Just in Time

Guidelines on ICT and Security Risk Management

EBA/GL/2019/04

Dario Esposito
Matteo Cecchin

Jun 2020

iason
ESSENTIAL SERVICES FOR
FINANCIAL INSTITUTIONS

At a Glance

01

Introduction

Introduction 1/4

- **Technology has never been more important to financial institutions,** both for supporting existing operations and developing new capabilities: the Covid-19 crisis has exposed the value of technologies which enable the economy to operate at arm's length and partially overcome social distancing.

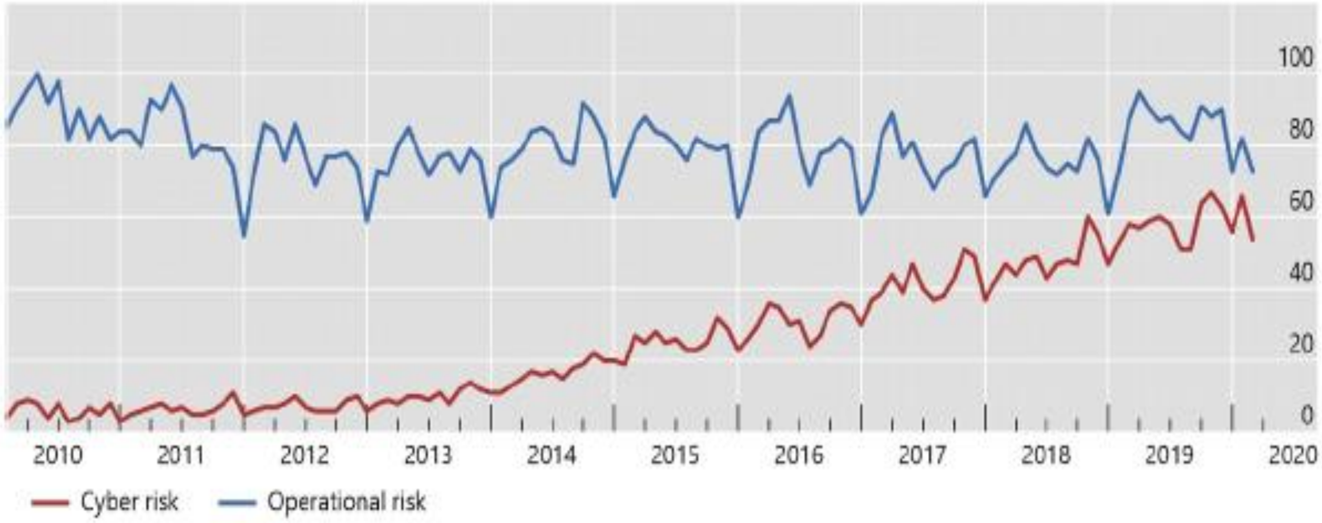
“Even in the financial intermediation sector, the health crisis and containment measures have made the benefits of digital solutions. An acceleration in investments will only result in new technologies, which with the achievement of the appropriate economies of scale can be carried out at lower costs and with greater benefits…..There are many sectors that can benefit from technological innovation: distribution of services, evaluation and monitoring of the customer creditworthiness, regulatory compliance processes. In retail payments sector, traditional innovation incubator, the opportunities offered by technology can bring concrete advantages to users of the services”.
(*source: Bank of Italy, Final Remarks by the Governor - Annual report, Rome, Italy, 29 May 2020)*

- **The 2020 Single Supervisory Mechanism risk map identified cybercrime and IT deficiencies as one of the top risks** faced by the euro area banking system.

“In general, financial authorities are warning financial institutions to be particularly watchful in relation to their IT networks and non-public data; third-party risk; cyber security incident response plans and to focus effort on staff training and awareness.
Tackling cyber security risks as part of effort to ensure the continuity of critical financial services, including through requirements to bolster firms’ operational resilience or business continuity.”
(source: Financial Stability Institute-BIS, Financial crime in times of Covid-19 – AML and cyber resilience measures, J.C. Crisanto and J. Prenio, May 2020)

Introduction 2/4

Interest on cyber risk is on par with operational risk.



