EBA Guidelines on ICT and security risk management – EBA/GL/2019/04
Establishing harmonized requirements for ICT and security risk management across the Single Market
Introduction

On 28 November 2019, the European Banking Authority (EBA) published the Final Report on the Guidelines on ICT and security risk management (EBA/GL/2019/04) to establish requirements for credit institutions, investment firms and payment service providers (PSPs) on the mitigation and management of ICT and security risks.

The purpose of the Guidelines is to establish requirements for the management of ICT and security risks, both of which have escalated in recent years due to the increasing digitalization of the financial sector and the growing interconnectedness with other financial institutions and third parties through telecommunication channels.

The Guidelines, which will enter into force on 30 June 2020, set out expectations of how all financial institutions should manage internal and external ICT and security risks that they may be exposed to.

The Guidelines represent a further step in harmonizing the ICT and security risk management approach in the European Single Market.


This article is intended for credit institutions, investment firms and payment service providers operating in Luxembourg and will cover the following key questions:

- Why effective ICT and security risk management is important to financial institutions?
- How are the different financial institutions impacted by the Guidelines?
- What are the main principles and domains of the Guidelines?
- How can Deloitte help?
Why effective ICT and security risk management is important to financial institutions?

ICT (Information and Communication Technology), using the terminology from the EBA Guidelines, but also more commonly known as IT (Information Technology), is a key resource in developing and supporting banking services. Financial institutions are embracing large scale digitalization and rely on the use of ICT for processing and analyzing information and reengineering operations.

ICT can be implemented by financial institutions to improve internal processes or to offer innovative services and new functions to customers in order to best serve their ever-increasing expectations and needs. However, the complexity of adopted technologies, and the continuously growing dependency on them, can itself lead to greater ICT and security related incidents.

- Failure of ICT systems and services can have dramatic consequences for financial institutions.
- Backbone of almost all banking processes and distribution channels
- Source of competitive advantage
- Support the automated controls environment
- Materiality of ICT costs and investments

- Given the growing reliance of financial institutions on ICT for their operational functioning, failure of ICT systems and services can have a dramatic impact on financial institutions.
- Technological innovation plays a crucial role in the banking sector from a strategic standpoint and as a source of competitive advantage. It is a fundamental tool to compete in the financial market with new products as well as through facilitating the restructuring and optimization of the value chain.
- ICT systems are not only key enablers of institutions’ strategies, forming the backbone of almost all banking processes and distribution channels, but they also support the automated controls environment on which core banking data is based.
- ICT systems and services also represent material proportions of institutions’ costs, investments and intangible assets.
In this regard, ICT and security risk management is an essential and integral part of successful enterprise management.

According to the definition provided in the Guidelines, the concept of ICT and Security Risk implies a risk of loss due to:

- Breach of confidentiality, failure of integrity of systems and data
- Inappropriateness or unavailability of systems and data
- Inability to change information technology within a reasonable time and with reasonable costs when the environment or business requirements change

This includes security risks resulting from:

- Inadequate or failed internal processes
- External events including cyber-attacks
- Inadequate physical security

The concept so defined promotes a consistency with an operational risk approach (i.e., risks arising from inadequate or failed internal processes, people and systems or from external events) because, if the risk is realized, it results in a loss.

Consequently, operational, ICT, information security and more specific risks (i.e. Cyber risks) are now directly interrelated, as presented in the taxonomy below.

The correlation with operational risks is further prescribed by current EBA Supervisory Review and Evaluation Process (SREP) Guidelines. In the Guidelines, intended to promote common procedures and methodologies for the supervisory evaluation process, competent authorities are required to assess ICT and security risk as a sub-category of operational risk.

Indeed, in the broader context of the Capital Requirements Directive IV (CRD IV), ICT and security risk management plays a crucial role in the calibration of the additional capital requirements covering material risks.

The Guidelines also highlight the new role of ICT and security risk management as an accelerator for financial institutions to improve their operational resilience by continuously adapting to the evolution of threats.
How are the different financial institutions impacted by the Guidelines?

The Guidelines are intended to help with defining how organizations should comply with provisions of CRD IV (Directive 2013/36/EU – Article 74) and PSD2 (Directive 2015/2366/EU – Article 95).

Article 74 of Directive 2013/36/EU (CRD), mandates the European Banking Authority to harmonize governance, processes and mechanisms of all financial institutions.

Furthermore, establishment, implementation and monitoring of security aspects for operational risks is derived from a mandate to issue guidelines on Article 95(3) of Directive (EU) 2015/2366 (PSD2).

Both above-mentioned directives support the action plan set forth by European Commission, due to which, the Guidelines on ICT and security risk management have been developed and will be mandatory to comply with as of 30 June 2020.
When focusing on the scope of the Guidelines, the previous Guidelines in force (EBA/GL/2017/17) are applicable only for Payment Service Providers for their payment services.

