EIOPA-BoS-19-526
12.12.2019

Consultation paper on the proposal for Guidelines on Information and Communication Technology (ICT) security and governance

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany - Tel. + 49 69-951119-20;
Fax. + 49 69-951119-19; email: info@eiopa.europa.eu site: www.eiopa.europa.eu

1 Contents

Responding to this paper

1. EIOPA welcomes comments on the proposal for Guidelines on Information and Communication Technology (ICT) security and governance.
2. Comments are most helpful if they:
   a) contain a clear rationale; and
   b) describe any alternatives EIOPA should consider.
3. Please send your comments to EIOPA by 13 March 2020 responding to the questions in the survey provided at the following link:

   https://ec.europa.eu/eusurvey/runner/ICT_GLs

   Contributions not provided using the survey or submitted after the deadline will not be processed and therefore considered as they were not submitted.

Publication of responses

4. Contributions received will be published on EIOPA's public website unless you request otherwise in the respective field in the template for comments. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure.
5. Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to documents and EIOPA's rules on public access to documents[1].
6. Contributions will be made available at the end of the public consultation period.

Data protection

7. Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published. They will only be used to request clarifications if necessary on the information supplied. EIOPA, as a European Authority, will process any personal data in line with Regulation (EU) 2018EC) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regardregard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and decision No 1247/2002/EC. More information on data protection can be found with this link.

Consultation paper overview & next steps

8. EIOPA carries out consultations in the case of Guidelines and Recommendations in accordance with Article 16(2) of Regulation (EU) No 1094/2010. This Consultation Paper presents the draft Guidelines.
9. The analysis of the expected impact from the proposed policy is covered under Annex I (Impact Assessment).

[1] Public Access to Documents

Next steps

10. EIOPA will consider the feedback received, publish a Final Report on the consultation and submit the Guidelines for adoption by its Board of Supervisors.

Background

11. Under Article 16 of Regulation (EU) No 1094/2010 EIOPA may issue guidelines and recommendations addressed to competent authorities and financial institutions with a view to establish consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of Union law.

12. In accordance with Article 16(3) of that Regulation, competent authorities and financial institutions are required to make every effort to comply with those Guidelines and recommendations.

13. EIOPA identified the need to develop specific guidance on Information and Communication Technology (ICT) security and governance in relation to Articles 41 and 44 of Directive 2009/138/EC in the context of the analysis performed to answer to the European Commission FinTech Action plan (COM(2018) 109 final), the EIOPA Supervisory Convergence Plan 2018-2019[2] and following interactions with several other stakeholders[3].

14. As reported in the Joint Advice of the ESAs to the European Commission, EIOPA's Guidelines on system of governance "do not properly reflect the importance of taking care of ICT risk management (including cyber risks)". There is no guidance regarding vital elements that are generally acknowledged as being part of proper ICT security and governance".

15. Analysis of the current (legislative) situation in the EU for the above Joint Advice showed that a majority of EU-Member States have defined national rules for ICT security and governance. Although the requirements are similar, the regulatory framework is still fragmented. In addition, a survey on the current supervisory practices revealed a wide variety of practices - from 'no specific supervision' to 'strong supervision' (including 'off-site-inspections' and 'on-site inspections').

16. Furthermore, the complexity of ICT is increasing and the frequency of ICT related incidents (including cyber incidents) is also on the rise, as is the detrimental impact of such incidents on undertakings' operational functioning. For this reason, ICT and security risk management is fundamental for an undertaking to achieve its strategic, corporate, operational and reputational objectives.

17. In addition, across the insurance sector, including both traditional and innovative business models, there is an increasing reliance on ICT in the provision of insurance services and in the undertakings' normal operational functioning, e.g. digitalisation of the insurance sector (InsurTech, IoT, etc.) as well as interconnectedness through telecommunications channels (internet, mobile and wireless connections and wide area networks). This makes undertakings' operations vulnerable to security incidents including cyber attacks. It is therefore important to ensure that undertakings are adequately prepared to manage their ICT and security risks.

18. Furthermore, recognising the need for being prepared for cyber risk[4] and the a sound cyber security framework by undertakings, these Guidelines also cover cyber security as a part of the undertaking's information security measures. Whilst

[2] https://eiopa.europa.eu/Publications/Reports/Supervisory%20Convergence%20Plan%202018-2019.pdf

[3] The report published by EIOPA as answer to the European Commission FinTech Action plan can be obtained here

[4] For a definition of cyber risk please refer to the FSB Cyber Lexicon, 12th of November 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

these Guidelines recognise that cybersecurity should be addressed as part of an undertaking's overall ICT and security risk management, it is important to point out that cyber attacks have some specific characteristics, which should be taken into account to ensure that information security measures adequately mitigate cyber risk:

a) cyber attacks are often more difficult to manage (i.e. to identify, protect, detect, respond to and to fully recover from) than most of the other sources of ICT and security risk and also the extent of the damage is difficult to determine;

b) some cyber attacks can render common risk management and business continuity arrangements, as well as disaster recovery procedures ineffective, as they might propagate malware to backup systems in order to make them unavailable or to corrupt backup data;

c) service providers, brokers, (managing) agents and intermediaries may become channels to propagate cyber attacks. Contagious silent threats may use interconnectivity through third party telecommunications links to travel to the undertaking's ICT system. Therefore, an interconnected undertaking having individual low relevance may become vulnerable and a source of risk propagation and may result in a systemic impact. Observing the weakest link principle, cyber-security should not only be a concern for major market participants or critical service providers.