Notes: Number of online searches for "cyber risk" and "operational risk" over the last decade. Worldwide search interest is relative to the highest point (=100). Data accessed on 7 Feb 2020.

(source: BIS Working Papers, The drivers of cyber Risk, May 2020)

Introduction 3/4

- **ICT and security risk is a risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs** when the environment or business requirements change (i.e. agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.

- Strictly related to ICT and security risk is the **operational resilience** which is broadly related to the ability of financial institutions to prevent, adapt, respond to, recover and learn from, operational disruptions. A lack of operational resilience poses a systemic threat to the stability of the financial services industry.

- The purpose of the EBA guidelines is to address ICT and security risks that have increased in recent years due to the **increasingly interconnected IT systems** between multiple financial institutions or between financial institutions and third-party service providers.

- **The guidelines** respond to the European Commission's FinTech Action plan published in March 2018 and **outline how financial institutions (credit institutions, investment firms and payment services providers – PSPs) should manage their ICT and security risks**: they contribute to a level playing field for all EU financial institutions.

Introduction 4/4

- These guidelines complement the supervisory assessment to the applicable institutions on ICT risk assessment under the Supervisory Review and Evaluation Process - SREP - (EBA/GL/2017/05) and other relevant guidelines on outsourcing arrangements (EBA/GL/2019/02).

- **These guidelines comply with the provisions in the CRD and PSD2**:
  a) Article 74 of Directive 2013/36/EU (CRD), which strengthens the governance requirements for institutions and effective processes to identify, manage, monitor and report the risk they are or might be exposed to;
  b) Article 95 of Directive 2015/2366/EU (PSD2), which contains explicit provisions for the management of operation and security risks of PSPs.

- Financial institutions should refer to the existing standards and leading best practice: **the guidelines intend to be technology and methodology agnostic.**

- **The implementation of these guidelines should be carried out in accordance with the principle of proportionality**, taking into account the scale and complexity of operations, the nature of the activity engaged in, the types of services provided and the corresponding ICT and security risks related to the processes and services of financial institutions. **These guidelines apply from 30 June 2020**.

02

Governance and Strategy

Governance and Strategy 1/4

Governance 1/2

- **The establishment of sound internal governance and an internal control framework** for ICT and security risks that sets responsibilities for financial institutions' staff and their management bodies.
- **The guidelines are compatible with the three lines of defense model**, with the ICT operational units being the first line of defense. The guidelines focus in particular on the responsibilities of the management body (Board) and the second line of defence (which usually includes the information security function) which must be appropriately segregated from ICT operations processes and not responsible for any internal audit (i.e. third line of defence).
- **The management body should ensure that financial institutions define the decision-making framework with clear steps and measures of success and allocates responsibilities and accountabilities** to ensure that the right stakeholders are engaged to manage ICT and security risks (ICT functions, information security risk management, business continuity).
- The Board is ultimately responsible for overseeing the entire ICT and security risk' framework, while senior management oversees the implementation of the policies, procedures and controls.

Governance and Strategy 2/4

Governance 2/2

- **The management body should ensure that ICT operational needs and their ICT and security risk management processes are adequately staffed** (i.e. in qualitative and quantitative way) **and** the competencies of relevant personnel are maintained and regularly enhanced through **a structured training program** (on an annual basis, or more frequently if required). Senior management demonstrates commitment by creating an organizational environment where staff are encouraged to report or escalate ICT and security incidents to management.

- **The Board and senior management view ICT and security risk framework not simply as a cost to be borne, but as an investment to ensure the security and reliability of financial services**: a good ICT and security risk' framework is a necessary competitive advantage element for a financial institution. The management body should allocate sufficient budget including budget for technology tools and other support, training and communication programs at all levels of the organization. Peer comparison (i.e. benchmarking) can help identify areas where investments should be channeled.

