Deloitte.

EIOPA Guidelines on Information and Communication Technology Security and Governance

Key insights and self-assessment checklist

April 2021

MAKING AN IMPACT THAT MATTERS since 1845

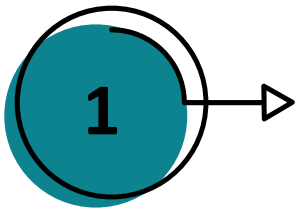
Introduction

Introduction

On 12 October 2020, the **European Insurance and Occupational Pensions Authority** (EIOPA) issued its **Guidelines on Information and Communication Technology Security and Governance** ("the Guidelines") in accordance with Article 16 of Regulation (EU) No 1094/20104 harmonizing the European Commission's FinTech Action Plan (COM/2018/0109 final) and EIOPA's Supervisory Convergence Plan 2018–2019.

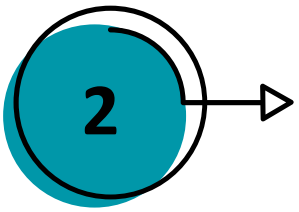
The Guidelines provide guidance on the sound information and communication technology (ICT) governance and security practices that insurance and reinsurance undertakings should implement to mitigate their technological risks appropriately.

The Guidelines encompass seven main areas:



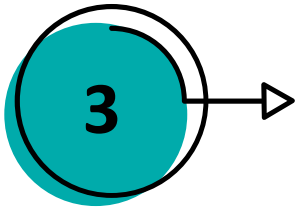
Governance and strategy

Establish governance to effectively support the ICT strategy



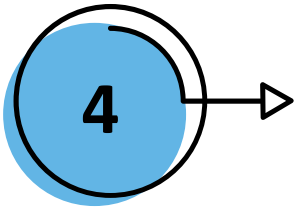
ICT and security risk management

Ensure ICT and security risks are identified and addressed appropriately



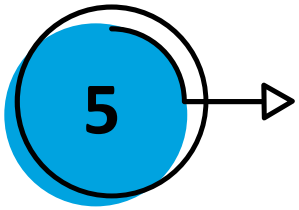
ICT operations management

Implement efficient and controlled ICT operations processes



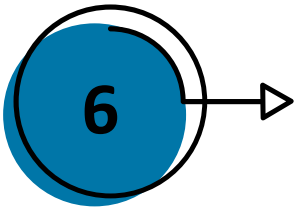
Information security

Protect the confidentiality, integrity and availability of customer and business data



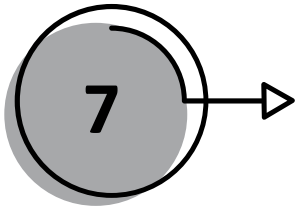
ICT project and change management

Manage projects and changes effectively to meet business and security objectives



Business continuity management

Maintain the business function under unforeseen circumstances



Outsourcing

Protect outsourced IT services appropriately

The Guidelines represent a key step for the insurance sector to align with the European Commission's aim to improve and harmonize the digital operational resilience of the EU's financial services (as envisioned by the legislative proposal for a Digital Operational Resilience Act).