19. The objective of these Guidelines is to:

a) provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;

b) avoid potential regulatory arbitrage;

c) foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

Guidelines on Information and Communication Technology (ICT) security and governance

2 Introduction

1. In accordance with Article 16 of Regulation (EU) No 1094/2010[5] EIOPA issues these Guidelines addressed to the supervisory authorities to provide guidance on how insurance and reinsurance undertakings should apply the governance requirements foreseen in Directive 2009/138/EC[6] ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/35[7] ("Delegated Regulation") in the context of ICT security and governance. To that end, these Guidelines build on the provisions on governance provided by Articles 41, 44, 46, 47, 93, 132 and 246 of the Solvency II Directive and Article 258 to 260, 266, 268 to 271 and 274 of the Delegated Regulation. Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on system of governance (EIOPA-BoS-14/253)[8] and by EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-19/270)[9].
2. The Guidelines apply to both individual undertakings and *mutatis mutandis* at the level of the group[10].
3. Supervisory authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality[11]. The proportionality principle aims at ensuring that governance arrangements are consistent with the nature, scale and complexity of respective risks undertakings face or may face.
4. These Guidelines should be read in conjunction with and without prejudice to the Solvency II Directive, the Delegated Regulation, EIOPA Guidelines on system of governance and EIOPA Guidelines on outsourcing to cloud service providers.

Definitions

5. If not defined in these Guidelines, the terms have the meaning defined in the Solvency II Directive. For the purpose of these guidelines, the following definitions apply:

[5] Regulation (EU) No 1094/2010 Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pension Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[6] Directive 2009/138/EC 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), (OJ L 335, 17.12.2019, p. 1)

[7] Commission Delegated Regulation (EU) 2015/35Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 12, 17.1.2015, p. 1)

[8] EIOPA-BoS-14/253: https://eiopa.europa.eu/GuidelinesSII/EIOPA_Guidelines_on_System_of_Governance_EN.pdf

[9] EIOPA-BoS-19/270 https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf

[10] As defined by Article 212 (1) of Directive 2009/138/ECDirective 2009/138/EC

[11] The application of the principle of proportionality, in the context of these Guidelines, should be done in accordance to recitals 19, 20, 21 and Article 29 of Directive 2009/138/EC Directive 2009/138/EC

Asset owner	Person or entity with the accountability and authority for an information and ICT asset.
Availability	Property of being accessible and usable on demand (timeliness) by an authorised entity.
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
Cyber attack	Any type of hacking leading to an offensive / malicious attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorised use of an information asset that targets ICT systems
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.
ICT asset	An asset of either software or hardware that is found in the business environment.
ICT projects	Any project, or part thereof, where ICT systems and services are changed, replaced or implemented.
ICT and security risk	As a sub component of operational risk; the 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 ICT within a reasonable time and costs when the environment or business requirements change (i.e. agility). This includes cyber risks as well as information security risks resulting from inadequate or failed internal processes or external events including cyber attacks or inadequate physical security.
Information security	Preservation of confidentiality, integrity and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
ICT services	Services provided through ICT systems and service providers to one or more internal or external users.
ICT systems	Set of applications, services, information technology assets, ICT assets or other information-handling components, which includes the operating environment.

Information asset	A collection of information, either tangible or intangible, that is worth protecting.
Integrity	Property of accuracy and completeness..
Operational or security incident	A singular event or a series of linked unplanned events which have or will probably have an adverse impact on the integrity, availability and confidentiality of ICT systems and services.
Service provider	Means a third party entity that is performing an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.
Threat Led Penetration Testing	A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations..
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

6. These Guidelines shall apply from 01-07-2020

Guideline 1 – ICT within the system of governance

7. The administrative, management or supervisory body (AMSB) should ensure that undertakings' system of governance, in particular the risk-management and internal control system, adequately manage undertakings' ICT and security risks.

8. The AMSB should ensure that the quantity and skills of the undertakings' staff is adequate to support their ICT operational needs, ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy.

9. The AMSB should ensure that the budget allocated to fulfilling the above is continually appropriate. Furthermore staff should receive appropriate training on ICT and security risks, including information security, on a regular basis.

Guideline 2 – ICT strategy

10. The AMSB has overall responsibility for setting and approving the undertakings' ICT strategy as part of and aligned with their overall business strategy as well as overseeing its communication and implementation.

11. The strategy should define at least:

a) how undertakings' ICT should evolve to effectively support and implement their business strategy, including the evolution of the organisational structure, business models, ICT system and key dependencies with service providers;

b) the evolution of the ICT architecture, including service provider dependencies; and

c) clear information security objectives, focusing on ICT systems and services, staff and processes

12. Undertakings should ensure that ICT strategy is implemented, adopted and communicated to all relevant staff and service providers where applicable and relevant, in a timely manner.

13. Undertakings should establish a process to monitor and measure the effectiveness of the implementation of the ICT strategy.

Guideline 3 – ICT and security risks within the risk management system

14. The AMSB has overall responsibility to establish effective system for managing ICT and security risks as part of the undertaking's overall risk management system. This includes the determination of the risk tolerance for those risks, in accordance with the risk strategy of the undertaking and a regular written report about the result of the risk management process addressed to the AMSB.