Governance and Strategy 3/4

Strategy

- **The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy** as well as for the establishment of an effective risk management framework for ICT and security risks.
- **The ICT strategy should define**:
  a) how financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organizational structure, ICT system changes and key dependencies with third parties;
  b) the planned strategy and evolution of the architecture of ICT, including third party dependencies;
  c) clear information security objectives, focusing on ICT systems and ICT services, staff and processes.
- **Financial institutions should establish sets of action plans** that contain measures to be taken to achieve the objective of the ICT strategy. Action plans should be:
  a) communicated to all relevant staff - including contractors and third party providers;
  b) periodically reviewed to ensure their relevance and appropriateness;
  c) monitored and measured the effectiveness of their implementation.

Governance and Strategy 4/4

Third party providers

- Financial institutions should ensure **the effectiveness of the risk-mitigating measures** as defined by their risk management framework when operational functions of payment services and/or ICT services and ICT systems **of any activity** are **outsourced, including to group entities, or when using third parties**.
- **To ensure continuity of ICT services and ICT systems**, financial institutions **should ensure that contracts and service level agreements - SLA -** (both for "business as usual" as well as in the event of service disruption – business continuity) **with providers** include the following:
  a) appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements;
  b) specifications of the financial institution's data life cycle;
  c) any requirements regarding data encryption, network security and security monitoring processes;
  d) the location of data centers;
  e) operational and security incident handling procedures including escalation and reporting.
- **Financial institutions should monitor and seek assurance of the level of compliance** of these third party providers.

03

Risk Management Framework and Business Continuity

Risk Management Framework and Business Continuity 1/5

ICT and security risk management framework 1/3

- Financial institutions should have **adequate processes and controls to ensure that all risks are identified, analyzed, measured, monitored, managed, reported and maintained within the limits of the financial institution's risk appetite**. Responsibility for managing and supervising ICT and security risks is assigned to a control function.

- **The ICT and security risk management framework** should include processes in place to:
  a) set a risk appetite for ICT and security risks;
  b) identify and evaluate the ICT and security risks define mitigation measures;
  c) supervise the effectiveness of measures and the number of reported incidents;
  d) report to the management body on the ICT and security risks and controls;
  e) identify and evaluate if there are ICT and security risks arising from significant changes in ICT system or ICT services, processes or procedures, or after significant operational or security incident.

- Financial institutions should **identify, establish and maintain an updated mapping of their business functions, roles and supporting processes** (and the information structure to support them) to identify the relevance of each and their interdependencies related to ICT and security risks. To define the criticality they should consider the requirements of confidentiality, integrity and availability.

Risk Management Framework and Business Continuity 2/5

ICT and security risk management framework 2/3

- Financial institutions should **identify the ICT and security risks that affect business functions**, **processes and information assets** at least annually. They should ensure constant monitoring of threats and vulnerabilities and periodically review risk scenarios.

- Financial institutions should determine which actions are required to **mitigate identified ICT and security risks to acceptable levels**, considering the time required to implement these improvements to remain within the financial institution's ICT and security risk appetite.

- Financial institutions **should report the results of the risk assessment** to the management body in a clear and timely manner.

- **Periodical audits** should be carried out by auditors with sufficient knowledge, skills and expertise to guarantee an independent assurance of their effectiveness. For better effectiveness of the audit activity, a **follow-up process** - including provisions for the timely verification and remediation of critical ICT audit findings - should be established.

Risk Management Framework and Business Continuity 3/5

ICT and security risk management framework 3/3

Requirements for Payment Service Users (**PSUs**) relationship management.

PSPs should**:**

- establish and implement processes to increase PSUs’ awareness on the security risks associated with the payment services;
- update the assistance offered to PSUs considering new threats and vulnerabilities, every changes should be reported to the PSU;
- allow PSUs to disable specific payment functions related to the payment services offered by the PSP to the PSU;
- provide the payer with the option to adjust the limits up to the agreed maximum limit;
- provide PSUs with the option to receive alerts about initiated or unsuccessful attempts to initiate payment transactions, allowing them to detect fraudulent use of their accounts;
- keep PSUs informed of updates of security procedures;
- provide support to PSUs and inform them of how to obtain such assistance.

