EIOPA CONFIDENTIAL USE
Supervisory Processes Department
24 August 2020

EIOPA-BoS-20/550

Resolution of comments of Guidelines on ICT governance and security

General considerations by EIOPA addressing main general points raised by stakeholders

Nr.	Issue	EIOPA response	
1	Coherence with (1) the initiative from the European Commission on digital resilience and (2) the current applicable EBA-Guidelines on ICT security.	(1) EIOPA is aware of the initiatives from the EU-Commission on the area of digital operational resilience. At the moment of drafting these Guidelines, the details regarding COM initiatives are still under development. EIOPA is closely following the initiatives of the Commission and provides the Commission with feedback regarding possible changes in the legal framework. The intention of EIOPA is not to duplicate any ruling or legislation. COM initiatives evidence the urgency of operational resilience and these Guidelines are a contribute in the right direction. The aim is to create a baseline for ICT security and governance requirements across the insurance and reinsurance sector in the EU within the current Solvency II framework. (2) EIOPA is in close contact with EBA. The EIOPA Guidelines on ICT security and governance are based on the recently published EBA – Guidelines on ICT security. EIOPA does not deviate from EBA Guidelines except when specificities of the (re)insurance sector require so.	

2	Proportionality	The application of the principle of proportionality, in the context of the proposed Guidelines, should be carried out in accordance to recitals 19, 20, 21 and Article 29 of Directive 2009/138/EC. Therefore, 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 (in this case EIOPA emphasises the link to the specific risk profile of an insurance or reinsurance undertaking where it comes to collecting and use of data). To underline this principle EIOPA has introduced an additional Guideline (GL1). This Guideline focuses solely on 'proportionality' and again highlights the importance of applying proportionality, both in complying with the rules and in supervising these rules. Additionally, EIOPA has incorporated several references to the proportionality principle into the Guidelines.	
3	How to apply these Guidelines in case of outsourcing (partly or fully)	(Re)insurance undertakings have to consider the requirements defined in Article 49 of Directive 2009/138/EC and in Article 274 of COMMISSION DELEGATED REGULATION (EU) 2015/35 when outsourcing any business activities, key functions etc.. Guideline 25 of the EIOPA Guidelines specifies the requirements on outsourcing in the context of ICT systems and ICT services. The provisions shall apply according to reasonable proportionality and therefore no special exemptions for specific business models (e.g. captive undertakings) have been foreseen in the Guidelines. To underline the principle that the implementation of the requirements should be done in a proportionate manner, EIOPA has added an additional Guideline (GL1) as a follow up to the comments received during the consultation phase. This Guideline focusses solely on 'proportionality' and again highlights the importance of applying proportional measures, both in complying with the rules and in supervising these rules.	
4	How to apply these Guidelines in case of the group is taking care of ICT.	In case the insurance or reinsurance undertaking is part of a Group and the ICT activities are (partially) outsourced to another entity within the Group, these requirements also apply to the ICT Security and Governance activities and measures undertaken by the 'group entity' with regards to the applicable insurance or reinsurance undertaking.	

Allianz SE

Response to the public consultation question	EIOPA's comments
Guidelines § 5	
"Regarding the definition on ICT projects we suggest to change the definition as follows: ""Any project, or part thereof, where ICT systems and services are changed, replaced or implemented, with changes having impact on the control methods and the intensity of controls.""""	EIOPA notes the concerns raised by the respondent but believes the issues should be considered from a proportionality perspective rather than amending a definition. Please refer to general consideration (1)
General comments	
"1. Regarding Section 5 – Analysis of the impacts - 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: We believe that cross-referencing with existing international IT/IS standards and also with non-EU legislation would help to identify potential "improvements". 2. General comment: We welcome EIOPA's draft guidelines which describe already well known good practices in ICT security and governance as they will result in harmonized interpretation of the regulatory standards within Europe. We recommend to align the guidelines with already existing international IT / Information Security standards to create international convergence of ICT risk oversight. De-facto standards or industry good practices, like ISO2700x, COBIT, ITIL, TOGAF and ArchiMate are broadly applied by the respective functions. Having the definitions of key terms in the guidelines directly taken from these documents and having the structure of the guidelines following the frameworks laid out by these documents, would greatly support the implementation of the respective rules in the organizational context, avoiding costly translations and potential misinterpretations."	**EIOPA notes the concerns raised by the respondent** EIOPA will include in the final version of the Guidelines in section 5 cross-referencing to existing frameworks.
§ 9	
We would appreciate concrete details on budget and resource allocation under the ICT system of governance (e.g. a certain percentage of the business budget).	**EIOPA notes the concerns raised by the respondent** Further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines. In addition, concrete budget und resource allocation highly depends on the business particulars; therefore, EIOPA does

Response to the public consultation question	EIOPA's comments
	not intend to provide such details. A detailed impact assessment on each of the considered policy issues has however been provided in the consultation.
§ 15	
We are of the opinion that undertakings should establish a mandatory yearly risk assessment cycle.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that ICT risk management is part of the undertakings' overall risk management system. Requirements on risk management and risk assessment are captured in the Solvency II regulation and Guidelines on System of Governance. EIOPA does not see the need for further specification of these requirements.
§ 29	
We would suggest to include legacy systems in the context of the ongoing renewal of the ICT landscape as legacy ICT systems are identified not always on par with respect to update and review.	**EIOPA notes the concerns raised by the respondent** Monitoring and management of the lifecycle of ICT assets is addressed in GL 14, § 44.
§ 65	
We would like to raise the awareness that Recovery Time Objects (RTO) and Recovery Point Objectives (RPO) differ across financial sectors like insurance, banking and asset management.	**EIOPA notes the concerns raised by the respondent** The comment argues that RTOs and RPOs differ between various segments of the financial sector, which does not contradict the GLs. Accordingly, paragraph 67 describes that RTOs and RPOs shall be relevant to the undertakings as follows: "The response and recovery plans should aim to meet the recovery objectives of undertakings' operations.
§ 78	
The imposed regulation on the usage of cloud service, should be complemented by an overarching regulatory framework for cloud providers, making it easier for cloud users to validate control effectiveness and receive relevant assurance. In this regard, we support a specific framework, certification and oversight regime for ICT providers (including cloud providers). Current sector-specific outsourcing regulation and supervision of the outsourcing party does not reach the source of the risk which typically concentrates at provider level and not at the level of insurers.	**EIOPA notes the concerns raised by the respondent** The comment argues that an overarching regulatory framework for cloud providers shall be implemented. EIOPA is inclined to agree with the necessity of such a framework that is beyond the scope of present guidelines, and should be addressed separately. Refer to general consideration (1)

Nordea Life Assurance Finland Ltd

Response to the public consultation question	EIOPA's comments
Guidelines § 50	
"We suggest amending the draft guideline as follows, so that Lean/Agile methods are also taken into account: 50. Undertakings should implement a methodology for ICT development (including independent security requirement considerations) with adequate governance process and methods to assign responsibilities and leadership to effectively support the implementation of the ICT strategy through ICT change initiatives. The methodology can consist of management of projects and project portfolios, or management of agile development portfolios and programmes. Motivation: insurance undertakings are increasingly using Lean/Agile methods for ICT system development instead of traditional waterfall projects and project portfolio management concepts. The key driver in agile development is fast creation of value to customers, with the ability to redirect and reprioritise development actions based on feedback from customers and business processes. In agile development typically a development team is the fundamental entity and the team takes work from a backlog prioritised according to the undertaking's business strategy. Hence "project governance" or "projects with interdependencies" and "using same resources" are concepts important in waterfall projects but not relevant in Lean/Agile development. In Lean/Agile development the clarity of strategy, customer value and prioritisation are the essential elements. These both concepts coexist in the insurance sector, but we recommend taking both of them into account."	**EIOPA notes the concerns raised by the respondent** These guidelines are intended to be technology and methodology agnostic. Therefore 'ICT project methodology' is used in its general meaning and covers also new and upcoming methodologies. On top of this, 'methods to assign responsibilities' are comprised by an adequate governance process.
§ 51	
"We suggest amending the draft guideline as follows, so that Lean/Agile methods are also taken into account: 51. Undertakings should appropriately monitor and mitigate risks deriving from the portfolio of ICT development initiatives, considering also risks that may result from interdependencies between different initiatives, dependencies	**EIOPA notes the concerns raised by the respondent** These Guidelines are principle-based and do not address the different kinds of project methodologies. In this way agile development are included. When 51 addresses "the portfolio of ICT projects" this indicates all development initiatives, big and small projects/tasks, including lean/agile methods.