15. As part of their overall risk management system, undertakings should in relation to ICT and security risks (while defining the ICT protection requirements as described below), consider at least the following:

a) Undertakings should establish and regularly update a mapping of their business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) in order to identify the importance of each and their interdependencies to ICT and security risks.

b) Undertakings should identify and measure all relevant ICT and security risks they are exposed to and classify the identified business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) in terms of criticality. Undertakings should also assess the protection requirements of, at least, confidentiality, integrity and availability of those business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) . Asset owners, who are accountable for the classification of the assets should be identified.

c) The methods used to determine the criticality as well as the level of protection required (in particular, with regard to the protection objectives of integrity, availability and confidentiality) should ensure that the resulting protection requirements are consistent and comprehensive.

d) The measurement of ICT and security risks should be conducted on the basis of the defined ICT and security risk criteria taking into account the criticality of their business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets), extent of known vulnerabilities and prior incidents that impacted the undertaking.

e) The assessment of ICT and security risks should be carried out and documented regularly. This assessment should also be performed before any major change in infrastructure, processes or procedures affecting the business

processes and activities, business functions, roles and assets (e.g. information assets and ICT assets).

f) Based on their risk assessment undertakings should, at least, define and implement measures to manage identified ICT and security risks and protect information assets in accordance with their classification. This should include the definition of measures to manage the remaining residual risks.

16. The results of the ICT and security risk management process should be approved by the AMSB and transferred to the process of operational risk management as part of the undertakings' overall risk management.

Guideline 4 - Audit

17. Undertakings' governance, systems and processes for its ICT and security risks should be audited on a periodic basis in line with the undertakings' audit plan[12] by auditors with sufficient knowledge, skills and expertise in ICT and security risks to provide independent assurance of their effectiveness to the AMSB. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

Guideline 5 – Information security policy and measures

18. Undertakings should establish a written information security policy which should define the high-level principles and rules to protect the confidentiality, integrity and availability of undertakings' information in order to support the implementation of ICT strategy

19. The policy should include a description of the main roles and responsibilities for information security management and it should set out the requirements for staff, processes and technology in relation to information security, recognising that staff at all levels have responsibilities in ensuring undertakings' information security.

20. The policy should be communicated within the undertaking and should apply to all staff. Where applicable and relevant, the information security policy or parts of it should also be communicated and applied to service providers.

21. Based on this policy, undertakings should establish an information security function (see Guideline 6), establish and implement more specific information security procedures and information security measures to, inter alia, mitigate the ICT and security risks that they are exposed to. These procedures and information security measures should include every process described in these Guidelines where applicable.

Guideline 6 - Information security function

22. Undertakings should establish, within their system of governance and in accordance with the proportionality principle, an information security function, with the responsibilities assigned to a designated person. The undertaking should ensure the independence and objectivity of the information security function by appropriately segregating it from ICT development and operations processes. The function should report directly to the AMSB.

[12] Article 271 of the Delegated Regulation

23. The information security function is typically:

a) defining and maintaining the information security policy for undertakings and control its deployment;

b) report and advise the AMSB regularly, and on an ad hoc basis as needed, on the status of information security and its developments;

c) monitor and review the implementation of the information security measures;

d) ensure that the information security requirements are adhered to when using service providers; and

e) ensure that all employees and service providers accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions.

f) coordinate operational or security incident examination and report relevant ones to the AMSB.

Guideline 7 – Logical security

24. Undertakings should define, document and implement procedures for logical access control or logical security (identity and access management) in line with the protection requirements (as defined in Guideline 3). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. The procedures for logical security should, at a minimum, implement the following elements, where the term 'user' also comprises technical users:

a) need-to-know, least privilege and segregation of duties: undertakings should manage access rights, including remote access to information assets and their supporting systems on a 'need-to-know' basis. Users should be granted the minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to data or that the allocation of combinations of access rights may be used to circumvent controls (principle of 'segregation of duties').

b) user accountability: undertakings should limit, as much as possible, the usage of generic and shared user accounts and ensure that users can be identified and traced back to a responsible natural person or an authorised task for the actions performed in the ICT systems at all times.

c) privileged access rights: undertakings should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access (e.g. administrator accounts).

d) remote access: In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.

e) logging of user activities: users' activities should be logged and monitored in a risk proportionate manner, comprising privileged users' activities at a minimum. Access logs should be secured to prevent unauthorised modification or deletion and shall be retained for a period in line with the criticality of the identified business functions, supporting processes and information assets, without prejudice to the retention requirements set out in EU and national

law. Undertakings should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of services.

f) access management: access rights should be granted, removed and modified in a timely manner, according to predefined routines for approval where the applicable information asset owner is involved. In case access is no longer required, access rights should be promptly withdrawn/removed.

g) access assessment: access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn/removed when no longer required.

h) the granting, modification, withdrawal/removement of access rights should be documented in a way that facilitates comprehension and analysis.

i) Authentication methods: undertakings should enforce robust authentication methods to ensure that access control documentation procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed, and the privileges of the user. In order to ensure secure communication and reduce risk, at least in the case of remote administrative access to critical ICT systems, strong authentication solutions should be used. These methods may include password complexity requirements and/or other authentication methods.

25. Electronic access by applications to data and ICT systems should be limited to the minimum required to provide the relevant service.

Guideline 8 – Physical security

26. Undertakings' physical security measures (e.g. protection against power failure, fire, water and unauthorised physical access) should be defined, documented and implemented to protect its premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

27. Physical access to ICT systems should be permitted only to authorised individuals. Authorisation should be assigned in accordance with the individuals' tasks and responsibilities, limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly withdrawn / removed when not required.

28. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

Guideline 9 – ICT operations security

29. Undertakings should implement procedures to ensure the confidentiality, integrity and availablility of ICT systems and ICT services in order to respectively minimise the impact of security issues on ICT service delivery. These procedures should include, at least, the following measures:

a) identification of potential vulnerabilities which should be evaluated and remediated by ensuring that ICT systems are up-to-date, including the software provided by undertakings to its internal and external users, by

deploying critical security patches including antivirus definitions updates or by implementing compensating controls;

b) implementation of secure configuration baselines for all critical components such as operating systems, databases, routers or switches;

c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic;

d) implementation of protection of endpoints including servers, workstations and mobile devices. Undertakings should evaluate whether an endpoint meets the security standards defined by undertakings before it is granted access to the corporate network;

e) ensuring that integrity-checking mechanisms are in place to verify the integrity of ICT systems;

f) encryption of data at rest and in transit.