Risk Management Framework and Business Continuity 4/5

Business continuity management 1/2

- Financial institutions should establish a **Business Continuity Management (BCM) process** to maximize their ability to provide ongoing services and to limit losses during serious business disruption events.
- Financial institutions should conduct **Business Impact Analysis (BIA) by analyzing their exposure to serious business disruptions and evaluating potential impacts** (quantitatively and qualitatively) using internal or external data and scenario analysis and ensuring that their ICT systems and ICT services are designed and aligned with their BIA.
- Financial institutions should establish **Business Continuity Plans (BCP)**, **in order to guarantee an adequate response to potential failure scenarios** (with specific conditions that lead to their activation) and the ability to resume critical business operations (critical ICT systems and services) within a recovery time target.
- Financial institutions should develop **Response and Recovery Plans**, specifying which conditions may require activation of the plans and which actions should be taken. These plans should:

a) consider both short-term and long-term recovery options;

b) focus on the recovery of critical business functions, processes, information assets and their interdependencies;

c) be documented and made available to the business and support units and easily accessible in case of an emergency;

d) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and adjusted recovery targets and priorities;

e) consider alternative choices where recovery may not be possible in the short term due to costs, risks, logistics or unexpected circumstances.

Risk Management Framework and Business Continuity 5/5

Business continuity management 2/2

- Financial institutions should **test and update BCPs** at least once a year. BCP test should prove that they are **able to sustain the profitability of their businesses until critical operations are re-established**. In particular they should:
  a) include testing of an adequate set of serious but plausible scenarios;
  b) be designed to challenge the assumptions on which BCPs is based;
  c) include procedures to verify the ability of staff and contractors.
- Test results should be documented and any identified gaps resulting from the tests should be analyzed and reported to the management body.
- Financial institutions should ensure that **appropriate crisis communication measures** are in place so that all relevant internal and external stakeholders (including the competent authorities and relevant providers) are informed in a timely and adequate manner.

04

Information Security and Operations Management

Information Security and Operations Management 1/6

Information Security 1/3

- Information security (IS) policies should be **well documented** by financial institutions.
- The guidelines set out several **requirements** for the institution's policy. The policies should:
  a) define high-levels principles and rules to protect the **confidentiality, integrity and availability** of the customers' **data and information**;
  b) be **in line** with the institution's IS **objectives**;
  c) based on the results of the risk assessment process;
  d) be approved by the management body;
  e) include a **description of the main roles** and responsibilities of IS management;
  f) set out requirements for staff and contractors, processes and technology;
  g) ensure confidentiality, integrity and availability of critical assets, resources and sensitive data;
  h) be **communicated to all staff and contractors**.

Information Security and Operations Management 2/6

Information Security 2/3

- Institutions should implement security measures to mitigate ICT and security risks.
- Besides the overall organization and governance requirements, these measures should include:

Logical security

- Definition, documentation and implementation of measures that cover items such as:
  - a) definition and segregation of duties;
  - b) user accountability and activity logging;
  - c) access rights, management, and recertification;
  - d) authentication methods.
- Users should be granted the least amount of access-right privileges to perform their own duties

Physical security

- Physical access to ICT systems should be permitted to authorized individuals only.
- Authorized individuals should be appropriately trained.
- Physical assets should be protected by environmental hazards in a way that is proportional to the criticality of related ICT operations.

ICT operation security

- Procedures should prevent or minimize the impact of issues in ICT systems and services.

Information Security and Operations Management 3/6

Information Security 3/3

Security Monitoring

- Procedures should aim to detect and report intrusions and breaches.
- Monitoring processes should **cover internal and external** factors, misuse of access and threats.

Information security reviews, assessment and testing

- Testing should be performed periodically by independent testers and should include vulnerability and penetration tests.
- Security measures should be updated based on test results.

Information security training and awareness

- Employees and contractors should be trained periodically and undergo security awareness programs.

