Position Paper

Response to EIOPA consultation on the proposal for Guidelines on information and communication technology (ICT) security and governance

Our reference:	EXCO-CS-20-020	Date:	13 March 2020
Referring to:	EIOPA consultation paper on the proposal for Guidelines on information and communication technology (ICT) security and governance		
Contact person:	Áine Clarke, Policy Advisor	E-mail:	Clarke@insuranceeurope.eu
Pages:	24	Transparency Register ID no.:	33213703459-54

Key points

- The proposed timeline for the application of the guidelines is too short, as it does not allow a reasonable time for transposition at national level and for undertakings to react, should they need to review their compliance.
- EIOPA should avoid adopting a one-size-fits all approach to ICT security and governance, rather favouring a risk-based approach.
- The principle of proportionality must be clearly incorporated into the guidelines, which should be applied in proportion with the nature and scale of ICT operations stemming from an undertaking's business profile.
- There is a need to ensure that there is no duplication of efforts in the area of ICT security and governance, given the many ongoing initiatives in this area. EIOPA should focus rather on areas where additional guidelines could prove to be of added value.

General comments

- Regarding the general content of the Guidelines, the quality and adequacy of the content of the guidelines should be favoured over the speed at which they are introduced. In this regard, Insurance Europe would welcome an opportunity to provide comments on a second draft of EIOPA's proposed Guidelines. Insurance Europe also notes that, while EIOPA's Guidelines mirror, to a large extent, the content of similar EBA Guidelines, in many areas they go beyond the EBA's guidelines, which appear more principle-based. As a result, the EBA's Guidelines take less of a 'one-size-fits-all' approach. It is our view that EIOPA should give due consideration to the distinctive nature of the business of insurance, when compared with the business of banking, and ensure that the Guidelines are in line with the ICT security risks in insurance (which are, in many respects, less critical than those found in banking).

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

- EIOPA's proposed guidelines are one of a number of proposals for regulation in this area. Insurance Europe stresses the importance of **alignment** between EIOPA's and the European Commission's initiatives[1], in order to avoid overlap and compliance issues. Insurance Europe notes that the consultation launched by the European Commission, on a digital operational resilience framework for financial services, is aimed at establishing one framework to cover the entire financial sector, however it is unclear how this will be achieved in practise, considering, in particular, that both the content and the definitions given in EIOPA's guidelines differ from those of the EBA's. In this regard, EIOPA should consider the results of the EC's consultation when finalising its own guidelines on ICT security and governance. Due consideration must also be made for the work being carried out in parallel on cyber resilience, threat led penetration testing and certification of critical cloud vendors, as any outcomes will undoubtedly impact on the ICT security and governance of (re)insurers. Clarification of how the various EU-level initiatives will interact in practise is necessary.

- The **proposed timeline** for the application of the guidelines is too short, as it does not allow a reasonable time for transposition at national level and for undertakings to react, should they need to review their compliance. The approach taken by the EBA in its Guidelines on ICT and security risk management is preferred (Consultation launched December 2018; Final Guidelines published 28 November 2019; Guidelines must be applied by 30 July 2020). The date of application must be extended to 30 July 2021, at the earliest.

- Although it is referred to in the introduction, the **principle of proportionality** is not sufficiently incorporated into the guidelines. Given that the scale and nature of an entity's activity has a direct impact on ICT security management, this principle should be explicitly recognised in an introductory guideline, stating that the principles outlined in the document should be applied in proportion with the nature and scale of ICT operations stemming from an undertaking's business profile. A practical articulation of proportionality and/or reference to this introductory principle throughout the guidelines, when appropriate, would greatly assist in the implementation of and compliance with these guidelines.
    - Compare the EBA's Guideline 1 on 'Proportionality': "All financial institutions should comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, the financial institutions' size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide". The EBA's approach is preferred.

- The proposed guidelines combine principles for information security and measures for IT security, however there is a lack of clear distinction between principles that *should* be applied following a risk-based approach and measures that *could* be applied based on the specific risk and criticality. We suggest that wherever there are principles that should be applied, wording such as "these procedures should include, at least, the following measures" be replaced with the following wording: "these procedures should consider the following measures…". The former may be interpreted as minimum requirements, thereby unnecessarily limiting organizations' freedom to implement procedures and measures they deem suitable to mitigate different kinds of risks. A more detailed explanation can be found in the comments on Guideline 9.29.