Guideline 10 – Security monitoring

30. Undertakings should establish, implement and document procedures to detect anomalous activities that may impact undertakings' information security, and to respond to these events appropriately. As part of this continuous monitoring, undertakings should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover, at least, the following:

a) internal and external factors, including business and ICT administrative functions;

b) transactions resulting from misuse of access by service providers or other entities and internal misuse of access; and

c) potential internal and external threats.

31. Undertakings should establish and implement processes and organisational structures to identify and constantly monitor security threats that could materially affect their ability to maintain services. Undertakings should implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware.

32. The security monitoring process should also help undertakings to understand the nature of operational or security incidents, to identify trends and to support the undertaking's internal investigations.

Guideline 11 – Information security reviews, assessment and testing

33. Undertakings should perform a variety of different information security reviews, assessments and testing, so as to ensure effective identification of vulnerabilities in its ICT systems and services. For instance, undertakings may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews.

34. Undertakings should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers threats and

vulnerabilities, identified through threat monitoring and the ICT and security risk assessment process.

35. This information security testing framework should ensure that tests are proportionate to the level of risk identified and are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures.

36. The tests should include vulnerability scans and penetration tests (including threat led penetration testing where necessary and appropriate), carried out in a safe and secure manner. Tests should be performed on a regular basis and for critical ICT systems at least annualy

37. Undertakings should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed critical applications. Undertakings should monitor and evaluate results of the security tests, and update their security measures accordingly without undue delays in case of critical ICT systems.

Guideline 12 – Information security training and awareness

38. Undertakings should establish an information security training programme for all staff, including AMSB, to ensure that they are trained to perform their duties and responsibilities to reduce human error, theft, fraud, misuse or loss. Undertakings should ensure that the training programme provides training for all staff on a regular basis.

39. Undertakings should establish and implement periodic security awareness programmes to educate their staff, including the AMSB, on how to address information security related risks.

Guideline 13 – ICT operations management

40. Undertakings should manage their ICT operations based on the ICT strategy. Documents should define how undertakings operate, monitor and control the ICT systems and ICT services, including documenting critical ICT operations.

41. Undertakings should implement logging and monitoring procedures for critical ICT operations to allow for detection, analysis and correction of errors.

42. Undertakings should maintain an up-to-date inventory of their ICT assets. The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification, and ownership.

43. Undertakings should monitor and manage the lifecycle of ICT assets to ensure that they continue to meet and support business and risk management requirements. Undertakings should monitor that the ICT assets are supported by their vendors or in-house developers and that all relevant patches and upgrades are applied based on a documented process. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated. Decommisioned ICT assets should be safely destroyed.

44. Undertakings should implement performance and capacity planning and monitoring process to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

45. Undertakings should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set in line with business recovery requirements and the criticality of the data and the ICT systems, evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be performed on a regular basis.

46. Undertakings should ensure that data and ICT system backups are stored in one or more locations out of the primary site, which are secure and sufficiently remote from the primary site so as to avoid being exposed to the same risks.

Guideline 14 - ICT incident and problem management

47. Undertakings should establish and implement an incident and problem management process to monitor and log operational or security incidents and enable undertakings to continue or resume critical business functions and processes when disruptions occur.

48. Undertakings should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.

49. To minimise the impact of adverse events and enable timely recovery, undertakings should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents to make sure that the root causes are identified and eliminated in order to prevent the occurrence of repeated incidents. The incident and problem management process should, at least, establish:

a) the procedures to identify, track, log, categorise and classify incidents according to a priority defined by the undertaking and based on business criticality and service agreements;

b) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber attacks);

c) a problem management procedure to identify, analyse and solve the root cause behind one or more incidents - undertakings should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. Undertakings should consider key lessons learned from these analyses and update the security measures accordingly;

d) effective internal communication plans, including incident notification and escalation procedures - covering also security-related customer complaints - to ensure that:

   i. incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management;

   ii. the AMSB is informed on an ad-hoc basis in case of significant incidents and at least informed of the impact, reaction and additional controls to be defined because of the incidents.

e) incident response procedures to mitigate the impact related to the incidents and to ensure that the service becomes operational and secure in a timely manner;

f) specific external communication plans for critical business functions and processes in order to:

   i. collaborate with relevant stakeholders to effectively respond to and recover from the incident;

   ii. provide timely information, including incident reporting, to external parties (e.g. customers, other market participants, the relevant (supervisory) authority, as appropriate and in line with an applicable regulation).

Guideline 15 – ICT project management

50. Undertakings should implement a ICT project methodology (including independent security requirement considerations) with an adequate governance process and project implementation leadership to effectively support the implementation of the ICT strategy through ICT projects.

51. Undertakings should appropriately monitor and mitigate risks deriving from the portfolio of ICT projects, considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

Guideline 16 - ICT systems acquisition and development

52. Undertakings should develop and implement a process governing the acquisition, development and maintenance of ICT systems in order to ensure the confidentiality, integrity, availability of the data to be processed are comprehensibly assured and the defined protection requirements are met. This process should, at least, include:

   a) setting objectives during the development phase;

   b) technical implementation (including secure coding/programming guidelines);

   c) quality assurance standards; and

   d) testing, approval and release, irrespective of whether the development is done in house or externally by a service provider.

53. Undertakings should ensure that before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements), technical specifications are clearly defined.