Response to the public consultation question	EIOPA's comments
between development teams, or priority conflicts on different development tracks, teams or skills. Motivation: insurance undertakings are increasingly using Lean/Agile methods for ICT system development instead of traditional waterfall projects and project portfolio management concepts. The key driver in agile development is fast creation of value to customers, with the ability to redirect and reprioritise development actions based on feedback from customers and business processes. In agile development typically a development team is the fundamental entity and the team takes work from a backlog prioritised according to the undertaking's business strategy. Hence "project governance" or "projects with interdependencies" and "using same resources" are concepts important in waterfall projects but not relevant in Lean/Agile development. In Lean/Agile development the clarity of strategy, customer value and prioritisation are the essential elements. These both concepts coexist in the insurance sector, but we recommend taking both of them into account."	

Unipol Gruppo S.p.A.

Response to the public consultation question	EIOPA's comments
Guidelines § 2	
Considering that often most ICT systems, information and assets are centralized within a group and shared among all entities belonging to the group, the application of the Guidelines should take into account the structure and ICT organization of the group. Therefore, suggestion is adding specification that the Guidelines should apply first on the undertaking(s) having centralized ownership over ICT functions and systems, whereas other supervised entities belonging to the group and sharing those ICT functions and systems should comply with the guidelines according to a proportional and risk-based approach. Otherwise, risk is duplicating the efforts to comply with the numerous requirements and hindering the organizational efficiency with little or no benefit in the perspective of the overall ICT security. Thus, we suggest rephrasing paragraph 2 as follows: "The Guidelines apply to both individual undertakings and mutatis mutandis at the level of the group. Supervised entities within the group should comply with the guidelines depending on the degree of centralization of the ICT functions and systems and according to a proportional and risk-based approach".	**EIOPA notes the concerns raised by the respondent** Refer to general consideration (4)
§ 3	
The principle of proportionality seems to have a marginal role in these guidelines as their prescriptive requirements and obligations are applicable to all insurance undertakings, without further distinctions based on risk, scale and complexity. A more proportionate approach would entail narrowing the scope of some provisions exempting smaller and/or less risky undertakings. As it emerged during Solvency II review, the principle of proportionality is effective only when the regulation provides ex ante for exemption thresholds or less stringent requirements. On the contrary, past experience has shown that generic regulatory provisions entitling NCAs of interpreting the principle of proportionality force the supervised entities to undertake all the measures and investments to be fully compliant with the regulations, thereby making useless any waiver granted ex post.	**EIOPA notes the concerns raised by the respondent** Refer to general consideration (2)
§ 5	
In order to avoid interpretative uncertainties, suggestion is specifying that information asset does include only the information that is actually and legally	**EIOPA notes the concerns raised by the respondent**

Response to the public consultation question	EIOPA's comments
available to the insurance undertakings. Narrowing the scope of the definition seems appropriate considering that insurance undertakings cannot be held responsible for information that is entirely collected by external service providers and falling out of the scope of outsourcing agreements, all the more so when such information has no use for the execution of the contract: for example, car makers and OEMs often share with the insurance undertakings only part of the data collected by their devices whereas the other part of data which is not conveyed to the insurance undertakings and not used for the execution of the contract should be retained out of the scope. Given that, it would be appropriate specifying that EIOPA guidelines do not apply to information that falls outside the scope of outsourcing agreements and is entirely collected and managed by third parties (which do not qualify as data processors) and not shared with the insurance undertaking. In other words, insurance undertakings can in no way adopt measures or be held responsible over assets that do not fall into the scope of an outsourcing agreement and that belong to third party providers which are separate legal entities and do not qualify as data processors. On the same ground, suggestion is also specifying that an ICT asset is "asset of either software or hardware that is found in the business environment and over which the insurance undertaking has legal availability". Furthermore, in the definition of "cyber security" we suggest replacing "cyber medium" with "internet", which is less vague."	EIOPA believes that by defining the scope of these Guidelines, items not defined are automatically 'out of scope' and there is no need to exclude specifically certain items. It is fundamental for EIOPA to ensure consistency, whenever applicable to both the Insurance and Banking sector, with the final version of the EBA Guidelines. Furthermore, EIOPA emphasises that processes and controls can be outsourced, however, the responsibility for these controls remain with the undertaking and therefore cannot be outsourced.
§ 6	
Given the material and extensive organizational impact of these guidelines, it would be appropriate to set their entry into force not earlier than 18 months from the publication of the final version. Besides, in order to achieve a coordinated regulatory framework and a better regulation, it would be advisable publishing the final version of these guidelines after the disclosure of the European Commission's conclusions on the public consultation on "Digital Operational Resilience Framework for financial services".	**EIOPA notes the concerns raised by the respondent** The implementation date is set to 1 July 2021. Also refer to general consideration (1)
§ 7	
Given the multiplicity of actors and internal functions involved in ICT and in order to achieve an efficient protection from frauds and errors, Unipol Group would recommend including mention of the "principle of separation of duties", according to which a single task should be distributed among multiple users (i.e. entitling a single person/corporate function with a critical responsibility increases the possibility of conflicts of interests, abuses and errors, whereas	**EIOPA notes the concerns raised by the respondent** The principle of segregation of responsibilities is already defined in Level 1 and Level 2 (Article 41 of Directive 2009/138/EC as well as Article 294 COMMISSION DELEGATED REGULATION (EU) 2015/35).

Response to the public consultation question	EIOPA's comments
those risks can be mitigated by disseminating the critical responsibility among several persons/corporate functions, each of which checks and balances the others).	
§ 9	
In order to make the provision less vague, it seems advisable to add a parameter for assessing the appropriateness of the budget. Therefore, suggestion is rewording the first phrase as follows: "The AMSB should ensure that the budget allocated to fulfilling the above is continually appropriate, according to the defined risk tolerance".	**EIOPA notes the concerns raised by the respondent** Further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines. In addition, concrete budget und resource allocation highly depends on the business particulars.
§ 10	
Suggestion is specifying that the ICT strategy should also be aligned with the undertaking's overall risk strategy.	**EIOPA notes the concerns raised by the respondent** Undertakings should develop as defined by Level 2 a risk management strategy (Article 259 COMMISSION DELEGATED REGULATION (EU) 2015/35). This strategy needs to be consistent with and is based on the undertakings' overall business strategy but should be considered as part of the undertaking's risk management system. As both the ICT strategy and the risk management strategy should be aligned / consistent with the overall business strategy by definition, the suggested alignment of this Guideline is not deemed necessary.
§ 13	
Suggestion is specifying that the ICT strategy should be periodically reviewed and that undertakings should also monitor the alignment of the ICT strategy with their overall business and risk strategies.	**EIOPA agrees with the concerns raised by the respondent** Guideline was amended accordingly; also in line with Guideline 6 of the Guidelines on System of governance (EIOPA BoS 14/253 EN). **EIOPA has updated the Guidelines accordingly.**
§ 15	
The provision of the second sentence of point 15(e) seems unduly prescriptive considering that the expression "major changes" may be subject to heterogeneous interpretations from national supervisors, whereas the undertakings should be fully responsible of identifying the appropriate time to carry out a thorough assessment. Therefore, suggestion is to keep the general obligation of assessing the ICT and security risks on a regular basis and deleting the second part of the provision.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion the undertakings should determine by themselves what a major change is, taking proportionality into account.
§ 21	