- **Interaction with Solvency II and its Delegated Acts** - In some areas, the Guidelines go beyond the legal requirements instead of merely concretising them and/or expand the scope of activities and services beyond those covered by Solvency II and its Delegated Acts. This can be seen in Guideline 3 on ICT and security risks within the risk management system, which assigns responsibilities to ASMBs which do not fall within their scope, including the task of establishing an effective system for managing ICT and security risks within the undertaking. The creation of any new requirements must

[1] See: European Commission consultation on a Digital Operational Resilience Framework for financial services; European Commission roadmap "Shaping Europe's digital future", which refers to a review of the NIS Directive.

be avoided, as it risks imposing undue burden on entities and moving away from a level playing field. The guidelines should therefore focus instead on particular aspects of ICT security and governance, as laid out in existing requirements, which necessitate further clarification. EIOPA must also ensure that all definitions used in the guidelines are consistent with those found in Solvency II and its Delegated Acts.

- **National transposition** – NSAs are at various stages when it comes to issuing national guidelines on ICT security and governance; some have already done so, and others are in the process of doing so. It must be clarified how EIOPA's guidelines will interact with the guidelines of NSAs, in order to ensure their coordinated implementation across all Member States. In addition, the transposition of EIOPA's guidelines at national level must take into account the existing security requirements on insurers in markets where they have been designated as "operators of essential services" by their national governments, during the transposition process of the NIS Directive into national law. An excessive fragmentation of ICT security requirements must be avoided.

- **Consideration of well-known and used industry standards** is necessary (i.e. ISO 27000-series on information security), not least for the definitions used. In this regard, Insurance Europe supports a supervisory approach based on measurement against globally recognised industry benchmarks, rather than the development of an additional dedicated approach.

- **Alignment with other EIOPA Guidelines** is essential to avoid confusion and complexity in compliance. Here, we refer in particular to Guidelines on System of Governance (2013) and Guidelines on Outsourcing to Cloud Service Providers (2020).

- **Consideration of different insurance business models:** EIOPA's proposed guidelines appear to have been drafted with large self-managed undertakings in mind, who own their own ICT assets and processes and have sufficient oversight and control over such assets to effectively manage and implement ICT security and governance processes and procedures. However, (re)insurance entities are not uniform in the nature, scale and complexity of their business models. Smaller undertakings, such as captive (re)insurance companies ("captives"), which operate a fully outsourced model, outsource all key functions and processes and do not have any staff. As such, these undertakings rely on the ICT assets, ICT systems and ICT processes of their outsourced service provider. Under Article 274 of Commission Delegated Regulation (EU) No 2015/357, captives and other small undertakings operating a fully outsourced model must have an outsourcing agreement in place with the outsourced service provider. The outsourcing agreement must ensure that the service provider has adequate contingency plans in place to deal with emergency situations or business disruptions and periodically tests backup facilities where necessary, taking into account the outsourced functions and activities. As such, captives and other smaller undertakings operating a fully outsourced model would not have sufficient access to and oversight of the ICT assets, systems and processes of the outsourced service provider to effectively implement EIOPA's proposed guidelines. We believe that the requirements of GDPR and (EU) No 2015/357, which apply to such undertakings who operate a fully outsourced model, provide sufficient protection. Considering this, Insurance Europe believes that these guidelines should only apply to those undertakings that own their own ICT systems and processes; and not to captive (re)insurance companies, and other undertakings with similar business models.

Introduction

1. In accordance with Article 16 of Regulation (EU) No 1094/20105 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/EC6 ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/357 ("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)

2. The Guidelines apply to both individual undertakings and mutatis mutandis at the level of the group.

- EIOPA should extend paragraph 2 to provide additional clarification on the scope and applicability of these guidelines.
- Regarding insurance groups, EIOPA should reconsider the application of the Guidelines at solo level versus group level. The usual mutatis mutandis approach, i.e. an application at entity level and on top of that at group level, is particularly ill-designed for those Guidelines as it would fail to recognize that IT systems and functions are mutualized across one group. The guidelines should seek to promote an efficient and agile ICT risk management instead of creating inefficient redundancies. For groups, the GLs should apply at group level first and part of them may be applied to the most relevant legal entities depending on the outcome of a risk-based assessment that takes account of both the subsidiarity and proportionality principles.