54. Undertakings should ensure that measures are in place to prevent unintentional alteration or intentional manipulation of the ICT systems during development.

55. Undertakings should have a methodology in place for testing and approval of ICT systems, ICT-services and information security measures.

56. Undertakings should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

57. Undertakings should ensure segregation of production environments from development, testing and other non-production environments.

58. Undertakings should implement measures to protect the integrity of source code (where available) of ICT systems. They should also document the development, implementation, operation, and/or configuration of the ICT systems in a

comprehensive manner to reduce unnecessary dependency on subject matter experts.

59. Undertakings' processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside of the ICT organisation (e.g. business managed applications or end user computing applications) in a risk based approach. The undertakings should maintain a register of these applications that support critical business functions or processes .

Guideline 17 - ICT change management

60. Undertakings should establish and implement an ICT change management process to ensure that all changes to ICT systems are assessed, tested, approved and implemented in a controlled manner. The ICT change management process should contain, at least, the following elements:

a) a process for recording all change requests to ICT systems;

b) an evaluation, testing, and approval process for all change requests to ICT systems. Specifically, undertakings should evaluate the impact of the proposed changes and the potential implementation risks (e.g. compatibility and security). Following approval, the process should include a formal acceptance of any new residual risks;

c) an authorisation process, only after which ICT changes move to production. This authorisation process should be undertaken by responsible personnel in such a way that a rollback can be performed in case of a malfunction;

d) a process for urgent or emergency ICT changes. Such changes should be traceable and notified ex-post to the relevant asset owner for ex-post analysis;

e) a process to update ICT systems' documentation to reflect the changes carried out, where necessary.

Guideline 18 – Business continuity management

61. The AMSB has the responsibility for setting and approving the undertakings' ICT continuity policy, as part of the undertakings overall business continuity policy. The ICT continuity policy should be communicated appropriately within undertakings and should apply to all staff and if relevant, to service providers.

Guideline 19 – Business impact analysis

62. As part of a sound business continuity management, undertakings should conduct a business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impact, quantitatively and qualitatively, using internal and/or external data and scenario analysis. The BIA should also consider the criticality of the identified and classified business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets) , and their interdependencies in accordance with Guideline 3.

63. Undertakings should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

Guideline 20 – Business continuity planning

64. The overall Business Continuity Plans (BCP) of the undertaking should consider material risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets. Undertakings should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

65. Undertakings should put BCPs in place to ensure that they can react appropriately to potential failure scenarios within a Recovery Time Objective (RTO, the maximum time within which a system or process must be restored after an incident) and a Recovery Point Objective (RPO, the maximum time period during which data can be lost in case of an incident).

66. Undertakings should consider a range of different scenarios in their BCPs, including extreme but plausible scenarios and cyber-attack scenarios, and assess the potential impact that such scenarios might have. Based on these scenarios, undertakings should describe how continuity of ICT systems and services, as well as undertakings' information security, is ensured.

Guideline 21 – Response and recovery plans

67. Based on the BIA and plausible scenarios undertakings should develop response and recovery plans. These plans should specify what conditions may require activation of the plan and what actions should be taken to ensure the integrity, availability, continuity and recovery of, at least, undertakings' critical ICT systems, ICT services and data. The response and recovery plans should aim to meet the recovery objectives of undertakings' operations.

68. The response and recovery plans should consider both short-term and, if nessesary, long-term recovery options. The plans should, at least:

    a) focus on the recovery of the operations of important ICT services, business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of the undertaking;

    b) be documented and made available to the business and support units and readily accessible in case of emergency, including a clear definition of roles and responsibilities; and

    c) be continuously updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

69. The plans should also consider alternative options where recovery may not be feasible in the short term because of cost, risks, logistics, or unforeseen circumstances.

70. As part of the response and recovery plans, undertakings should consider and implement continuity measures to mitigate failure of service providers, which are of key importance for undertakings' ICT service continuity (in line with the provisions

of EIOPA Guidelines on System of Governance and Guidelines on outsourcing to cloud service providers[13]).

Guideline 22 – Testing of plans

71. Undertakings should test their BCPs, and ensure that the operation of their critical business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets and their interdependencies (including those provided by service providers) are tested regularly based on the undertakings risk profile..

72. BCPs should be updated regularly, based on testing results, current threat intelligence and lessons learned from previous events. Any relevant changes in recovery objectives (including RTO and RPO) and/or changes in business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets, should also be included.

73. Undertakings' testing of their BCPs should demonstrate that they are capable of sustaining the viability of the business until critical operations are re-established.

74. Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the AMSB.

Guideline 23 - Crisis communications

75. In the event of a disruption or emergency, and during the implementation of the BCPs, undertakings should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the relevant competent authorities when required by regulation, and also relevant service providers, are informed in a timely and appropriate manner.

Guideline 24 – Outsourcing of ICT systems and ICT services

76. Without prejudice to the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-19/270[14]) undertakings should ensure that in cases where ICT services and systems are outsourced - irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service - the relevant requirements for the service or system should be met.

77. Undertakings should ensure that contracts and service level agreements with the service provider include, at least, the following:

    a) appropriate and proportionate information security objectives and measures including requirements such as minimum information security requirements, specifications of undertakings' data life cycle, audit and access rights and any requirements regarding location of data centres and data encryption requirements, network security and security monitoring processes;

[13] Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers EIOPA-BoS-19/270 1 July 2019 / to be updated after consultation

[14] To be updated after consultation

b) service level agreements, to ensure continuity of ICT services and systems and performance targets under normal circumstances as well as those provided by contingency plans in the event of service interruption; and

c) operational and security incident handling procedures including escalation and reporting.