Response to the public consultation question	EIOPA's comments
Given that Guideline 5 deals with policy and measures, suggestion is removing the reference to the "information security function". For further observations related to the establishment of the information security function please refer to our next comment below.	**EIOPA agrees with the concerns raised by the respondent** The reference to "information security function" was removed from this paragraph. **EIOPA has updated the Guidelines accordingly.**
§ 22	
Suggestion is to replace "information security function" with the "ICT and security risk management framework" and to delete "with the responsibilities assigned to a designated person", as the obligation to establish a new information security function – structurally separated from the other corporate functions – seems inappropriate and too prescriptive from an organizational point of view. According to the principle of proportionality, undertakings should be in charge of identifying and implementing the appropriate organizational measures to achieve the outcomes required by the regulation. In this regard, it is worth noting that EBA shared the stakeholders' concerns and deleted the provision of the new information security function in the final report of EBA Guidelines on ICT and security risk management.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that establishing an information security function is a vital and necessary function for a sound information security management. Therefore, its establishment is essential. This requirement takes the principle of proportionality into account as the actual implementation of this function within the undertakings structure is not specified further. The reference to "direct" reporting to AMSB was delete but reporting to AMSB is still required and its independence and objectivity needs to be considered in this respect.
§ 23	
The responsibilities conferred to the new information security function seem in contrast with the best practice according to which the risk mitigation should be carried out by three lines of defence (3LoD), given that the new function would group together competencies typical of the first line of defence (e.g. the coordination of operational or security incident examination) with others typical of the second line of defence (e.g., monitor the implementation of the information security measures). Therefore, suggestion is to replace "information security function" with "ICT and security risk management framework".	**EIOPA notes the concerns raised by the respondent** Regarding the three lines of defence model, EIOPA would like to stress that this model is not explicitly part of the Solvency II regulation; therefore, EIOPA can only stress that the organisational position of the information security function needs to be in line with the requirement specified under § 23, 2nd sentence. This requirement takes the principle of proportionality into account as the actual implementation of this function within the undertakings structure is not specified further. The reference to "direct" reporting to AMSB was delete but reporting to AMSB is still required and its independence and objectivity needs to be considered in this respect.
§ 29	
The provisions about encryption seem vague as it is not clear if all network traffic (letter (c)) and data (letter (f)) shall be encrypted, which would be disproportionate. Therefore, in order to avoid interpretative uncertainties, suggestion is to rephrase the provisions as follows: "…c) implementation of network segmentation, data leakage prevention system and the encryption of network traffic, in accordance with a risk-based approach; (,) f) encryption of	**EIOPA partially agrees with the concerns raised by the respondent** These guidelines are subject to the principle of proportionality. To underline this principle, EIOPA has added an additional guideline – guideline 1 on proportionality – focusing solely on this principle. Please also refer to general consideration (2).

Response to the public consultation question	EIOPA's comments
critical or sensitive data at rest and in transit, according with a risk based approach". In this respect, it is worth considering that also EBA narrowed the scope of the provisions related to encryption in the final version of EBA Guidelines on ICT and security risk management.	However, it serves the clarity of this document to amend § 30 as follows, in order to underline the validity of the principle of proportionality : '... ~~These procedures should include, at least, the following measures:~~These procedures should appropriately include the following measures:... ' On top of this, for further clarification, the following amendments are made in line with the respective EBA guidelines, whereby instead of 'data classification', used by EBA, the term 'information asset classification' is used, as the term 'information asset' is covered by the definitions: .... c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic (in accordance with the information asset classification) ... f) encryption of data at rest and in transit (in accordance with the information asset classification).'" **EIOPA has updated the Guidelines accordingly.**
§ 36	
The current provision could be interpreted as if penetration tests should be mandatory. If so, such provision would be disproportionate considering that performing penetration tests on an annual basis would be highly demanding for undertakings (in terms of budget, time and personnel). Although penetration tests are generally considered as a best practice, in first instance it could be more appropriate relying on thorough gap analysis and, only after that, the undertaking may assess if it is worth performing a penetration test. Besides, without prejudice to the provision according to which "tests should be performed on a regular basis", it is recommended that undertakings should autonomously assess which is the appropriate periodicity for testing the ICT systems. Therefore, suggestion is to rephrase point 36 as follows: "The tests should include vulnerability scans and/or 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". In this regard, it is worth noting that in the final report of EBA Guidelines on ICT and security risk management, EBA specified that penetration tests are not mandatory but a good practice.	**EIOPA partially agrees with the concerns raised by the respondent** Security incidents and their consequences are observed as the operational risk with biggest economic consequence. To oblige a minimum measure for identifying possible vulnerabilities in the undertakings' ICT infrastructure (HW and SW) EIOPA GL require a yearly vulnerability scan. These GL also require that critical ICT systems should be tested annually to ensure operational stability and security. EIOPA made this decision after evaluating consequences for budget, time and personnel. On top of this, tests should be performed on a regular basis, whereby the scope, frequency and method of testing are to be proportionate to the level of risk identified. Please refer also to general consideration (2). The new wording of the GL is as follows: 37. Undertakings should perform tests on a regular basis. The scope, frequency and method of testing (such as penetration testing, including threat led penetration testing) should be performed commensurate proportionate to the level of risk identified. Testing of critical ICT systems and vulnerability scans should be performed annually.