3. Supervisory authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality. 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

General Comments:

- Insurance Europe stresses the importance of consistency in the use of definitions in order for EIOPA to achieve its supervisory objectives. In this regard, alignment between the definitions employed in the various EU-level initiatives is essential to avoid confusion. Furthermore, EIOPA should ensure that any definitions are consistent with established industry standards (such as the ISO 2700 series).
- Some of the below definitions need further clarification. In certain cases, which are indicated below, the definitions included in the EBA's Guidelines on ICT security and risk management are preferred.
- As readers of this document are likely to include ICT professionals, each time EIOPA refers to terms which are already defined in previous EU regulation (such as "Undertaking", "proportionality" and "AMSB"), the definition should be recalled in the Guidelines.

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

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.

- What is meant by "cyber medium" must be clarified.

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.

- It must be clarified that the terms "security risk" and "physical security" used in this definition refer to the security/physical security of Information and ICT infrastructure. The current definition creates confusion as physical security can also cover workplace and employee security.
- In giving one single definition for both "ICT" and "security" risk, EIOPA is merging two risks of a different nature. The "inability to change ICT within a reasonable time and costs when the environment or business requirements change" is not necessariy a security risk. Providing a separate definition for "security risk" would align EIOPA's document with other legal references, such as the NIS Directive ("any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems").

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.

- Adding examples to this definition would provide further clarification. See the EBA's Guidelines.

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.

- This definition is inconsistent with industry definitions and could be confused with the definition of data quality. We would suggest "Property of being sensitive to inappropriate or accidental modification."

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.

- The current wording of this definition could lead to a differentiation between an "operational" incident and a "security" incident. Consequently, "security incident" would have to be defined. We suggest aligning this definition with the NIS Directive ("any event having an actual adverse effect on the security of network and information systems").
- The last part of the sentence should be modified to: "…, availability and/or confidentially…".

Service provider
Means a third party entity that is performing an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.

- We disagree with the suggested definition of "service provider", because a service provider does not always need to be part of an outsourcing arrangement, which EIOPA's definition would seem to imply. Instead, refer to EIOPA definition of "service provider" in its recently published Guidelines on outsourcing to cloud service providers, where "outsourced" is removed from the definition. Mirroring this would ensure alignment between EIOPA's Guidelines.

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

- The date of applicability does not allow a reasonable time for publication and for undertakings to react, should they need to review compliance. 01-07-2021 would be the earliest possible date of implementation for these comprehensive guidelines.

Guideline 1 - ICT within the system of governance

- EIOPA must ensure that any guidelines which outline the role of the AMSB (such as Guideline 1) leave sufficient room for the adaption of this role to the realities of the variety of corporate structures in place across different member states. With this in mind, we find it unnecessary to in this guideline specifically refer to corporate governance for ICT security risks, as corporate governance is covered elsewhere and should not unduly restrict organizations in choosing how to organize themselves. Point 15 of EIOPA's Guidelines on

System of Governance already states that: "the administrative, management or supervisory body of the undertaking is ultimately responsible for ensuring the effectiveness of the risk management system". ICT and security risks belong to the general risk management system and internal control system. Even if the AMSB has ultimate oversight and therefore has to approve the ICT strategy, it should not have to review the details of the undertaking's ICT and security risks.

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.

- This point goes beyond what is outlined in Article 258 of Solvency II's delegated act, on "General governance requirements", in which point 1.b specifies that it is the (re)insurance undertaking that must "establish, implement and maintain effective decision making procedures and an organisational structure which clearly specifies reporting lines, allocates functions and responsibilities, and takes into account the nature, scale and complexity of the risks inherent in that undertaking's business". Undertakings must therefore be free to define operating models to enable them deliver the required outcome. Point 7 places undue responsibility with the AMSB.

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.

- The reference to "adequate" in point 8 is vague, and therefore open to wide interpretation. In order to ensure Pan-European consistency and a uniform application of this guideline, the point should either be deleted or precised.
- EIOPA should delete the sentence "and to ensure the implementation of their ICT strategy" and rather highlight a "principle of risk-based approach".
- As outlined above, EIOPA must ensure that any guidelines which outline the role of the AMSB (such as Guideline 1) leave sufficient room for the adaption of this role to the realities of the variety of corporate structures in place across different member states. In some member states, the role of the AMSB does not extend beyond monitoring the activities of the company. In France, for instance, this is clearly defined in corporate law. It is therefore not always the AMSB's responsibility to manage the quantity and skills of the undertaking's staff, as suggested by point 8. Such duties might rather fall within the scope of companies' managing departments.