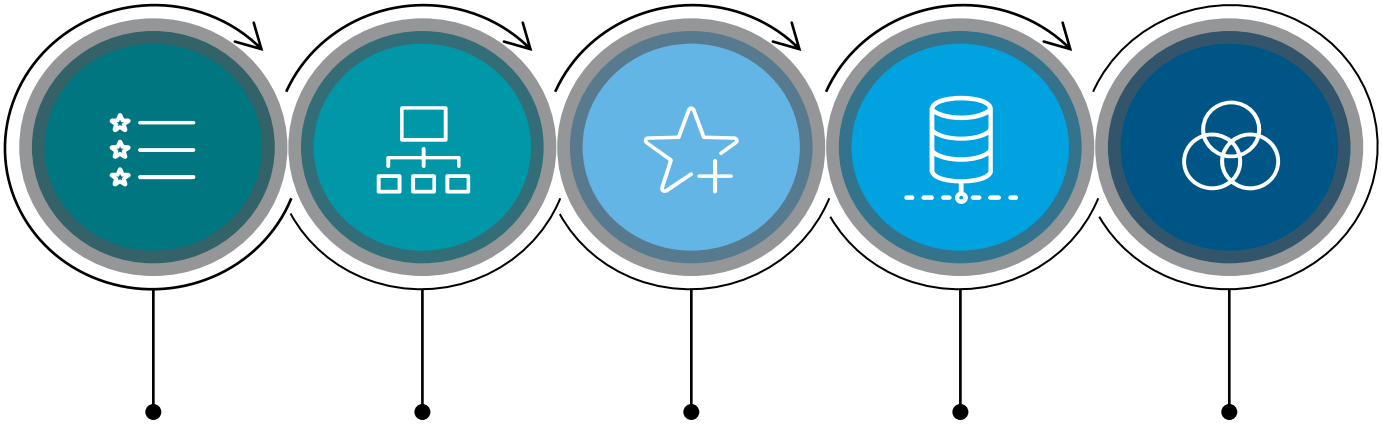
Objectives

The Guidelines aim to increase the resilience of insurance and reinsurance undertakings' digital operations against the risks they face. In particular, the Guidelines:

- Provide clear requirements of minimum expected information security practices;
- Provide compliance guidance; and
- Harmonize the ICT security requirements in relation to supervisory governance processes.

The Guidelines will **come into force on 1 July 2021** and shall apply to both **individual undertakings and mutatis mutandis at the group level.**

The Guidelines address the following key aspects:



Mitigation and management of ICT risks

Undertakings should establish expectations on the mitigation and management of ICT security and governance risks.

Principle of proportionality

Undertakings should apply the Guidelines in a manner that is proportionate to the nature, scale and complexity of the risks inherent in their business.

Rely on adapted standards and leading best practices

In implementing the Guidelines, undertakings can refer to the most adapted standards and leading best practices.

Responsibilities of the management body and risk management

The Guidelines focus on the responsibilities of the administrative, management or supervisory body (AMSB) and risk management.

To be read in conjunction with other directives/regulations/ guidelines

The Guidelines should be read in conjunction with the Solvency II Directive, the Delegated Regulation, EIOPA's Guidelines on System of Governance and EIOPA's Guidelines on Outsourcing to Cloud Service Providers.

Implementation of the Guidelines in the Luxembourg insurance sector

Context

Insurance services and undertakings' **growing reliance on ICT**, coupled with **increased levels of digitalization** during the COVID-19 pandemic, have left **the insurance sector more exposed to information security incidents and cyberattacks**.

Implementing the Guidelines will ensure that insurance services and undertakings are **prepared and capable** of preventing and handling these threats through managing their ICT- and governance-related risks.

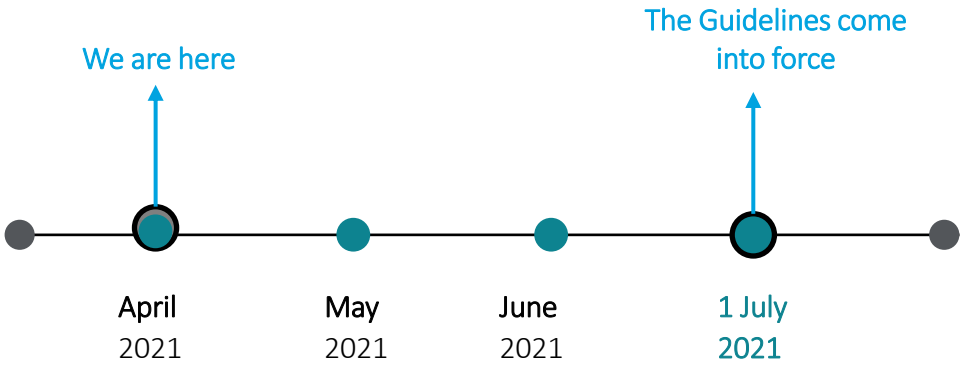
Compliance requirements

Competent authorities and undertakings are required to comply with the Guidelines and the respective recommendations. Consequently, undertakings should **incorporate the Guidelines into their regulatory framework, while competent authorities should implement the Guidelines into their supervisory framework.**