Response to the public consultation question	EIOPA's comments
	EIOPA has updated the Guidelines accordingly.
§ 52	
The second sentence of point 52 seems overly prescriptive as it is incompatible with the agile software/ICT development, which is based on delivering the outcome iteratively and incrementally, favouring a dynamic and flexible approach over detailed plans and procedures established ex ante. The adoption of the agile approach (which is also based on the collaboration between small self-organizing teams) is especially suited when there is need of adapting quickly the scope and features of software/ICT development to new needs and requirements. The current provision seems instead more suitable for the so-called "waterfall"/traditional approach, according to which the scope of work is defined ex-ante and the ICT development is carried out following pre-determined steps. In order to have a technology-agnostic regulation that allows the insurance undertakings to choose autonomously the most suitable approach for ICT development, suggestion is deleting the second sentence of point 52.	**EIOPA partially agrees with the concerns raised by the respondent** The guidelines aim to be methodologically agnostic and to provide for a risk-based approach; therefore, EIOPA has amended this paragraph as follows: "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 be designed using a risk-based approach." **EIOPA has updated the Guidelines accordingly.**
§ 60	
The second part of the provision seems disproportionate as it prescribes analytically how insurance undertakings are supposed to achieve the outcomes set forth by the regulatory provision. On the contrary, a proportionate regulation should be principle-based by providing the desired outcomes and leaving the insurance undertakings in charge of assessing the most suitable way to manage and mitigate the risks. Therefore, suggestion is to delete the second phrase of point 60. Should EIOPA keep the provision – notwithstanding the above reasoning and the fact that EBA deleted an analogous provision in the final version of its guidelines on ICT and security risk management – we advocate the following amendments: - Letter b), removal of the provision "following approval, the process should include a formal acceptance of any new residual risks", which would be totally disproportionate in most cases, considering that it would entail a formal and thorough risk assessment for any change in ICT systems, including minor software updates that sometimes could also be automated, and	**EIOPA partially agrees with the concerns raised by the respondent** Based on the feedback from the consultation EIOPA GL has been adjusted in line with the EBA guidelines. **EIOPA has updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
- Letter c), specifying that the rollback procedure can be carried out only when it is feasible and proportionate.	
§ 65	
Although the provision of point 65 may be appropriate for credit institutions and payment service providers, it seems too wide and disproportionate for insurance undertakings, which are less exposed to systemic and contagion risks. Therefore, in order to take into account the specific nature of insurance business, suggestion is narrowing the scope of the provision by specifying that undertakings should put BCPs in place in accordance with the proportionality principle, the Business Impact Analysis results and with the assessment of IT and security risk carried provided by Guideline 3.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that the paragraph contains the generic, very basic concepts of business continuity, and contains the basics of business continuity. Also, Proportionality and the results of the BIA and the risk assessment shall be considered in BCPs, which is included in paragraph 67 as follows: "Based on the BIA and plausible scenarios undertakings should develop response and recovery plans" as well as "The response and recovery plans should aim to meet the recovery objectives of undertakings' operations."
§ 71	
In order to avoid possible interpretative uncertainties and heterogeneous supervisory practices across the Member States, suggestion is rewording the provision as follows "[…] are tested regularly through suitable methods based on overall risk tolerance of the undertakings and on the criticality assigned to the relevant activities and assets". Otherwise, risk is that certain supervisory authorities may adopt an overly restrictive approach imposing de facto the most expensive testing method (e.g. full recovery test) for all the insurance undertakings and with reference to the full scope of activities and assets, in spite of the principle of proportionality.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that this requirement already refers to critical business processes and activities for which BCPs shall be regularly tested, and in addition in line with the risk profile of the undertakings. Therefore, the requirement is sufficiently proportionate to allow undertakings to decide which processes and activities are critical, and also allows them to perform the regular testing thereof according to their risk profiles.
§ 76	
Given that both "primary service" and "ancillary service" have not been defined, these two concepts may lead to interpretative uncertainties and do not seem to add much value to the provision. Therefore, suggestion is deleting the sentence between the indents.	**EIOPA agrees with the concerns raised by the respondent** Accordingly EIOPA will delete "- irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service -". **EIOPA has updated the Guidelines accordingly.**

Polish Chamber of Insurance

Response to the public consultation question	EIOPA's comments
§ 49	
Please clarify the responsibilities for reporting safety incidents to the Authority. Please indicate the criteria, modalities, mode and scope (as for example EBA has done in its Guidelines of 19.12.2017 on major incident reporting under Directive (EU) 2015/2366 (PSD2)). Alternatively PIU propose to delete this guideline.	**EIOPA notes the concerns raised by the respondent** Insurance specific reporting requirements on major incidents are in the process of being developed and are being specified outside of these guidelines. Apart from this, also other regulations (e.g. NIST) could apply to undertakings. Therefore references to evolving regulations are worded in a general way. Also refer to general considerations (1)
§ 75	
Please clarify the rules for reporting of crisis communication measures to the supervisory authority with criteria, modalities, procedures and scope (as EBA did in its guidelines of 19.12.2017). Alternatively PIU propose to delete this guideline.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that the requirement refers to crisis communication to competent authorities - among others - when required by regulation. Such regulation - as applicable - shall contain details of crisis reporting rules, and shall be adhered to.

NFU - Nordic Financial Unions

Response to the public consultation question	EIOPA's comments
§ 16	
NFU welcomes the discussion on ICT and security risk management, particularly when seen through the perspective of the Nordic countries, who have always been front-runners at both using ICT solutions and at the number of Fintech companies that operate in the region. Given that the financial sector is the largest consumer of ICT services globally, this indeed brings a higher propensity (three times higher than any other sector, in fact) for cyber-attacks and other security issues. In the pursuits to properly address these risks, we would also like to add that ICT and security risk management are also fundamental for ensuring sound consumer protection, given the sensitivity of data management; as well as for the sector as a whole, in addition to the strategic, corporate, operational and reputational objectives of an undertaking. With today´s level of interconnectedness and cross-border activity, even if one major financial institution suffers a reputational risk due to faulty ICT and security risk management, it can destabilize the sector as such, and shake consumer trust.	**EIOPA notes the concerns raised by the respondent** EIOPA believes that it is important that stakeholders understand and acknowledge the importance of the topic and the need to understand that ICT and security risk management are also fundamental for ensuring sound consumer protection, given the sensitivity of data management. Furthermore, already during the development of the Joint Advice, the ESAs' objective was that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority.
§ 17	
The insurance sector, as the rest of the financial sector, has seen an increase in ICT usage, which has also contributed to changed business models and distribution channels. In Sweden, a recent trend has been noted by insurance companies who are now internalizing the development of such solutions, which once was strictly outsourced. The increased risk does not only affect undertakings´ operations but also the safety of consumer data.	**EIOPA notes the concerns raised by the respondent** EIOPA believes that it is important that stakeholders understand and acknowledge the importance of the topic and the need to understand that ICT and security risk management are also fundamental for ensuring sound consumer protection, given the sensitivity of data management. Furthermore, already during the development of the Joint Advice, the ESAs' objective was that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority.
§ 18	
In this context, NFU would like to express the need for a level-playing field in terms of legislation and regulation. As business models change and evolve, many of the innovative models include Insures start-ups who can offer the same services and products as an established insurance provider. Thus, levelling the playing field on supervision and ensuring cyber-security measures	**EIOPA notes the concerns raised by the respondent** EIOPA believes that it is important that stakeholders understand and acknowledge the importance of the topic and the need to understand that ICT and security risk management are also fundamental for ensuring sound consumer protection, given the sensitivity of data management. Furthermore, already during the development of the Joint Advice, the ESAs' objective was

Response to the public consultation question	EIOPA's comments
are in place throughout the market would ensure fairness, consumer protection and increased safety.	that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority. What EIOPA wants to achieve is a level playing field for all undertakings in the insurance sector.
§ 3	
It would be beneficial to include the reference made in Recital 19 from the Solvency II Directive that proportionality refers to both the requirements imposed on undertakings, as well as to the exercise of supervisory powers.	Refer to general consideration (2)
§ 7	
The importance of the compliance function should also be highlighted in this context, having in mind the current EU-wide focus on better regulation in the areas of AI and digitalization in general, as well as having in mind the current GDPR framework. Additionally, it is essential that the AMSB looks at the internal structures that would allow for system protection for whistle-blowers (disclosing system risks, discrepancies, ethical concerns, either in the segment of accountability and transparency or in the segment of governance). These structures are important to ensure that actual or potential concerns regarding the introduction and development of ICT systems is taken seriously and can act preventively towards potential or actual breaches and risks later on.	**EIOPA notes the concerns raised by the respondent** EIOPA does not see a need to prescribe the need for a compliance function in these guidelines, as it is already prescribed in Level 1 (Article 46 of Directive 2009/138/EC). The same accounts for appropriate internal structures for a system for whistle-blowers.
§ 8	
Training and ongoing competence development of staff is essential in the context of ICT. Depending on the sophistication of the tools used, it is important that staff members acquire necessary skills to understand and operate the systems, properly carryout data management and security, and ensure sound consumer protection. It is within the AMSB responsibility to ensure that such trainings are taking place regularly and are included as part of employees´ working hours to the extent possible.	**EIOPA notes the concerns raised by the respondent**
§ 9	
In addition to the allocation of appropriate budget, which we welcome, we also encourage following up the implementation of such training programmes, especially in light of changing regulatory requirements.	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion that further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines.
§ 11	
Given that the development and adoption of ICT strategies is a long and costly process, which can also affect the tasks and responsibilities of employees, it is	**EIOPA notes the concerns raised by the respondent**