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.

- EIOPA should devote a separate point each to the topics of "budget" and "training", given that they are not at all the same, and involve very different concerns / processes / objectives.

- We deem the reference to the necessity of appropriate training for "staff" too broad, given that "staff" is commonly understood to mean the collective of an undertaking's employees. However, within an insurance company, functions and daily tasks can vary greatly, particularly with regard to the degree of involvement in areas of ICT. As a consequence, we consider it more precise to modify the wording of Point 9 as follows: "the staff should receive appropriate training on ICT and security risks, in each case adapted to the different levels and intensities of use of ICT assets, (…)".

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.

- The words "its communication" should be deleted from this sentence, as the reason why the AMSB of an insurance company should oversee the communication of the ICT strategy has not been justified. Here is an example of where EIOPA's Guidelines go beyond the EBA's, as the same responsibility has not been placed on banks' AMSBs.

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

- Guideline 2 (particularly points 10/11) goes too far in attempting to control companies' internal management systems. Rather than defining a list of minimum requirements within the company's ICT strategy, EIOPA should allow companies the freedom to define the content of their own ICT strategies, provided that they achieve an adequate level of ICT security.

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.

- The requirement to communicate to all relevant staff and service providers the ICT strategy is excessive and contrary to basic principles of confidentiality; this reference should be deleted.

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

- We advocate the substitution of the word "measure" by "check". Though the bulk of audit processes on ICT implementation are carried out with the use of quantitative measure(s), in our opinion the Guidelines should not prejudge the way or method used by any undertaking to assure a sound and robust implementation of their ICT strategy, but should instead focus on whether or not this is achieved.

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

- EIOPA should include a note acknowledging that provisions from points 14 and 15 under Guideline 3, on ICT and security risks within the risk management system, already form part of Solvency II rules and practises.

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.

- The wording of paragraph 14 is unclear, as it would appear to suggest that it is the task of the AMSB to determine the risk tolerance to ICT and security risks, while, in reality, this should be the task of the risk management function. Again, this point does not appear in the EBA's Guidelines, and its addition here is not justified. Furthermore, we e do not support an additional internal written report on ICT risk management addressed to the AMSB, as ICT risk management reporting should instead be integrated into the regular overall risk management reporting. We therefore suggest deleting the second sentence of the paragraph

and propose adding the task of determining the risk tolerance in a new point b) under Guideline 6.

- EIOPA should clarify whether the requirement is to set a risk appetite or a risk tolerance, given definitions under Solvency II.

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.

- Points 15.a and 15.b provide a set of measures to be implemented by undertakings. If interpreted literally, they could result in burdensome costs and efforts, maybe unneccessary for the tasks at hand. Therefore we suggest the following changes:
  - Point 15.a: "Undertakings should establish and regularly update a mapping of their **relevant** business processes and activities (…)"
  - Point 15.b: "(…) of, at least, confidentiality, integrity and availability of those **relevant** business process and activities (…)"

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.

- It must be clarified what is meant by "security risk criteria"

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).

- We suggest deleting the second sentence as, if the assessment is to be carried out and documented regularly, it should not be necessary to specify that this also be performed before any major changes are made.

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.

- The reference to "criticality" in Guideline 3 is vague, and Insurance Europe would prefer that EIOPA highlight more clearly that there is a distinction between managing risks related to critical functions/assets and less critical functions. The EBA guidelines clearly distinguish

between critical functions (information assets) and less critical functions, which is not the case in EIOPA's proposal. See for example EBA guideline 3.3.2 paragraph 16 "…, to be able to, at least, manage the information assets that support their critical business functions and processes", and 3.3.3 paragraph 20: "according to their criticality".

- In order to apply the above change, the order of points (c) and (b) should be switched to introduce the concept of criticality. Any later reference to it will otherwise be unclear.

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.

- The requirement of approval of the ICT and security risk management process by the AMSB is unnecessary (going beyond the duties of the AMSB as defined in System of Governance/SII). It is not the duty of the AMSB to know and validate the details of the company's ICT and security risks. Furthermore, it remains unclear how the approval by the AMSB could be given. (For example a note in an AMSB meeting protocol would be feasible.)

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 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.

- We stress the importance of the last sentence, as it is essential that audits be carried out in proportion to the size of the risk.