Information Security and Operations Management 4/6

ICT Operation Management

- Institutions are required to do the following, in order to ensure the efficiency and safety of their ICT operations:
  - a) maintain and improve efficiency, while minimizing potential errors arising from manual tasks;
  - b) implement logging and monitoring procedures;
  - c) maintain **detailed** inventory of ICT assets;
  - d) plan and monitor performance and capacity of their ICT systems in to order to prevent, detect and respond to performance issues in a timely manner;
  - e) ensure appropriate procedures are in place to backup and restore data in case of required recovery.
- Institutions are required to manage ICT incidents by implementing of the following:
  - a) establish and implement processes to monitor and log incidents, in order to promptly react and resume critical business functions;
  - b) establish criteria to classify and prioritize incidents;
  - c) establish procedures to quickly identify root causes behind different types of incidents;
  - d) establish an efficient communication plan and define an escalation process;
  - e) identify roles and responsibility for different incidents scenarios.

ICT Operations should be managed with the goal of maximizing efficiency while minimizing the occurrence of issues. When issues do arise, institutions should have processes in place to minimize their impact based on past experience, correct classification and prioritization, function allocation and quick identification of the root cause of the issue.

Information Security and Operations Management 5/6

ICT Project and Change Management 1/2

ICT Project Management

- When monitoring and mitigating ICT risk deriving from their ICT project portfolios, institutions should take into consideration the risks that may result from interdependencies of projects and of resources allocated on different projects.
- Project management policy should at the very least cover objective, responsibilities, risk assessment, plan with timeframe and steps, key milestones and change management requirements.
- The progress of ICT projects and their associated risks should be reported to the management body.
- Project risk should be included in the institution's risk management framework.

ICT Systems Acquisition and Development

- Functional and non-functional requirements of new systems should be clearly identified.
- Institutions should have processes in place to mitigate the risk arising from any alteration of ICT systems during development and implementation.
- Testing and approval procedures should be in place to ensure that systems perform as intended, prior to their first use.
- Systems should be monitored and tested to identify potential threats.
- Production environment should be segregated from development, testing and other non-production environments.
- Institutions should protect and accurately document the source codes of ICT systems.

Information Security and Operations Management 6/6

ICT Project and Change Management 2/2

ICT Change Management

- All changes to ICT systems should be recorded, tested, assessed, approved, implemented and verified in a controlled manner.
- If these changes occur during emergencies, they should follow a set of procedures that provide adequate safeguards.

05

Final Remarks

Final Remarks

Information technology has become a critical component of well-functioning economies, underpinning economic growth over the past decades *(source: BIS Working Papers, The drivers of cyber Risk, May 2020).*

Nevertheless, **it is of paramount importance for financial institutions to find a trade-off** between ICT/security resilience and avoiding imposing an excessive burden that could hinder their delivering of key financial services. In the coming years **Supervisory pressure is likely to increase in the area of ICT and security risk**, not only because of pandemic crisis in progress.

Then to best exploit these EBA guidelines, financial institutions urgently need to:

- provide **human resources with adequate knowledge and experience** in ICT and security risk management (for example, assess even if management body and internal control functions fully understand the main risks related to ICT and security; make sure adequate “Tone at the Top” is maintained);
- have **sound and well documented processes** in place to mitigate ICT and security risk and, in particular, efficiently run ICT operations and projects, to manage system change and to maximize information security, by mitigating the risk deriving from these aspects of the business;
- implement **efficient and robust ICT protection procedures** to minimize the impact of possible issues on the business and on its customers in case these issues (ICT and security risk) do occur; reduce dependency on end-of-life IT systems;
- have a **Business Continuity Plans (BCP)** practically and not only theoretically applicable (avoid underestimating low-probability risks and outcomes); institutions should also constantly update the BCPs to ensure that they are able to sustain the businesses profitability until critical operations are re-established.
- be able to **manage new emerging risks** as risks from “smart/remote working” and dependency on third party providers.

Company Profile

Iason is an international firm that consults Financial Institutions on Risk Management. Iason integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning

Dario Esposito
Senior Manager

Matteo Cecchin
Business Analyst

This document was prepared in collaboration with Simone Manca, who at the time were working for Iason Consulting.

www.iasonltd.com