Response to the public consultation question	EIOPA's comments
important that the ICT strategy includes a section that explores the impact, needs and long-term development of employees in the context of ICT evolution at company level, beyond just mere changes in the organizational structure. This is a particular point in which employees and/or their representatives can play a significant role.	EIOPA agrees with the comments, however EIOPA is of the opinion that further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines.
§ 12	
To ensure space for dialogue and input, involving relevant staff in the preparation and roll-out of the ICT strategy could be beneficial.	**EIOPA notes the concerns raised by the respondent** EIOPA agrees with the comments, however EIOPA is of the opinion that further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines.
§ 13	
The process to monitor and measure should be accompanied with a process to (periodically or based on need or detected vulnerability) review and amend the ICT strategy.	**EIOPA notes the concerns raised by the respondent** Undertakings should develop as defined by Level 2 a risk management strategy (Article 259 COMMISSION DELEGATED REGULATION (EU) 2015/35). This strategy needs to be consistent with and is based on the undertakings' overall business strategy but should be considered as part of the undertaking's risk management system. As both the ICT strategy and the risk management strategy should be aligned / consistent with the overall business strategy by definition, the suggested alignment of this Guideline is not deemed necessary.
§ 18	
Special consideration should be given to the accountability regarding any information containing personal data. Additionally, employees need to be made aware and made able to influence how and where their own data is stored, moved to, edited and made accessible to.	**EIOPA notes the concerns raised by the respondent** Data protection issues (GDPR) are not an issue to be addressed by these Guidelines as they are not within the scope of financial regulation.
§ 19	
Given that staff has a significant responsibility to carry out the ICT strategy and to ensure information security company-wide, it should also be made clear that employees that use digital devices or automated tools for their work must never be liable for shortcoming in protection of third parties' data by their employer or for any shortcomings that caused damage to consumers.	**EIOPA notes the concerns raised by the respondent** Collective agreement and employment law are not issues to be addressed by these Guidelines as there are not within the scope of financial regulation.
§ 22	
The function should also be seen in the context of the compliance function, given the implications made by regulatory requirements. We find that if such functions are assigned to individual employees, there needs to be a clear definition of the scope of responsibilities, appropriate training, and an	**EIOPA notes the concerns raised by the respondent** § 20 provides for setting out requirements for staff and defining responsibilities for information security management. §39 provides for information security trainings.

Response to the public consultation question	EIOPA's comments
understanding that the accountability for following rules and procedures still resides at the top.	
§ 23	
As mentioned above, it is essential that the scope of responsibilities and accountability are defined for this function, as well as appropriate training and clarification about the final responsibility always residing at the top. At the same time, in the context of operationalization, the same goes when it comes to individual liability when following agreed rules and directions.	**EIOPA notes the concerns raised by the respondent** §20 provides for setting out requirements for staff and defining responsibilities for information security management. EIOPA is of the opinion that further guidance is not deemed necessary due to the principle-based approach embedded in the guidelines.
§ 37	
When it comes to reactions to security breaches or risks, and updated security measures that follow, it is important that such updates are communicated in a timely manner to employees, and that employees are given enough time and resources to understand the changes made and ensure that appropriate level of customer service is kept, when relevant.	**EIOPA notes the concerns raised by the respondent** This paragraph should be read without prejudice to the rest of the guidelines including paragraph 60, which describes the need to implement changes to the ICT environment in a controlled manner.
§ 38	
While we welcome that such training is foreseen generally, and on a regular basis, it is also important that it takes place during working hours. Once again, in terms of the responsibility and accountability of individual staff, it should be made clear that individual liability for staff does not apply when following company rules and policies.	**EIOPA notes the concerns raised by the respondent** EIOPA's activities don't cover labour law, however it can be assumed that, generally, the information security training programme takes place during working hours. Also individual liability of staff is subject to labour law specifications.
§ 39	
In addition to addressing, it is important to also ensure education on preventing security-related risks and appropriate data management and governance.	**EIOPA notes the concerns raised by the respondent** The intention of § 39 is to emphasize that all kinds of security related matters should be included in a periodic awareness programme. If new risks are identified this will be included.
§ 40	
In addition to ICT operations, critical processes should also be documented.	**EIOPA partially agrees with the concerns raised by the respondent** This guideline uses the word "operations" generically, and not as operations being a step of a process. Nonetheless, to avoid misinterpretation that only the critical steps of an entire critical process should be documented, EIOPA has modified this paragraph as follows: "including documenting critical ICT processes, procedures, and operations." **EIOPA has updated the Guidelines accordingly.**
§ 43	

Response to the public consultation question	EIOPA's comments
In order for the ICT assets to truly support the everyday work of employees, ensuring that they are updated and supported should be imperative. Outdated systems can often be the reason for many repetitive and time-consuming tasks in the financial sector.	**EIOPA notes the concerns raised by the respondent** This is indeed one of the possible risks stemming from outdated or unsupported ICT assets and should therefore be assessed and mitigated appropriately.
§ 52	
Given that the sensitivity of data being processed in certain occasions, and especially personal or health data, ethical considerations should also be taken into account when developing ICT solutions.	**EIOPA partially agrees with the concerns raised by the respondent** The guidelines aim at ensuring that the confidentiality, integrity, availability of the data to be processed are comprehensibly assured and the defined protection requirements are met. The new wording of the paragraph is as follows: "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 be designed using a risk-based approach." **EIOPA has updated the Guidelines accordingly.**
§ 54	
In addition to the unintentional alteration or intentional manipulation of the ICT system, the same considerations should be applied when it comes to data. The acquisition, storage, editing, ownership and usage of data needs to be an important consideration.	**EIOPA notes the concerns raised by the respondent** These are principle based guidelines and the unintentional alteration or intentional manipulation of data are implicitly addressed in §52 (confidentiality, integrity, availability of data in connection with defined protection requirements), §54 (manipulation of system), §55 (methodology for test/approval), §56 (security testing), §57 (separation of production environment from test environment) and §58 (integrity of source code, documentation and configuration data).
§ 64	
In the context of using ICT systems and specifically in the context of employees and consumer data, as mentioned previously, it is important to have in mind that trust and employee and consumer protection are significantly affected by the security of these systems.	**EIOPA notes the concerns raised by the respondent**
§ 67	
The response and recovery plans also need to meet and have in mind the goals of consumer and employee data protection.	**EIOPA notes the concerns raised by the respondent**

Response to the public consultation question	EIOPA's comments
	This paragraph requires to "ensure the integrity, availability, continuity and recovery of, at least, undertakings' critical ICT systems, ICT services and data.", which includes consumer and employee data.