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

- There is a need to clarify if "information security policy" refers to (just) an administrative document (written document) or a policy carried out by the organisation. Compare guideline 2 on "strategy" which requires a specific content and purpose but does not (explicitly) refer to a written strategy policy document.

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.

- The wording of point 21 is linked to the definition of "ICT and security risk" provided in the introduction (see comment on definition). Therefore, it could be interpreted that changes made to ICT infrastructure in an adequate timeframe and at a reasonable cost, when required, are equivalent to "security measures", which we deem incorrect. We suggest removing "…ICT and…" from sentence and introducing a new paragraph to cover ICT risks.

- What is meant by "every process described in these guidelines…" must be clarified. After clarification, the wording should be altered to "These procedures and information security measures should generally include the processes described in these Guidelines where applicable".
- Reference to an "information security function" should be removed from Point 21, which deals instead with the establishment of procedures and measures. This point should be left to Guideline 6.

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.

- It must be acknowledged that most of what is detailed in Guideline 6 is already provided for in the System of Governance procedures and because of other existing regulation, such as the GDPR.
- With this in mind, it must be clarified that Guideline 6 does not establish a new list of "key functions", further than the ones referred to in Solvency II and EIOPA's Guidelines on System of Governance. EIOPA should therefore review this article to reflect the following points:
  - Replace "function" with "role", in order to avoid confusion.
  - Change to "in accordance with the proportionality principle **applied to a risk based approach".** Delete "the function should report directly to the AMBS" as: 1/ this point is covered in para 23.b; 2/ the change of reporting line may imply burdensome restructure of firms' organisations conflicting with the freedom of all firms to choose how to organize themselves, provided diligence and objectivity are ensured ; 3/ there is already a reporting line to the AMSB in place via the risk management function who is tasked with reporting on risks that have been identified as potentially material, as per EIOPA's Guidelines on the System of Governance (Guideline 19).
  - As a result, para 22 of Guideline 6 would read better as follows: "Undertakings should establish, within their system of governance and in accordance with the proportionality principle, an information security role, with the responsibilities assigned to a designated person. The undertaking should ensure the independence and objectivity of the information security role by appropriately segregating it from ICT development and operations processes."

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.

- In line with the comment on the definition of "operational and security incident", we believe that "operational and" should be removed.
- In addition, we suggest adding to the list of typical tasks carried out by the information security officer the task of "determining the risk tolerance for ICT and security risks in accordance with the overall risk tolerance of the undertaking"

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.

- It should be clarified that the processes laid out in point e) must be without prejudice to existing retention and data protection requirements.

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.

- Regarding the reference to "strong authentication" in point i), it is important to stress that what is meant by "strong" might very well differ over time and depend on how it is defined. The last sentence; "These methods may include…", does not provide clarity and should be left out.

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

- The purpose of point 25 is unclear.

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.

- This section should be risk based. The wording appears to mandate a full coverage (physical security of laptops…).
- The sentence refers to "access to ICT systems". If the suggested definition of "ICT system" is employed, which includes basically every information asset ("... set of applications, services, information… or other components …" see page 9 in the consultation draft), this guideline will be very hard (or impossible) to apply. We would therefore like to question EIOPA's intention here.

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.

- This topic is already captured in Guideline 19 on "Business Impact Analysis" (see point 63) and should therefore be deleted to avoid unnecessary duplication.

Guideline 9 - ICT operations security

- Generally speaking, this Guideline is not adapted to smaller entities.

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:

- As detailed in the general introductory observations, point 29 (a-f) formulates some specific measures that could be relevant to apply (in different ways, according to the specific nature of the information asset and risk exposure) but does not represent an exhaustive list of measures. However, the list of measures could be interpreted as the minimum security measures that should be implemented, even though such measures are not necessarily proportionate or effective in mitigating a certain information security risk given the nature of the risk and the underlying ICT systems and services. Therefore, the final sentence of point 29 ("These procedures should include, at least, the following measures:") should be changed to: "When implementing such procedures, the following measures should be considered:". This will also ensure that point 29 can be adapted to smaller entities.