78. Undertakings should monitor and seek assurance on the level of compliance of these service providers with their security objectives, measures and performance targets.

3 Compliance and reporting rules

79. This document contains Guidelines issued under Article 16 of Regulation (EU) No 1094/2010. In accordance with Article 16(3) of that Regulation, competent authorities and undertakings are required to make every effort to comply with Guidelines and recommendations.

80. Competent authorities that comply or intend to comply with these Guidelines should incorporate them into their regulatory or supervisory framework in an appropriate manner.

81. Competent authorities need to confirm to EIOPA whether they comply or intend to comply with these Guidelines, with reasons for non-compliance, within two months after the issuance of the translated versions.

82. In the absence of a response by this deadline, competent authorities will be considered as non-compliant to the reporting and reported as such.

4 Final provision on review

83. The present Guidelines will be subject to a review by EIOPA.

Annex I: Impact Assessment

Section 1 – Procedural issues and consultation of interested parties

1. In accordance with Article 16 of EIOPA Regulation, EIOPA conducts analyses of costs and benefits in the policy development process. The analysis of costs and benefits is undertaken according to an Impact Assessment methodology.
2. The draft Guidelines and its Impact Assessment are envisaged to be subject to a public consultation. Stakeholders' responses to public consultation will serve as a valuable input in order to revise the Guidelines.

Section 2 – Problem definition

3. As already highlighted by the EIOPA report "Cyber risk for insurers – Challenges and Opportunities"15, Having clear, comprehensive and common requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. As indicated by the feedback received from the industry, a good number of undertakings is aware of the potential cyber threats and have incorporated cyber risk explicitly in their risk management frameworks. Further actions to strengthen the resilience of the insurance sector against cyber vulnerabilities are essential, in particular considering the dynamic nature of cyber threats. This would include streamlining of the cyber incident reporting frameworks across the insurance and financial sector, to avoid inconsistencies in the reported information and ultimately enhance operational resilience. Therefore, action is needed to strengthen the resilience of the insurance sector against cyber vulnerabilities, considering in particular the dynamic nature of cyber threats. The insurance sector needs to have some guidance at hand regarding how to build a sound cyber resilience framework. In particular, there seems to be a lack of clear, comprehensive and common requirements with respect to the governance of cybersecurity as part of operational resilience.
4. Furthermore, it is necessary to build a level playing field on which standards and approaches adopted by the national competent authorities do not contribute to enlarge the currently existing scattered landscape, also cross-sectorally speaking. Such an option would generate many negative impacts on the (re)insurance sector regarding, for example:
    - Uncoordinated supervisory practices diverging from the common supervisory culture,
    - Weak resilience and poorly developed strategies that can lead to higher probability of occurrence for systemic events,
    - Lack of coherence with similar initiatives launched in the banking sector
    - etc.
5. EIOPA identified the above mentioned needs in the context of the analysis performed to answer the European Commission FinTech Action plan (COM(2018) 109 final) and following interactions with several other stakeholders.

[15] https://eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf

6. The work carried out by EIOPA highlighted the following main areas that need to be clarified:
   - Outlining the relevant definitions as the basis to set out a minimum cyber resilience framework
   - Identifying the sinergies between ICT governance and the system of governance in general
   - Identifying the sinergies between ICT risks and the Risk Management System in general
   - Identifying the sinergies between the content of the EIOPA Guidelines on ICT security and Governance and the EIOPA Guidelines on outsourcing to cloud service providers
   - Application of audit, access (taking into account both logical and physical security) and security requirements to ICT
   - Incident and crisis management
   - Business continuity and recovery planning and testing
7. Moreover, taking into account the work carried out by the European Banking Authority (EBA) in the fields of Guidelines on ICT security and risk management16, another gap that these draft Guidelines aim to address is the lack of guidance for the regulatory framework and supervisory assessment of risks connected to ICT security in EU insurance and reinsurance undertakings. Inconsistency in the treatment of potential ICT risks and cyber threats in general may also lead to an uneven playing field across jurisdictions.
8. When analysing the impact from proposed policies, the impact assessment methodology foresees that a baseline scenario is applied as the basis for comparing policy options. This helps to identify the incremental impact of each policy option considered. The aim of the baseline scenario is to explain how the current situation would evolve without additional regulatory intervention.
9. For the analysis of the potential related costs and benefits of the proposed Guidelines, EIOPA has applied as a baseline scenario the effect from the application of the current general requirements on governance and risk management in the Solvency II framework, including:
   - Articles 41, 44, 46, 47, 41, and 246 of the Solvency II Directive;
   - Articles 258, 259, 260, 266, 268 to 271 and 274 of the Solvency II Delegated Regulation; and
   - EIOPA Guidelines on System of Governance, supplemented by EIOPA Guidelines on Outsourcing to Cloud Service Providers.

Section 3 – Objectives pursued

10. The objective of these Guidelines is to:

[16] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

a) provide clarification and transparency to market participants on the minimum expected information technololology and cyber security capabilities, i.e. security baseline;

b) avoid potential regulatory arbitrage;

c) foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT risk management.

11. The mentioned objectives for the Guidelines are connected to the general objectives of the Solvency II framework (deepen the integration of the EU insurance market, enhance the protection of policyholders and beneficiaries and promote better regulation) and in particular they are connected to:

- the improvement of governance and risk management for insurance and reinsurance undertakings;
- the harmonisation of supervisory methods; and
- the promotion of consistency of prudential supervision of insurance and banking.

12. The objectives of the Guidelines are also consistent with the following objectives of EIOPA, as reflected in the Regulation of the Authority:

- ensure a sound, effective and consistent level of regulation and supervision;
- ensure the taking of risks related to (re)insurance activities is appropriately regulated and supervised; and
- consumer protection.