Authority compliance

Competent authorities will be **obliged to inform EIOPA of their compliance status within two months of the translated versions' issuance.** In the event of non-compliance, competent authorities must provide a reasoning to EIOPA within the same timeframe.

If EIOPA has not received any communication from the competent authorities by this deadline, **EIOPA will consider these authorities as non-compliant** and will take further action.



Self-assessment checklist

Evaluate your compliance readiness

Self-assessment checklist

The Guidelines cover 25 topics, each containing a set of specific requirements*.

This self-assessment checklist summarizes the 25 topics, allowing you to determine the readiness level of your current ICT security and governance management processes and to identify any potential gaps before the Guidelines come into force.

The Guidelines require The competent authorities to consider the **principle of proportionality**, meaning that the application of security and governance measures should be **proportionate to the scale and complexity of the potential risks**.

No.	Topic	Question	Yes	Partially	No
1	ICT governance	Are your staff members, including upper management, adequately and regularly trained on ICT and security risks, including information security? Do you have periodic awareness sessions in place?			
2	ICT strategy	Do you have an approved and implemented ICT strategy in place? Is it clearly communicated to the relevant stakeholders, and is it frequently reviewed and updated?			
3	ICT and security risks	Do you have an ICT and security risk management framework in place, which includes ICT and related cyber risks and respective risk tolerance levels and defined mitigation actions? Is there a regular ICT and security risk reporting mechanism in place for senior management?			
4	ICT and security risks	Do you carry out regular ICT and security risk assessments, including assessments before implementing any major changes to your infrastructure, processes or procedures?			
5	Audit	Do you perform regular audits of your ICT governance, ICT systems and ICT processes?			
6	Information security	Do you have an information security policy in place that outlines staff members' main roles, responsibilities and requirements? Is it communicated to all relevant stakeholders?			
7	Information security	Is there a separate and independent information security function established within your company that is appropriately independent of ICT operations?			
8	Logical security	Do you have strict access controls implemented in line with need-to-know and least privilege principles?			

* Please refer to the appendix of this document for a more detailed view of the structure of the Guidelines.

Evaluate your compliance readiness

Self-assessment checklist—continued

No.	Topic	Question	Yes	Partially	No
9	Physical security	Do you have physical security measures in place, such as restricted physical access and adequate protection against environmental hazards?			
10	ICT operations security	Do you have the relevant ICT operations security procedures in place, including vulnerability and patch management, log management, encryption of data at rest and in transit, etc.?			
11	Security monitoring	Have you defined an effective security monitoring procedure for detecting potential internal and external security threats?			
12	Information security	Have you defined a process for performing regular information security reviews, assessments and testing?			
13	ICT operations management	Do you have an up-to-date, accurate inventory of ICT assets in place?			
14	ICT incident and problem management	Have you defined an adequate incident and problem management process, which governs appropriate incident identification, tracking, logging, categorization and classification?			
15	ICT project management	Do you have an implemented robust ICT project methodology in place?			
16	ICT systems acquisition and development	Have you implemented a process governing the acquisition, development and maintenance of ICT systems to ensure that security requirements are well defined and implemented?			
17	ICT change management	Do you have a clearly defined ICT change management process that ensures traceable and controlled changes?			
18	Business continuity	Do you have an established business continuity management framework in place, including a defined business continuity plan, business impact analysis, business recovery plan and disaster recovery plan?			
19	Crisis communications	Do you have effective crisis communication measures in place to inform all relevant stakeholders in a timely manner in case of a crisis?			
20	Outsourcing of ICT services and systems (if applicable)	If you have outsourced your ICT services, have you included specific provisions in the contractual documentation for establishing requirements in terms of service performance, service continuity and data security?			