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;

- Suggest changing point c) to "Implementation of measures in order to ensure that network integrity is protected, incorporating network segregation and encryption where appropriate, as well as implementation of appropriate measures in order to prevent data leakage".
- **Comments with regard to the suggested change:** In general, the required measures are, on the one hand, too generalised and do not take into account the principle of appropriateness of measures in dependence of the protection level/criticality of data/processes. On the other hand, the required measure of "implementation of a specific system" is too specific and does not take into account the principle of appropriateness.
- In addition, given that one of the stated main goals of the Guideline is to have: "minimum expected information and cyber security capabilities", Guideline 9 does not correspond with requiring in general the implementation of the highest possible security standards, measures and specific systems while taking into account the principle of "appropriateness".
- Adapting the Guidelines to reflect the principle of "appropriateness" is essential given that the implementation of network segmentation, data leakage prevention systems and the encryption of network traffic are very burdensome requirements for small entities. Regarding network segmentation, this may not be appropriate in the case of a small network; regarding encryption of network, it is a very costly solution; and regarding data leakage prevention systems, it is very burdensome to implement and may have limitations, for ex. how do you counter the user who takes a picture of the screen with his smartphone to steal data ?

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

- The implementation of endpoints including servers, workstations and mobile devices requires a network access control, which is a very costly solution and very burdensome for small entities.

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

- Ensuring that integrity-checking mechanisms are in place to verify the integrity of ICT systems is a very costly solution, and almost impossible for the entire perimeter of the information system. Such a measure could be acceptable if integrity-checking mechanisms are restricted to sensitive perimeters.

f) encryption of data at rest and in transit.

- Suggest changing point f) to: "Data should be encrypted in transit as well as rest, where appropriate"
- **Comments with regard to the suggested change:** As outlined before, the required measure is a generalised/undifferentiated measure that is not taking into account the principle of "appropriateness of measures in dependence of the protection level/criticality of data/processes"**.** Especially with regard to the aspect "data at rest", there are high resources and costs associated. Considering this, it should be left to the responsibility of the target audience of the Guideline to decide on the appropriate measures depending on the protection level, criticality and risks.

Guideline 10 - Security monitoring

- This Guideline requires the establishment of a security operations centre for all undertakings, which places an unequal burden on smaller entities.

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

- Guideline 11 does not appear to make reference to ongoing regulatory work on threat-led penetration testing (TIBER-EU etc.). EIOPA could add clarification on requirements impacting testing.

- We stress the point that testing must be carried out on a voluntary basis, must focus on critical infrastructure and must not happen annually to avoid tremendous costs and disadvantages for SMEs. The resources necessary in order to fulfil the requirements of such testing are enormously high. This Guideline must be reviewed to reflect the principles of appropriateness and proportionality.

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.

- Suggest changing point 34 to "Undertakings should establish and implement security testing measures that are validating and ensuring that identified threats and vulnerabilities by threat monitoring, the ICT and security risk assessment process are appropriately covered."
- **Comments with regard to the suggested change**: In practise, such "testing activities" are already covered as an integral part of specific company Guidelines/Standards. The wording "information security testing framework" implies that there is a binding need to create a new information security discipline. Furthermore, it implies that testing of information security will not be an integral, but rather a separate, part of information security activities. From our point of view, this will not reflect the common and current practise.

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.

- Suggest changing point 35 to: "The information security testing measures should ensure that tests are proportionate to the level of risk identified and are carried out by adequately anonymous testers from the area of ICT development and operations with sufficient knowledge, skills and expertise in testing information security measures."
- **Comments with regard to the suggested change:** As already outlined under point "34" there is no need to establish a new wording/discipline of an "information security testing framework". Furthermore, the requirement to conduct information security tests only by external testers is, on the one hand, not reflecting the current common information security practises and, on the other hand, we cannot see that such a requirement is given in any internationally acknowledged information security standard. That would in consequence imply that a company would be no longer able, for example, to conduct vulnerability scans on their own. This does not reflect the reality of how entities carry out information security testing.
- In addition, the importance of an information security review lies in its soundness and ability to ferret out any vulnerability, failure or gap existing in an undertaking's security system. In our opinion, this review has to be conducted with the appropriate level of autonomy that can assure a sound whistle blowing function. This can be assured within the undertaking's organization, as is acknowledged in several legal frameworks, from Solvency II to data protection. Consequently, we deem that the demand of the tester being "independent" could be interpreted as requiring that they be external from the undertakings which is both unnecessary and burdensome.