The new Guidelines (EBA/GL/2019/04) are applicable to:

- **Credit institutions** and **investment firms**, as defined in the Capital Requirements Regulation (EU) No. 575/2013, applicable to all their services
- **Payment Service Providers (PSPs)** subject to the revised Payment Service Directive (PSD2), applicable to all their payment services

The Guidelines on security measures for operational and security risks under PSD2 (EBA/GL/2017/17) have been fully integrated in the EBA Guidelines on ICT and Security risk management and will be repealed when the latter enters into force.

Guidelines on ICT and Security risk management will repeal the Guidelines on security measures for operational and security risks under PSD2 on **30 June 2020**
What are the main principles and domains of the Guidelines?

The Guidelines are principle-based and outline expectations in the following domains to mitigate ICT and security risks:

**Business continuity management**
Establishment of a sound business continuity management process, including business impact analysis, business continuity planning, and response and recovery planning activities.

**ICT operations management**
Implementation of documented processes to manage ICT operations in a controlled manner, including capacity management, incident management and problem management.

**Governance and strategy**
Implementation of adequate governance, accountability and the alignment of the ICT strategy with the overall business strategy.

**ICT and security risk management framework**
Establishment of an ICT and security risk management framework required by the Guidelines, including the performance of regular risk assessments, audit and reporting activities.

**Information Security**
Documentation and development of a comprehensive set of documents and other controls to achieve the implementation of adequate levels of logical and physical security, trainings and constant monitoring.
The implementation of the Guidelines should be done in accordance with the principle of proportionality.

The Guidelines do not outline how financial institutions are expected to implement the 3 Lines of Defense model, but they are compatible with the model (and aligned with EBA Guidelines on internal governance).

Cyber risks may require some mitigating measures that differ from traditional information security measures.

Complying with the Guidelines will allow financial institutions to develop secure ICT risk management.

Attention should be directed to the key themes and principles introduced in the Guideline and defined below.

The Guidelines complement and should be read in conjunction with the SREP Guidelines (EBA/GL/2017/05) and the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

Focus on the responsibilities of the management body and the second line of defence (which usually includes the information security function).

Introduce new concept of “operational resilience” through business continuity impact analyses.
How can Deloitte help?

Deloitte helps organizations to establish and improve their ICT and security risk management practices by supporting companies in:

- **Regulatory compliance assessment** – gap assessment against the regulatory requirements set forth in the EBA Guidelines on ICT and security risk management
- **ICT and security risk management capability enhancement** – ICT and security risk management policies and standards, processes, tools and technologies
- **ICT and security risk reporting and culture** – ICT, business and board ICT and Security risk reporting using KRI s to provide visibility to senior management
- **ICT and security risk assessment** – ICT and security risk assessment in the context of digital initiatives or major ICT changes, tailored to the organizations’ risk profile and integrated into the organizations’ risk management framework
- **Readiness ICT and security assessment** – simulation of competent authorities’ on-site inspection to test the readiness of companies’ processes and practices towards regulatory requirements set forth in EBA Guidelines

**Deloitte success stories**

- **ICT risk management framework** – Deloitte tailored a comprehensive ICT risk management program covering definition and implementation of strategy, operating model, policies, management processes, tools, reporting, etc.
- **ICT Risk assessment** – the assistance included the identification and evaluation of ICT risks based on a predefined ICT risk assessment methodology, including applicable EBA Guidelines principles and industry best practices
- **ICT risk measurement and monitoring** – Deloitte assisted the design and implementation of ICT risk dashboards (and related processes), supporting the organization in the definition of KRI s reporting functionalities to senior management

**Our approach and methodology**

Deloitte has developed a rich suite of proven accelerators and tools, supported by market insights, in order to address ICT risk management challenges. This includes a tested ICT risk management framework, comprehensive ICT risk and control catalogs aligned with latest regulatory requirements and standards, and more.
Contacts

Roland Bastin  
Partner – Risk Advisory  
+352 451 452 213  
rbastin@deloitte.lu

Irina Gabriela Hedea  
Partner – Risk Advisory  
+352 451 452 944  
ighedea@deloitte.lu

Frederic de Pauw  
Senior Manager – Risk Advisory  
+352 451 454 383  
fdepauw@deloitte.lu

Stéphane Hurtaud  
Partner – Risk Advisory  
+352 451 454 434  
shurtaud@deloitte.lu

Onur Ozdemir  
Director – Risk Advisory  
+352 451 452 207  
oozdemir@deloitte.lu

Francesco Martini  
Senior Manager – Risk Advisory  
+352 451 454 018  
fmartini@deloitte.lu