* Please refer to the appendix of this document for a more detailed view of the structure of the Guidelines.

Appendix

The Guidelines—detailed overview

The Guidelines list 74 requirements across all areas of ICT security and governance that are grouped into 25 higher level guideline topics.

No.	Guideline	Requirement no.
1	Proportionality	8
2	ICT within the system governance	9, 10, 11
3	ICT strategy	12, 13, 14, 15
4	ICT and security risks within the risk management system	16, 17, 18
5	Audit	19
6	Information security policy and measures	20, 21, 22, 23
7	Information security function	24, 25
8	Logical security	26, 27
9	Physical security	28, 29, 30
10	ICT operations security	31
11	Security monitoring	32, 33, 34
12	Information security reviews, assessment and testing	35, 36, 37, 38, 39
13	Information security training and awareness	40, 41
14	ICT operations management	42, 43, 44, 45, 46, 47, 48
15	ICT incident and problem management	49, 50, 51
16	ICT project management	52, 53
17	ICT systems acquisition and development	54, 55, 56, 57, 58, 59, 60, 61
18	ICT change management	62, 63
19	Business continuity management	64
20	Business impact analysis	65, 66
21	Business continuity planning	67, 68, 69
22	Response and recovery plans	70, 71, 72, 73
23	Testing of plans	74, 75, 76, 77
24	Crisis communications	78
25	Outsourcing of ICT services and ICT systems	79, 80, 81

How Deloitte can help

How can Deloitte help?

Deloitte helps organizations establish and improve the maturity of their ICT and security risk management practices and comply with regulatory requirements. Our services include:

- Regulatory compliance assessment: gap assessment against the Guidelines' regulatory requirements.
- ICT and security risk management capability enhancement: strengthening of 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 key risk indicators (KRIs) to provide visibility to senior management.
- ICT and security risk assessment: ad-hoc ICT and security risk assessments for digital initiatives or major ICT changes, tailored to the organization's risk profile and integrated with the organization's risk management framework.
- Readiness ICT and security assessment: simulation of competent authorities' onsite inspections to test the readiness of the company's processes and practices against the Guidelines' regulatory requirements.

Deloitte success stories

- ICT risk management framework: Deloitte tailored a comprehensive ICT risk management program to an organization's unique requirements, which covered the definition and implementation of the strategy, operating model, policies, management processes, tools, reporting, etc.
- ICT risk assessment: Deloitte assisted an organization to identify and evaluate ICT risks based on a predefined ICT risk assessment methodology that included applicable regulatory requirements and industry best practices.
- ICT Risk measurement and monitoring: Deloitte assisted the design and implementation of ICT risk dashboards (and related processes), supporting an organization to define KRI reporting functionalities to senior management.

Our approach and methodology

Deloitte has developed a rich suite of proven accelerators and tools supported by market insights to address organizations' ICT risk management challenges. These include a well-proven ICT risk management framework, and comprehensive ICT risk and control catalogs aligned with the latest regulatory requirements and standards.

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

Herve Marchand
Partner – Banking & Insurance
+352 451 452 292
hmarchand@deloitte.lu

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

Alexandre Heluin
Director – Risk Advisory
+352 451 454 030
aheluin@deloitte.lu

Michael Cravatte
Partner – Banking & Insurance
+352 451 454 758
mcravatte@deloitte.lu

Deloitte.

Deloitte Luxembourg
20 Boulevard de Kockelscheuer L-1821
Luxembourg Grand Duchy of Luxembourg

Tel.: +352 451 451
www.deloitte.lu