Section 4 – Policy Options

13. With the aim to meet the objectives set out in the previous section, EIOPA has analysed different policy options throughout the policy development process.

14. The section below reflects the most relevant policy options that have been considered in relation to the different aspects associated to the building up of a minimum baseline for cyber security and resilience. We have also listed relevant options which have been discarded in the policy development process.

Policy issue 1: Introduction of the Guidelines versus the status quo

15. Policy option 1.1 Introduction of EIOPA Guidelines on ICT security and Governance to provide clarity on how the minimum expectations for cyber security shall be built in (re)insurance undertakings.

16. Policy option 1.2 Keeping the status quo not issuing any guidance on the subject.

Policy issue 2: Development of dedicated Guidelines on ICT security and governance versus development of more detailed Guidelines on system of governance as a whole

17. Policy option 2.1 Development of standalone EIOPA Guidelines on ICT security and governance (taking as example the work done by EBA)

18. Policy option 2.2 Inclusion of the Guidelines on ICT security and governance in the already existing Guidelines on the system of Governance.

Section 5 – Analysis of the impacts

Policy issue 1: keeping the status quo versus issuing new Guidelines on ICT security and governance

Policy option 1.1 Keeping the status quo not issuing any guidance on the subject.

19. EIOPA believes that without the introduction of the additional guidance the current set of Guidelines on the system of governance fail to provide an adequate regulatory and supervisory framework for (re)insurance undertakings and the competent authorities in their handling of the daily business, which is inevitably supported by IT systems, in the (re)insurance sector.

20. Moreover, without the issuance of guidance on the subject the entire industry faces the risk to develop non-homogenous practices and apply them in a non-homogeneous pattern harming the goal of achieving a level playing field with respect to ICT security and governance.

21. Finally, given the systemic nature of cybe threats, not issuing proper guidance on the topic could increase the impact of operational risks overall for the entire industry, with potential impacts on policyholders.

Policy option 1.2 Introduction of EIOPA Guidelines on ICT security and Governance to provide clarity on how the minimum baseline for cyber security shall be built in (re)insurance undertakings.

22. On the basis of the analysis performed by EIOPA to answer the European Commission FinTech Action plan, taking into account the work already performed by the EBA and the fact that some jurisdictions have issued or plan to issue guidance on ICT security and governance and more generally on ICT security and risk

management, EIOPA has identified the existence of some room for potential regulatory arbitrages as risks for the market participants. Moreover, EIOPA has identified several specific risks associated to ICT security and governance that these Guidelines aim at mitigating.

23. Particularly, EIOPA is the opinion that the introduction of new Guidelines on ICT security and governance, also aligned with the work already done by EBA:

a) supports the (re)insurance undertakings in their prudent management of ICT risks;

b) provides a coherent minimum expectations on ICT security and governance for (re)insurance undertakings as much as possible aligned to the one proposed for the banking sector and impacting on banking and payment institutions;

c) maximises the investments made in terms of supervisory skills and knowledge by the national supervisory authorities who supervise, in addition to banking and payment institutions, also (re) insurance undertakings;

d) increases the protection of the policyholders providing a common set of expectations towards digital information assets wich are coherent with other relevant regulation (e.g. General Data Protection Regulation – GDPR).

e) In terms of cost of compliance with the Guidelines, it is reasonable to expect that the jurisdictions where the current practices overlap or show similarities with what is proposed in the Guidelines will bear less administrative cost both for the undertakings and the competent authorities. This is expected particularly for those jurisdictions where the competent authorities are jointly supervising the banking and insurance sector. On the other hand, potential additional costs for the industry could be expected due to specific IT requirements put in place to grant compliance with the minimum baseline set by the Guidelines.

Policy issue 2: Development of standalone Guidelines on ICT security and governance versus inclusion of the ICT security and governance Guidelines in the already existing EIOPA Guidelines on the system of governance

24. As reported above, while performing its internal assessment on the development of these Guidelines, EIOPA has taken into account the work carried out by the EBA in the fields of the system of governance in general and, more in detail, ICT security and governance.

25. On the basis of the results of the internal assessment, EIOPA believes that the risks arising from the usage of IT Systems for the day-to-day activities by (re)insurance undertakings are, generally, aligned to the risks insisting on banking players with few minor (re)insurance specificities.

26. The analysis of impacts on the Policy issue nr.2 takes into account the above.

Policy option 2.1 Development of dedicated standalone EIOPA Guidelines on ICT security and governance (taking as example the work done by EBA).

27. It must be acknowledged that ICT governance has some conceptual differences from the regular arrangements regarding the overall system of governance. However, full consistency when applicable needs to be ensured between both documents while not repeating System of Governance Guidelines.

28. The issuance of specific guidance on ICT security and governance gives the possibility to provide clarity and homogeneity across member states on how to apply a minimum baseline for ICT risks, while also minimising the impacts on (re)insurance undertakings.

29. In order to avoid inconsistencies between the banking and the insurance sector, the Guidelines build on the EBA Guidelines on ICT security risk management.

Policy option 2.2 Inclusion of the Guidelines on ICT security and governance in the already existing Guidelines on the system of Governance.

30. However, the issuance of more detailed Guidelines on governance arrangements, poses the risk of potential more significant implementation costs for the insurance undertakings as new provisions might not only require to re-assess the governance arrangements in place, but also to put in place compliance activities specifically meant to cover ICT risk items.

31. The following table summarises the main costs and benefits of the analysed options for for stakeholders, including policyholders, industry and supervisors.