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 annually

- EIOPA shouldn't specify that critical systems must be tested every year, but rather mention that "regular testing cycle must fit with the criticality of the ICT systems". If annual tests were required, it remains questionable if the proportionality of these tests, as required in point 35 above, could be guaranteed, as penetration test on an annual basis would be highly demanding for any undertaking and conflicts with the market practice of pluri-annual planning. In addition, as penetration tests are generally considered as a best practice, in the first instance it could be more appropriate to rely on thorough gap analyses and, only after that, the undertaking may assess if it is worth performing a penetration test. Therefore, we suggest changing the first sentence to: "The tests should include vulnerability scans and/or penetration tests". The two above suggestion makes paragraph 36 more risk based.

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.

- Suggest changing point 37 to: "Undertakings should ensure that tests of security measures are conducted appropriately, always under consideration of the criticality and the protection level of respective ICT systems, assets and services. This should include tests of new and significantly changed ICT systems/assets as well as tests after major security incidents. Undertakings should monitor and evaluate results of the security tests, and update their security measures accordingly."
- **Comments with regard to the suggested change:** The wording suggested by EIOPA is too specific. As outlined already in the points before, there will be a need to bring the requirement in line with the "spirit of the Guideline" (appropriateness, orientation on protection level, criticality, and risks).

Guideline 12 - Information security training and awareness

- This guideline is welcomed, given that IT security is an essential cornerstone of the business model. Insurance Europe therefore supports regular training programmes as long as this training is not required for all staff within the company. An identification of the relevant staff involved in the training would be welcomed. See comment under point 39.

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.

- Suggest changing point 37 to: "Undertakings should establish information security programs, adapted to the different tasks and daily missions of employees, including AMSB (…)"
- **Comments with regard to the suggested change**: The reference here to "an information security training program for all staff" can be easily interpreted as demanding a sole educational program that will be given to all staff members, no matter their current and daily use of ICT systems. This can lead to one of two undesirable consequences: either all staff will be over-trained in skills, dangers and actions that they should not perform; or the training will be sufficiently basic to cover even the most distant to ICT employees, thus creating training gaps amongst those who would need more comprehensive training.

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.

- EIOPA should add "in accordance with confidentiality or regulatory requirements" at the end of the paragraph.
- The definition of "ICT asset" can include both software and hardware (see section on definitions in introduction). As a result of "assets" also including hardware, devices would have to be destroyed as a whole, which is simply not feasible. As normally hardware does not carry a security classification, it shall not be subject to the duty to be safely destroyed. Furthermore, the duty to destroy decommissioned ICT software assets should not apply in cases where a data deletion method is applied and documented (Refer to National Institute of Standards and Technology SP 800-88, Rev.1, Media Sanitization Guidelines). EIOPA's

suggested approach would also contradict ongoing efforts to create a more sustainable workplace.

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).

- In the point f.ii, it is stated that undertakings should ensure a proper external communication process, in case of any event, "to external parties". We think that this should be completed with the expression "when relevant".
- A Guideline defining too broad an obligation of communicating with third parties could generate reputational damages to undertakings by way of obliging them to communicate

incidents with no actual consequences to third parties. It should at least be stated that this communication should only be compulsory when there is an actual harm to third parties. It must be further clarified that the obligation to provide timely information to external parties does not go beyond existing reporting as required by relevant "applicable regulation", such as the GDPR and NIS Directive. Beyond these existing requirements, for confidentiality reasons, incident reports should never be communicated to external parties.

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.

- This requirement is excessive and should only concern sensitive developments.

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.

- It is hard to justify why Guideline 17 goes far beyond EBA Guidelines on the same topic - Paragraphs 75 and 76 of EBA Guidelines pursue the same objectives while remaining principle-based, a relevant approach for Guidelines. As such, we believe that EIOPA''s Guideline 17 is over-engineered, constraining and restrictive.
- This can be seen in:
  - Point b, as requiring formal acceptance of any residual risks introduces an unnecessary layer of bureaucracy. Zero-risk does not exist in ICT, as in any domain, and it is common sense that any decision also implies the acceptance of the risk associated to it.
  - Point c, where the provision that "a rollback can be performed in case of a malfunction" is overly restrictive because, in practice, a complete rollback may not always be possible. The intention of the Guideline to require undertakings to minimize change risks is welcome, however some of its requirements may be, in some cases, impossible to implement, and therefore unrealistic.

Guideline 18 - Business continuity management

- Guidelines 18-22 on Business Continuity Planning & DRP appear to be consistent with the EBA's Guidelines on ICT and security risk management. Given the European Commission's current regulatory work on "digital operational resilience", we suggest trying as much as possible to ensure consistency between all ongoing work.

