it is good practice to have procedures for disposing of equipment at the end of their life cycle that logically and/or physically destroy any information

²⁸ See Annex B1 of the ANSSI's General Security Guidelines (<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>).

in memory. Lastly, at the application level, for publicly available applications (Internet applications and services, mobile applications, etc.) the institution should take measures to prevent any attempt at reverse engineering. This practice seeks to recover the source code of software in a usable form for the purpose of counterfeiting it (intellectual property infringement) or understanding its operation (e.g. to attack it).

Inadequate availability safeguards

External attacks can make the information system unavailable, either by completely preventing access or simply by slowing it down. Such cyber-attacks, called denial-of-service (DoS) attacks,²⁹ which saturate external accesses to a system, have become frequent in recent years. These attacks cause immediate disruption to users, and can damage the reputation of institutions in the banking and insurance sectors.

The protection of the information system from attacks against its availability should rely primarily on the same continuity management systems as those discussed in connection with the proper operation of the information system. To prevent DDoS attacks, the institution can use filtering solutions to recognise legitimate requests. If a website for customers is attacked, it may be beneficial to be able to activate a separate site that is a copy of the first site or that is used solely to post information, and which is accessible at a different address than the site under attack.

Inadequate management of security patches

Cyber-attacks often exploit security vulnerabilities in software or hardware. Publishers

usually update their IT solutions very quickly when security breaches are discovered. If an institution does not quickly change the versions it uses to take advantage of security patches, it will be exposed to attacks. This task is facilitated if the institution has an up-to-date asset inventory.

Protecting the information system against logical attacks requires promptly updating security patches for all relevant assets. A monitoring procedure should be set up to detect any vulnerabilities of the information system and provide fixes as quickly as possible. The configuration information available in the asset inventory can be used to verify the extent of vulnerabilities and establish an update plan. This plan should take into account the sensitivity level of the assets. To avoid creating new vulnerabilities, new hardware installed should have editors' support and up-to-date versions of security patches.

Inadequate security reviews

Security reviews refer to measures that test the effectiveness of defences implemented ("intrusion tests") or check for vulnerabilities by observing hardware and software configurations ("vulnerability scans" and "code reviews"). Institutions are increasingly using these techniques to supplement their protective measures. This enables testing the chances that an attacker may be able to circumvent defences. Without such reviews, the institution may incorrectly conclude that the measures it has implemented are adequate.

Therefore, it is recommended that regular security reviews be conducted to verify that the IT assets have no weaknesses that can be exploited. This should include periodic vulnerability scanning campaigns of

²⁹ If the attacker uses a large number of devices to attempt to connect to the system, the attack is called a distributed denial-of-service (DDoS) attack.

equipment connected to the Internet, which is by definition more exposed, but also of internal equipment (servers). Targeted intrusion tests should supplement vulnerability scanning to test the security of newly installed or upgraded hardware and applications. To obtain objective and reliable results, these campaigns should be conducted by external experts or independent third parties, using a variety of approaches and methodologies. Lastly, security-focused code audits should be conducted to identify and fix any potential vulnerability as quickly as possible.

Inadequate security of outsourced solutions

It is common that service providers manage part or all of the information system on behalf of institutions. These service providers may belong to the same group as the institution or may not be affiliated with it. In either case, service providers act in the name and on behalf of the institution, and the institution remains responsible for the management of its information system, including its security.

Therefore, protecting the security of the information system requires that the portions outsourced be protected to the same extent as the rest of the system. For this purpose, before any outsourcing, the institution must conduct a risk analysis to which the control functions, in particular the information security function need to contribute. The management body will decide on outsourcing projects taking into account security conditions. The risk analysis should identify the relevant activities that are sensitive in nature, and ensure that the service provider has solutions that guarantee data confidentiality (e.g. by using encryption) and backup capabilities. After the outsourced services have

been set up, they must meet the same security requirements as if they were performed by the institution itself. The outsourcing contract should specify that the security conditions applied by the service provider must comply with the institution's security policies. The institution must monitor the performance of outsourced services over time, including any incidents. The institution must have audit rights that are not unduly limited by restrictive clauses (long notice periods). With respect to outsourced cloud computing services, the ACPR published a number of data and systems security best practices in July 2013,³⁰ with which institutions are expected to comply, as well as with the EBA recommendations issued in December 2017.³¹

Inadequate information systems security awareness

Raising the awareness of staff and management about the security of information systems is a prerequisite to creating a risk culture on these issues. Such culture can be useful in thwarting malicious attacks, which often target employees and managers, and seek to manipulate them in order to hack into the system (e.g. infected USB sticks or email messages) or to carry out a fraud (social engineering). It also aims at reducing the risk of negligence from these users, which could enable a malicious action of a third party to be realised.