Policy issues 1 to 2: Guidelines on ICT security and governance		
Option 1.1: Keeping the status quo not issuing any guidance on the subject		
Costs	Policyholders	No additional costs are foreseen as the framework is kept as of today
	Industry	As the general governance and risks management arrangements are already in place and stably established no additional direct costs are envisaged. However, given the continuously changing nature of cyber threats and the systemic nature of ICT risks, increasing costs are foreseen to arise in the long run.
	Supervisors	Additional costs might arise in case ad-hoc information is needed in the newly identified areas for which information is needed regarding ICT risks that go beyond the regular governance and risk management arrangements currently in place in (re)insurance undertakings. Supervisory resources might not be used in an optimal way.
	Other	N/A
Benefits	Policyholders	No material impact as the status quo will be kept
	Industry	No material impact as the status quo will be kept
	Supervisors	No material impact as the status quo will be kept
	Other	N/A
Option 1.2: Introduction of EIOPA Guidelines on ICT security and Governance to provide clarity on how the minimum baseline for cyber security shall be built in (re)insurance undertakings.		
Costs	Policyholders	No material impact
	Industry	The application of new guidance on ICT security and governance is foreseen to complete the currently existing governance and risk management

		arrangements and might lead to one off costs on a first stage with regard to further investments on ICT security, restructuring of existing processes and procedures and staff training. Adaptation of systems in the future are likely to lower the overall likelihood to incur in disproportionate costs caused by cyber incidents.
	Supervisors	Some potential costs are envisaged to adequately train staff on ICT topics and to set out new supervisory activities related to ICT governance supervision.
	Other	N/A
Benefits	Policyholders	Principles set out in the ICT security and governance Guidelines are also in line other relevant regulation which has been excluded from the scope of the Guidelines (e.g. General Data Protection Regulation - GDPR). Adaptation of systems in the future are likely to lower the overall likelihood to incur in disproportionate costs caused by cyber incidents.
	Industry	Expenses incurred to comply with new expectations to meet the guidelenes are likely to produce benefits to the overall risk management framework and the overall governance as applied to ICT risks in the long run. Adaptation of systems in the future are likely to lower the overall likelihood to incur in disproportionate costs caused by cyber incidents.
	Supervisors	Enhanced risk based supervision. Adaptation of systems in the future are likely to lower the overall likelihood to incur in disproportionate costs caused by cyber incidents.
	Other	Initiative in line with the objectives set out by the European Commission regarding the importance of Cyber Resilience. Furthermore, with regard to the whole (re)insurance sector, an increase in the cyber resilience of a single undertaking also benefits and increases the resilience of the sector as a whole
Option 2.1: Development of dedicated standalone EIOPA Guidelines on ICT security and governance (taking as example the work done by EBA).		
Costs	Policyholders	No material impact
	Industry	Some initial costs might be estimated to reflect the specific assessment of ICT risks. In long term the cost burden is likely to be reduced in proportion to the initial costs incurred to set up the new arrangements.
	Supervisors	Some potential costs are envisaged following the need to appropriately train supervisors with reference to ICT-related topics.
	Other	N/A
Benefits	Policyholders	
	Industry	Cross-sectoral consistency and increased coherence with the provisions set out in other relevant regulations excluded from the scope of the Guidelines on ICT security and governance (e.g. GDPR). Furthermore, a

		new standalone set of Guidelines provide more clarity and details on ICT and are expected to be easier to be implemented.
	Supervisors	Supervisors have a bigger overview of governance arrangements, also related to ICT risks and in line with their relevant guidance (e.g. EIOPA Guidelines on: system of governance, outsourcing to the cloud, etc.)
	Other	Initiative in line with the objectives set out by the European Commission regarding the importance of Cyber Resilience
Option 2.2: Inclusion of the Guidelines on ICT security and governance in the already existing Guidelines on the system of Governance		
Costs	Policyholders	No material impact
	Industry	Some initial costs might be estimated to reflect the specific assessment of ICT risks. In long term the cost burden is likely to be reduced in proportion to the initial costs incurred to set up the new arrangements.
	Supervisors	Some potential costs are envisaged following the need to separate the general information on governance arrangements and the overall system of governance of (re)insurance undertakings.
	Other	N/A
Benefits	Policyholders	No material impact
	Industry	Might be easier to incorporate the concepts of the new ICT guidelines in the context of Solvency II
	Supervisors	Possibility to have lower need for specific ICT training and to rely on a join team for the overall governance assessment of (re)insurance undertakings.
	Other	N/A

Section 6 – Comparison of options

32. Regarding policy options 1.1 and 1.2 on the basis of the previous section, **EIOPA has chosen policy** option 1.2 "Introduction of EIOPA Guidelines on ICT security and governance" to provide clarity on how ICT risks should be dealt specifically in the broader context of governance arrangements and overall risk management.

33. Regarding policy options 2.1 and 2.2 on the basis of the previous section and considering the preparatory analysis performed in the context of developing its answer to the European Commission FinTech Action Plan, EIOPA has chosen policy option 2.1 "Development of dedicated standalone EIOPA Guidelines on ICT security and governance (taking as example the work done by EBA)". This option has been preferred to ensure cross-sectoral consistency.

Section 7 – Summary of other cost and benefit-related issues

34. With regard to other topics worth mentioning, the envisaged costs might also include, depending on the level of cyber resilience maturity in undertakings, staff

training, adaptation needs of internal processes (e.g. storage of documentation regarding Information Security policy, etc.), setting up a new function, etc.

35. On the other hand, these costs are counterbalanced by a deeper understanding of processes linked to ICT, a higher level of awareness across staff, a revised organisational structure able to coordinate and enhance undertakings' cyber resilience profile and ultimately to undertakings better prepared to mitigate the consequence of cyber attacks.