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.

- The reference to "all staff" is excessive; "operational staff" would be more appropriate.

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.

- In Guideline 20, EIOPA suggests provisions to include in a BCP. Here, we stress that companies must ultimately have the freedom to define the content of their BCP, provided that this enables them to achieve an adequate level of security of their ICT systems and ICT services.

In Guideline 20, EIOPA suggests provisions to include in a BCP. Here we stress that companies must ultimately have the freedom to define the content of their BCP, provided that this enables them to achieve an adequate level of security of their ICT systems and ICT services.

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).

- While this paragraph is tailored for banking services, such as payment services, it does not account for the nature and specificities of the insurance business. Paragraph 65 should therefore start by saying: "In accordance with the proportionality principle and the criticality assigned to the relevant business processes and activities, business functions, roles and assets (e.g. information assets and ICT assets), (…)"
- RPO (recovery point objective) should be defined according to the international standard ISO-22301: *point to which information used by an activity must be restored to enable the activity to operate on resumption*.
- The third parameter of Business Continuity Management is missing from point 65 - Maximum tolerable period of downtime (MTPOD). Not every application or service must be restored up to 100% at the point of recovery.

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).

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.

- Insurance Europe stresses the importance of Guideline 23 – ensuring that there are effective crisis communication measures in place.
    - National example: LKRZV has existed in Germany for 10 years - an event-related communication platform for the purpose of early detection of crises, alerting and crisis management together with the Federal Office for Information Security and insurance companies. In Germany, this platform is highly regarded and viewed as an example of 'best practise'. Any regulations at European level must therefore be flexible, leaving room for proven national solutions.

Guideline 24 - Outsourcing of ICT systems and ICT services

- Insurance Europe questions the value of having additional requirements on outsourcing, given EIOPA's recent adoption of its guidelines on outsourcing to cloud service providers. However, in the case that a specific guideline is to be included, the below comments should be considered.

76. Without prejudice to the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-19/27014) 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.

- Insurance Europe questions the introduction of terms such as "primary service" and "ancillary service" in the context of outsourcing. The requirements and terminology used should be aligned with the Solvency II Directive (Article 49) and its Delegated Regulation (Article 274 (3)) as regards critical and important operational functions or activities, in order to ensure legal certainty and consistency. This would also ensure consistency with the recently adopted EIOPA guidelines on outsourcing to cloud service providers.

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;
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.

- Suggest changing the first sentence of point 77 to: "Undertakings should ensure that contracts, service level agreements, service descriptions or data protection agreements with the service provider include, at least, the following:"
- **Comments with regard to the suggested change:** Contractual agreements with service providers are covering not only the "contract" and the "service level agreements". In practise, contractual agreements may also come in the form of "service descriptions" and "data protection agreements".

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

- Excessive regulations for sub-delegations (e.g. monitoring of these service providers) can, among other things, prevent or considerably impede cloud use for insurance companies. This leads to massive competitive disadvantages in the international environment and in relation to other industries. Furthermore, it contradicts the free flow of non-personal data in the European Union which is a key building block of the Digital Single Market in Europe and considered the most important element of the data economy. In addition, one of the stated aims of the European Commission's 2018 FinTech Action Plan is to implement technology-supported innovations in the financial sector. Monitoring and control rights for subcontractors are, in many cases, practically impossible to enforce to the required extent.

Consideration of policy issues

- In the discussion on Policy issue 2 (page 28ff), EIOPA expresses a clear preference for Option 1.2 (see section 6, 32). While Insurance Europe is, in principle, in favour of the introduction of Guidelines on ICT security and governance, we believe, in line with the comments included in our response, that the draft guidelines presented above do not sufficiently incorporate many important principles, and at times, go beyond what is justified (eg. the establishment of a separate information security function). We believe, therefore, that EIOPA's suggested Guidelines must be reviewed to reflect the considerations outlined above. We would, then, welcome the opportunity to review a second draft of the guidelines. Adapting the process in this way would, in addition, allow time for any developments regarding the EC's DORFS proposal to be taken into account.

- Furthermore, we would like to highlight that, in the cost assessment for this option (page 29f), only the one off cost is considered, despite the fact that most of the requirements laid out in the consultation paper will result not only in an one off cost for their implementation but also in regular BAU costs for their operation as well as the possible costs associated with running processes to support them. This will impose a significant financial burden on companies, which has not been reflected in this assessment.