Awareness-raising actions are advisable to prevent such actions. They should supplement existing procedures by providing information about risks and providing training in best practices with respect to the use and protection of the information system. Specific training programmes for employees with high privileges (administrators) or who

30 ACPR (2013): "The risks associated with cloud computing", July. <https://acpr.banque-france.fr/search-es?term=201307+Risques+associes+au+Cloud+computing>

31 <https://www.eba.europa.eu/documents/10180/1712868/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf>

perform sensitive functions (developers) should also be scheduled regularly. To the extent possible, awareness-raising actions should be extended to external staff, partners and customers. The effectiveness of each action conducted should be evaluated, and adjustments should be made if necessary.

4 Detection of attacks

Security can no longer be based solely on protective measures. The occurrence of “silent”³² cyber-attacks demonstrates the ability of attackers to intrude into an information system without being detected, in order to understand how it is organised and cause serious harm. Therefore, protective measures may not be sufficient and must be coupled with detection measures. These detection efforts usually focus on two areas. The first is collecting and analysing events (“traces”) recorded by the hardware, and the second is recognising unusual behaviour of users. If such detection tools are not used, or if they are incomplete, the institution may be unable to detect or block intrusions into its information system.

Inadequate trace collection and analysis

There are tools³³ available for collecting, centralising and correlating events (“traces”) recorded by the various types of information system hardware (e.g. firewalls, network routers, detection probes, as well as the production systems), which can be used to monitor this equipment. This monitoring may enable detecting intrusions or attempted intrusions into the information system and thus providing prompt alerts.

Best practices, especially for cybersecurity purposes, now require automatic tools for collecting and analysing traces, as well as

a monitoring team that can take action based thereon (such as a Security Operating Centre -SOC), which ideally should be operational 24/7. These SIEM tools should cover the entire information system, or at least its components that interface with the Internet and its components classified as sensitive. Traces collected should be time-stamped, archived, and protected against any attempted change. The most serious alerts should be handled by the monitoring team, which should stay constantly informed of new attack procedures or vulnerabilities exploited.³⁴ The organisation in place should enable information to be shared about incidents detected by the various internal units. Exchanges with peer institutions and the authorities should also be conducted.

Inadequate monitoring of unusual behaviour of users

External users (e.g. customers connecting online) and internal users (employees performing operations, IT staff) use the functionalities of the information system intended for their use. Malicious acts by them, or by attackers who usurp their rights, will result in an abnormal use of these functionalities. If mechanisms for monitoring abnormal behaviour of users are not put in place, the institution’s information system risks being hacked without its knowledge.

Best practice is to monitor suspicious actions in applications, administrative tools, databases or any other sensitive environment within the organisation. This monitoring should be done in real time to enable greater responsiveness to attacks. Unusual connections to the information system should be monitored (connections at unusual times or dates like holidays, numerous connections, access from new

32 Such attack do not provoke immediate disruption, but aim to gain progressively access to the different elements of the information system, in order to maximize the attack.

33 E.g. security incident event management (SIEM) tools.

34 This function may be performed by the SOC.

machines or Internet addresses, etc.). Anomalies during the authentication of external users (customers, service providers) and internal users should be recorded and analysed (e.g. multiple attempts). Unusual behaviour of customers who use transactional sites (e.g. online account management) should be detected. High-value disbursement transactions should be monitored and blocking mechanisms may be activated to prevent numerous or high-value outflows. Copying and mass delete functions on sensitive databases should be monitored or blocked, as well as privilege escalation functions on systems and databases.

5 Response to attacks

As provided in the cybersecurity management principles, the security of information systems requires, in addition to protection and detection measures, also setting up an attack response and information system security recovery approach. Several steps are required, starting with containing the system components affected, eliminating malware, returning to service in degraded mode and, finally, rebuilding a healthy and fully functioning information system. These various operations require a crisis management organisation, which of course should be set up in advance. Therefore, the risk factors that may prevent an appropriate response to attacks are related to failures in these various processes, whether crisis management, or containing attacks, or resuming operations.

Deficiencies in crisis management

The crisis management organisation should be based on procedures that indicate, depending on the various scenarios impacting the proper functioning of the institution, the

operating methods to be implemented to mitigate impacts and resume operations. The roles and responsibilities of decision-makers and key employees should be specified, and they must be provided with the resources (premises, equipment, communications or service providers) to meet and direct the operations. This type of organisation is required for banking and insurance institutions, in particular for dealing with a loss of resources (buildings, employees, IT systems). If the crisis management organisation does not cover the various information system security breach scenarios, institutions may not be able to manage them effectively.

Therefore, it is important that crisis management procedures adapted to cyber risk be adopted and be regularly tested and adjusted. These procedures should cover the various cyber-attack scenarios and their consequences in terms of availability, confidentiality, integrity and traceability. They should provide for coordinated action with external stakeholders (partners, customers) and, if necessary, the competent authorities. They should include communication measures (media, partners, customers) and information measures (the management body, supervisors).