Insurance Europe

Response to the public consultation question	EIOPA's comments
Guidelines § 2	
EIOPA should extend paragraph 2 to provide additional clarification on the scope and applicability of these guidelines. Regarding insurance groups, EIOPA should clarify the application of the Guidelines at solo level versus at group level. This clarification should take into account the principle of proportionality; that smaller entities should not have to comply with all governance requirements. To that extent, Insurance Europe welcomes paragraph 3 of the introduction, but would advocate for a specific guideline to be devoted to this principle, as highlighted in the general observations above.	Refer to general considerations (2) and (4)
§ 5	
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). 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. Some of the definitions need further clarification. In certain cases, which are indicated in the comments on individual definitions, the definitions included in the EBA's Guidelines on ICT security and risk management are preferred.	**EIOPA notes the concerns raised by the respondent** Definitions are set according to the content of the Guidelines and not to related guidelines and legislation, unless, when necessary, related to the Solvency II context; for this reason, the EIOPA Guidelines should always be read in combination with the Directive, the Delegated Regulation and any other relevant Solvency II provision.
§ 6	
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	**The implementation date is set to 1 July 2021**
General comments	

Response to the public consultation question	EIOPA's comments
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.	**The implementation date is set to 1 July 2021** Also refer to general consideration (1) and (2)
§ 7	
EIOPA must ensure that any guideline which outlines 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. Point 7 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.	**EIOPA notes the concerns raised by the respondent** This guideline stresses the importance of a sound information security management within the undertaking. Therefore, the involvement and responsibility of the AMSB is an essential key to this. Regarding the involvement of the AMSB within the undertakings risk management process the general principles for risk management laid down in the respective regulations and guidelines apply. Furthermore, the Guidelines are principle-based, leaving room for each undertaking to implement the requirements in a risk-based and proportionate manner. Guideline 1 states that the oversight of implementation of the undertakings' system of governance is by the AMSB, which is in line with the stated delegated regulations (cf. Guideline 17 of EIOPA Guidelines on System of Governance). In addition, EIOPA does not state that the AMSB should formulate and draft the policies but considers that the general ICT and security risk management and internal control system framework is of such particular importance that it should be administered by the AMSB.

Response to the public consultation question	EIOPA's comments
§ 8	
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.	**EIOPA notes the concerns raised by the respondent** A specification of the term "adequate" is not constructive. Each undertaking needs to define on its own/individually its adequate quantity and skills, depending on its ICT operational needs. Guideline 2 (§ 8) states that the oversight of implementation of the undertakings' system of governance is by the AMSB (cf. Guideline 17 of EIOPA Guidelines on System of Governance). In addition, EIOPA does not state that the AMSB should formulate and draft the policies but considers that the general ICT and security risk management and internal control system framework is of such particular importance that it should be administered by the AMSB.
§ 9	
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, (…)".	**EIOPA partially agrees with the concerns raised by the respondent** A split of this requirement into two paragraphs is not deemed necessary even though different topics are addressed. EIOPA sees the need for information security training for all staff members as a key element to a sound ICT management. In order to highlight that this requirement is further specified in Guideline 13, this Guideline was amended adding "(see Guideline)" at the end of the sentence. **EIOPA has updated the Guidelines accordingly.**
§ 10	
Guideline 2 (particularly points 10/11) goes too far in attempting to control companies' internal management systems. In this regard, 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.	**EIOPA notes the concerns raised by the respondent** EIOPA judges the overseeing of the ICT strategies' (internal) communication by the AMSB as in integral part of the system of governance. A proper communication of the strategy is important as e.g. the implementation of the (ICT) strategy may not succeed without its appropriate communication.

Response to the public consultation question	EIOPA's comments
§ 11	
As outlined above, this point 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.	**EIOPA notes the concerns raised by the respondent** The guideline specifies basic content to be addressed by the ICT strategy; therefore, this requirements adds value by giving information about the minimum requirements to be considered in the ICT strategy.
§ 12	
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.	**EIOPA notes the concerns raised by the respondent** The guideline limits the communication of the ICT strategy by using the term "where applicable and relevant"; therefore acknowledging e.g. the principles of confidentiality. Further, a missing communication of the ICT strategy might prevent its proper implementation.
§ 13	
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.	**EIOPA notes the concerns raised by the respondent** EIOPA clarifies that "measures" in this context refers to both qualitative and quantitative measures. Using "check" in this context does not seem appropriate.
§ 14	
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. The wording of point 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 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.	**EIOPA notes the concerns raised by the respondent** The wording of this requirement is in line with the general governance requirements, e.g. with the EIOPA Guidelines on the System of Governance.
§ 15	

Response to the public consultation question	EIOPA's comments
If interpreted literally, the measures suggested in a) and b) could result in burdensome costs and efforts, maybe unnecessary for the tasks at hand. Therefore we suggest the following changes: a) "Undertakings should establish and regularly update a mapping of their relevant business processes and activities (…)" b) "(…) of, at least, confidentiality, integrity and availability of those relevant business process and activities (…)" b) The reference to "criticality" here 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. Once criticality is defined, the order of points b) and c) should be switched, for clarity. d) The meaning of "security risk criteria" must be clarified e) 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.	**EIOPA notes the concerns raised by the respondent** EIOPA sees the need to include all business processes and activities, etc. in the mapping as a clear view on these needs to be established. Therefore, this requirement is not judged as too burdensome. Every undertaking needs to define "criticality" individually depending on its risk profile. Therefore, EIOPA does not see the need to specify this term further.
§ 16	
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 (a note in an AMSB meeting protocol would be feasible.)	**EIOPA notes the concerns raised by the respondent** This Guideline requires the approval of the results of the ICT risk management process and not of the ICT risk management process itself. Therefore, a change of the Guideline is not deemed necessary.
§ 17	
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.	**EIOPA notes the concerns raised by the respondent** Refer to general consideration (2)
§ 18	
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	**EIOPA agrees with the concerns raised by the respondent**

Response to the public consultation question	EIOPA's comments
organisation. Compare guideline 2 on "strategy" which requires a specific content and purpose but does not (explicitly) refer to a written strategy policy document.	The information security policy is both a written document and a policy to be carried out by the undertaking. In order to clarify the issue of "written" Guideline 3 was amended accordingly. **EIOPA has updated the Guidelines accordingly.**
§ 21	
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.	**EIOPA partially agrees with the concerns raised by the respondent** EIOPA agrees that changes made to ICT infrastructure are not equivalent to security measures. But EIOPA stresses that the information security procedures and measures aim at mitigating ICT and security risks. Therefore, a change of this requirement is not deemed necessary. Process in this context refers to processes affected by the information security measures that are part of these Guidelines. Especially Guidelines 8 to 25. The reference to "information security function" was removed from this paragraph. **EIOPA has updated the Guidelines accordingly.**
§ 22	
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	**EIOPA notes the concerns raised by the respondent and partly agrees.** This guideline specifies the general system of governance requirements in the context of ICT; therefore, clarifying their meaning in this context. Please be aware of that issues regarding the GDPR are not in the remit of financial regulation. EIOPA stresses that the information security function is not a key function as defined by the Solvency II regulation and further explained by EIOPA Guidelines on the System of Governance as the function is not mentioned in Article 268ff. COMMISSION DELEGATED REGULATION (EU) 2015/35; therefore, a change in wording is not deemed necessary. As the proportionality principle encompasses a risk based approach the suggested change in wording is not deemed necessary. The last sentence of this requirement, in comparison to the requirement under §. 24 b), specified that the reporting path for the information security function

Response to the public consultation question	EIOPA's comments
that have been identified as potentially material, as per EIOPA's Guidelines on the System of Governance (Guideline 19). - As a result, point 22 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."	report could be a direct one. However, to avoid burdensome restructuring of existing, good working, reporting lines, EIOPA deleted the word 'directly'. **EIOPA has updated the Guidelines accordingly.**
§ 23	
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"	**EIOPA notes the concerns raised by the respondent** Definition is headed "Operational or security incident" Regarding the suggestion to add a task of "determining the risk tolerance for ICT and security risks in accordance with the overall risk tolerance of the undertaking" please notice that the task prescribed is primarily the responsibility of the risk management function.
§ 24	
e) It should be clarified that the processes laid out in this point must be without prejudice to existing retention and data protection requirements. i) Regarding the reference to "strong authentication", 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.	**EIOPA partially agrees with the concerns raised by the respondent** EIOPA thinks no change is needed since EU and national law are prevalent requirements, as in EBA Guidelines section 3.4.2 - Logical security 31 (d) i) EIOPA agrees to change paragraph 25, using almost the same wording as in EBA Guidelines section 3.4.2 - Logical security 31 (g), in order to clarify the requirement: Authentication methods: financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include strong passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk. **EIOPA has updated the Guidelines accordingly.**
§ 25	
The purpose of point 25 is unclear.	**EIOPA notes the concerns raised by the respondent** The Guideline refers to the least privilege concept and is aligned with paragraph 32 of EBA Guidelines.

Response to the public consultation question	EIOPA's comments
§ 27	
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.	**EIOPA notes the concerns raised by the respondent** This paragraph refers – as the previous one (26) – to premises, data centres and sensitive areas.
§ 28	
This topic is already captured in Guideline 19 on "Business Impact Analysis" (see point 63) and should therefore be deleted to avoid unnecessary duplication.	**EIOPA notes the concerns raised by the respondent** This guideline refers to physical measures to be adopted in order to protect the buildings whereas Guideline 20 refers to the logical design of ICT services.
§ 29	
Generally speaking, this Guideline is not adapted to smaller entities and to the principle of "appropriateness". 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. Due to the word count limit, comments on points c)-f) can be found in the document sent by email.	**EIOPA partially agrees with the concerns raised by the respondent** These guidelines are subject to the principle of proportionality. To underline this principle, EIOPA has added an additional guideline – guideline 1 on proportionality – focusing solely on this principle. Please also refer to general consideration (2). However, based on the suggestion and in order to serve the clarity of this document, § 29 is amended as follows, to underline the validity of the principle of proportionality : '... ~~These procedures should include, at least, the following measures:~~ These procedures should appropriately include the following measures:... ' On top of this, regarding c) and f) - based on the suggestions - the following amendments are made for further clarification: 'c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic (in accordance with the information asset classification) ... f) encryption of data at rest and in transit (in accordance with the information asset classification).' **EIOPA has updated the Guidelines accordingly.**
§ 30	

Response to the public consultation question	EIOPA's comments
This Guideline requires the establishment of a security operations centre for all undertakings, which places an unequal burden on smaller entities.	**EIOPA notes the concerns raised by the respondent** Based on the received feedback from the consultations EIOPA has redrafted and split GL 11 to make it logically more clear. § 310: Monitoring activities § 321: Detecting, internal reporting and responding to anomalous activities § 332: Based on § 310 and 32, developing an understanding on how different anomalous activities could affect undertakings' information security. These guidelines are subject to the principle of proportionality. To underline this principle, EIOPA has added an additional guideline – guideline 1 on proportionality – focusing solely on this principle. Please also refer to general consideration (2). Also the establishment of a security operations centre is subject to the principle of proportionality and therefore is not required in any case. The requirements should be met by all undertakings acknowledging that their implementation needs to done proportional considering the specific risk profile of each undertaking. **EIOPA has updated the Guidelines accordingly.**
§ 31	
This Guideline requires the establishment of a security operations centre for all undertakings, which places an unequal burden on smaller entities.	**EIOPA notes the concerns raised by the respondent** Please refer to above comment on § 31.
§ 33	
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.	**EIOPA notes the concerns raised by the respondent** Undertakings should perform a variety of different information security reviews, assessments and testing. The scope, frequency and method of testing (such as penetration testing, including threat led penetration testing) should be performed commensurate proportionate to the level of risk identified. Also refer to general considerations (2) on the principle of proportionality.
§ 34	

Response to the public consultation question	EIOPA's comments
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.	**EIOPA notes the concerns raised by the respondent** A testing framework is more comprehensive than merely the establishment and implementation of security testing measures. In any case, the requirement does not impose the creation of a new and separate information security discipline, as the testing framework is expected to be an integral one.
§ 35	
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.	**EIOPA notes the concerns raised by the respondent** The reference to 'independent testers' includes internal as well as external testers. In EIOPA's view testers need to be independent. The anonymity of testers is only inherent to certain testing frameworks. The changes regarding § 36 refer to the switching of the requirement that tests should be carried out in a safe and secure manner from §36 to § 35 and to the deletion of the wording that 'this information security testing framework should ensure that tests are proportionate to the level of risk identified' for structural reasons. The resulting wording of §36 is as follows: "Testing should be carried out in a safe and secure manner and by independent testers with sufficient knowledge, skills and expertise in testing information security measures." **EIOPA has updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
§ 36	
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 multi-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.	**EIOPA partially agrees with the concerns raised by the respondent** Security incidents and their consequences are observed as the operational risk with biggest economic consequence. To oblige a minimum measure for identifying possible vulnerabilities in the undertakings' ICT infrastructure (HW and SW) the EIOPA GL require a yearly vulnerability scan. These GL also require that critical ICT systems should be tested annually to ensure operational stability and security. EIOPA made this decision after evaluating consequences for budget, time and personnel. On top of this, tests should be performed on a regular basis, whereby the scope, frequency and method of testing are to be proportionate to the level of risk identified. Please refer also to general consideration (2). The new wording of the GL is as follows: 37. Undertakings should perform tests on a regular basis. The scope, frequency and method of testing (such as penetration testing, including threat led penetration testing) should be performed commensurate proportionate to the level of risk identified. Testing of critical ICT systems and vulnerability scans should be performed annually. **EIOPA has updated the Guidelines accordingly.**
§ 37	
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).	**EIOPA notes the concerns raised by the respondent** This paragraph should be read without prejudice to the rest of the guidelines including § 61, which describes the need to implement changes to the ICT environment in a controlled manner.
§ 38	
Guideline 12 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	**EIOPA partially agrees with the concerns raised by the respondent** The establishment of an information security training programme is required for all staff to ensure that they are well informed in order to perform their

Response to the public consultation question	EIOPA's comments
company. An identification of the relevant staff involved in the training would be welcomed. See comment under point 39.	specific duties and responsibilities to reduce human error, theft, fraud, misuse or loss. For example, a combination of a general information security programme for all personnel and a specific one for some groups, could be set up. Therefore it serves the clarity of this document to amend § 39 as follows: 'Undertakings should establish information security training programmes for all staff...' **EIOPA has updated the Guidelines accordingly.**
§ 43	
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.	**EIOPA partially agrees with the concerns raised by the respondent** Introduction § 4 states that "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" Furthermore, as stated by the guidelines § 82, "Competent authorities that comply or intend to comply with these Guidelines should incorporate them into their regulatory or supervisory framework in an appropriate manner. " Finally, it is understood that these guidelines are not in conflict with other regulatory requirements. This guideline was initially drafted using the verb "to destroy" generically and not as the technically specific term from the NIST framework. To avoid further confusion, EIOPA has amended this paragraph (§44) as follows: "Decommissioned ICT assets should be safely processed and disposed of." **EIOPA has updated the Guidelines accordingly.**
§ 49	
In 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	**EIOPA notes the concerns raised by the respondent** Refer to general considerations (2) The complete phrase reads "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)." Therefore, this guideline is neither "too broad", in conflict with "relevant 'applicable regulation'", nor does it create the obligation to excessively divulge sensitive information.