Deficiencies in containment of attacks

Containing an attack consists in stopping the attack from spreading, including to third parties, then eliminating the attack vectors, such as malware, used by the attacker. This is a prerequisite to resuming operations and preventing the attack from spreading uncontrollably.

Dedicated operational teams, such as a Computer Security Incident Response Team (CSIRT) should be responsible for incident

response. These teams should be tasked with stopping attacks and eliminating the effects thereof. They should have the expertise and authority to determine what applications to shut down and what networks to disconnect, if necessary. Whenever required, these teams should be able to draw on additional external expertise, for which contracts have been entered into. Ideally, these teams should be able to set up decoys to distract or weaken the attacker during information system security operations.

Inadequate business recovery

Restoring the information system consists of putting it back into service. Generally, this

is a gradual process. If necessary, during the attack, operations may also be performed via degraded manual procedures, i.e. without using IT tools. When the attack vectors have been eliminated, a partial recovery of the information system is possible, using the components not impacted. Thereafter, the integrity of the system will have to be re-established to enable full and normal operation of the information system.

Restoring an information system impacted by an attack requires procedures established in advance, that are regularly tested and reviewed. These procedures should prioritise recovery actions and ensure the integrity of restored systems and data.

Appendix: Classification of IT risk

Macro process	Primary IT risk factors	Secondary IT risk factors
Organising the IS (including the ISS)	Insufficient involvement of the management body	<ul style="list-style-type: none"> • Inadequate understanding of issues • Inappropriate decisions • Insufficient monitoring
	IT strategy inadequately defined or aligned with the business strategy	<ul style="list-style-type: none"> • Failure to anticipate business needs and technological upgrades/issues/uses • Inadequate tools and service levels
	Deficient budget management	<ul style="list-style-type: none"> • Inadequate budget alignment with the strategy • Non-existent or insufficiently clear budget allocation • Inappropriate oversight of expenditures
	Roles and responsibilities of the IT and information security functions	<ul style="list-style-type: none"> • Poorly defined, allocated or communicated roles and responsibilities • Inadequate or insufficient staffing
	Inadequate rationalisation of the IT	<ul style="list-style-type: none"> • Lack of control over information system architecture (urbanisation) • Inconsistent IT standards • Failure to manage obsolescence
	Inadequate Control of outsourcing	<ul style="list-style-type: none"> • Inadequate contractual framework • Overdependence • Inadequate monitoring of service levels • Inadequate reversibility procedure
	Statutory and regulatory non-compliance	<ul style="list-style-type: none"> • Business needs not in compliance with applicable laws • Information system not in compliance with the business lines' legal instructions • Incompatibility of IT standards with applicable laws
	Inadequate risk management	<ul style="list-style-type: none"> • Non-existent or partial risk mapping • Default in the risk analysis • Inadequate permanent control system • Inadequate detection and management of operational risk incidents • Inadequate periodic control system

Macro process	Primary IT risk factors	Secondary IT risk factors
Operating the IS	Unsound operations management (systems and networks)	<ul style="list-style-type: none"> • Inadequate means of production • Inadequate process for detecting errors and anomalies • Inadequate management of incidents/problems • Non-compliance with service levels
	Unsound management of IT continuity	<ul style="list-style-type: none"> • Inadequate continuity organisation • Inadequate identification of unavailability scenarios • Non-alignment of IT continuity with business continuity • Inadequate protection of means of production and backup resources against accidents • Inadequate continuity systems • Inadequate testing
	Inadequate change management (projects, upgrades, fixes)	<ul style="list-style-type: none"> • Inadequately defined or applied change management standards • Poor project management organisation • Functional and technical requirements not adequately taken into account • Default in software • Inadequate testing • Improperly implemented changes
	Poor data quality	<ul style="list-style-type: none"> • Inadequate data standardisation • The information system uses or generates erroneous data • Inadequate data quality controls
Securing the IS	Inadequate physical protection of facilities	<ul style="list-style-type: none"> • Inadequate protection against intrusion into buildings • Inadequate protection of IT equipment
	Inadequate identification of assets	<p>Incomplete:</p> <ul style="list-style-type: none"> • asset inventory • asset classification
	Inadequate logical protection of assets	<p>Deficiencies in:</p> <ul style="list-style-type: none"> • Perimeter security systems • Protection against malware • Identity and access rights management • Authentication of employees • Protection of the integrity of systems and data • Protection of the confidentiality of data • Protection of availability • Management of security patches • Security review processes • Security of outsourced solutions • Information systems security awareness
	Inadequate process for detecting attacks	<p>Deficiencies in:</p> <ul style="list-style-type: none"> • Trace collection and analysis • Monitoring of unusual behaviour of users
	Inadequate attack response system	<p>Deficiencies in:</p> <ul style="list-style-type: none"> • Crisis management • Containment of attacks • Business recovery