Response to the public consultation question	EIOPA's comments
confidentiality reasons, incident reports should never be communicated to external parties.	
§ 56	
Testing must be carried out in proportion to the risk.	**EIOPA agrees with the concerns raised by the respondent** EIOPA has added a guideline focusing on the proportionality principle. Please refer to general consideration (2). For clarification, the paragraph is amended as follows: 'Undertakings should appropriately test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.' **EIOPA has updated the Guidelines accordingly.**
§ 60	
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.	**EIOPA agrees with the concerns raised by the respondent** Based on the feedback from the consultation EIOPA GL has been adjusted in line with the EBA guidelines. **EIOPA has updated the Guidelines accordingly.**
§ 61	
The reference to "all staff" is excessive; "operational staff" would be more appropriate.	**EIOPA agrees with the concerns raised by the respondent** EIOPA has run a check for the wording used in the EBA guidelines and it was not possible tofind any mentioning of "operational staff". We suggest changing the wording to "all relevant staff". **EIOPA has updated the Guidelines accordingly.**
§ 64	

Response to the public consultation question	EIOPA's comments
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.	**EIOPA notes the concerns raised by the respondent** This paragraph defines the basics of business continuity planning, which enables undertakings to achieve an adequate level of security and continuity of their ICT systems and ICT services, as suggested by the comment.
§ 65	
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.	**EIOPA notes the concerns raised by the respondent** The paragraph contains the generic, very basic concepts of business continuity, with no reference to payment services. The comment also does not state what insurance sector specific details should be considered. These guidelines are standard and technology agnostic, hence do not require conformance with specific standards or technologies. In our opinion the current definition of RPO explains the concept well enough. In EIOPA's opinion the MTPOD is not absolutely necessary to define an effective BCP. The commenter argued in the previous comment that undertakings shall have the freedom to define the content of their Business Continuity Plans, whereas the present comment asks for being more prescriptive, and prescribing more mandatory details to be included in undertakings' BCPs.
§ 75	
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.	**EIOPA notes the concerns raised by the respondent** The comment does not challenge the requirement, and emphasises that the guidelines shall allow the usage of national best practices, which is allowed by the guidelines. The guidelines set only the minimum requirements in terms of crisis communication.
§ 76	
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.	**EIOPA agrees with the concerns raised by the respondent** Accordingly EIOPA will delete "- irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service -".

Response to the public consultation question	EIOPA's comments
We question 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.	**EIOPA has updated the Guidelines accordingly.**
§ 77	
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".	**EIOPA agrees with the concerns raised by the respondent** Accordingly EIOPA suggests changing the first sentence as follows: "Undertakings should ensure that the contractual obligations of the service provider (e.g. contract, service level agreements, data protection agreements) include …." **EIOPA has updated the Guidelines accordingly.**
§ 78	
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.	**EIOPA notes the concerns raised by the respondent** The cloud outsourcing guidelines fall outside of the scope of present guidelines. However the protection of data, and continuity of services is of paramount importance, even if sub-outsourcing is applied.

AMICE

Response to the public consultation question	EIOPA's comments
Introduction § 18	
We invite EIOPA to correct the typo in the first sentence ("the a sound cyber security framework by undertakings") and delete "the".	**EIOPA agrees with the concerns raised by the respondent**

Response to the public consultation question	EIOPA's comments
	The new drafting of the ICT GLs will correct the typo. **EIOPA has updated the Guidelines accordingly.**
Guidelines § 2	
We invite EIOPA to add the following sentence: "Supervised entities within the group should comply with the guidelines depending on the degree of centralization of the ICT functions and systems and according to a proportional and risk-based approach". The Guidelines should apply first on the undertaking(s) having centralised ownership over ICT functions and systems, whereas other supervised entities belonging to the group and sharing those ICT functions and systems should comply with the guidelines according to a proportional and risk-based approach. Otherwise, we believe that this may lead to a new layer of requirements, duplication of efforts and hindering the organisational efficiency with little or no benefit in the perspective of the overall ICT security.	**EIOPA notes the concerns raised by the respondent** Refer to general considerations (3) and (4)
§ 3	
The principle of proportionality seems to have a marginal role in these guidelines as their prescriptive requirements and obligations are applicable to all insurance undertakings, without further distinction based on risk, scale and complexity. We urge EIOPA to include explicitly the principle of proportionality in the various provisions. The guidelines contain many requirements (new written policy, requirements regarding trainings of AMSB, enhancement of audit and control etc.) which could be very difficult to comply with, especially for SME undertakings.	**EIOPA notes the concerns raised by the respondent** Refer to general considerations (2)
§ 5	
Regarding the definition of the term "information asset", we invite EIOPA to clarify that it includes only the information that is actually available to the insurance undertakings. We believe that this is an appropriate approach given that insurance undertakings cannot be held responsible for information that is entirely collected by external service providers and falling out of the scope of outsourcing arrangement or when such information has no use for the executing of the contract. For example, vehicle manufacturers often share with insurers only part of the data collected by their devices whereas the rest of the data which is not provided to insurers and not used for the execution of the contract should be left out of the scope.	**EIOPA notes the concerns raised by the respondent** Refer to general considerations (1)

Response to the public consultation question	EIOPA's comments
Moreover, we believe that EIOPA should specify that the Guidelines do not apply to information that falls outside the scope of outsourcing agreements and is entirely collected, processed and managed by third parties (which do not qualify as data processors) and not shared with the insurance undertaking. Insurance undertakings can in no way adopt measures or be held responsible over assets that do not fall into the scope of an outsourcing agreement and that belong to third party providers which are separate legal entities and do not qualify as data processors. Following the same reasoning, we suggest adding the following wording in the definition of "ICT asset": "asset of either software or hardware that is found in the business environment and over which the insurance undertaking has legal availability". Regarding the definition of "cyber security" we invite EIOPA to clarify the term "cyber medium" or to replace it with 'internet' instead.	
§ 6	
Given that the application of the Guidelines will require significant efforts in terms of organisation, we believe that the date of application should be set not earlier than 18 months following the publication of the final Guidelines. Moreover, we question the timing of the adoption of these Guidelines given that there is an ongoing consultation carried out by the European Commission on "Digital operational resilience framework for financial services" (DORFS). In order to avoid constant changes to the regulatory framework and in line with the Better Regulation agenda, EIOPA should take into account the outcome of the Commission's DORFS consultation when finalizing its guidelines.	**The implementation date is set to 1 July 2021**
General comment	
We note that the different requirements in the draft Guidelines can be mapped to the requirements of the ISO 2700x and ISO 20 000 standards. In case an entity is already certified against one of these ISO 2700x, 20 000 norms, we invite EIOPA to clarify how the certificates related to these standards can be used as evidences to demonstrate the compliance with the guidelines. EIOPA may consider including a kind of "assumed equivalence" for undertakings which have the above certification.	**EIOPA notes the concerns raised by the respondent** EIOPA acknowledges the importance of existing certifications, for undertakings this is a good practice to use these certification for internal and external evidence and assurance on the reliability of internal processes and systems. These certifications can be taken into account by the relevant supervisory authority at its discretion. However, EIOPA cannot and will not rely on these certifications solely, because NCAs have their own responsibility in supervising compliance with the legislation.

Response to the public consultation question	EIOPA's comments
§ 7	
Bearing in mind the multiplicity of actors and internal functions involved in ICT and in order to achieve an efficient protection from fraud and errors, we invite EIOPA to include a reference to the principle of separation of duties, according to which a single task should be distributed among multiple users (i.e. entitling a single person/corporate function with a critical responsibility increases the possibility of conflicts of interests, abuses and errors, whereas those risks can be mitigated by disseminating the critical responsibility among several persons/corporate functions, each of which checks and balances the others).	**EIOPA notes the concerns raised by the respondent** The principle of segregation of responsibilities is already defined in Level 1 and Level 2 (Article 41 of Directive 2009/138/EC as well as Article 294 COMMISSION DELEGATED REGULATION (EU) 2015/35), therefore EIOPA does not consider that there is a need to specify this further.
§ 9	
We suggest rewording the first sentence as follows: "The AMSB should ensure that the budget allocated to fulfilling the above is continually appropriate, according to the defined risk tolerance".	**EIOPA notes the concerns raised by the respondent** Such a rewording is not deemed necessary due to the principle-based approach embedded in the guidelines. In addition, concrete budget und resource allocation highly depends on the business particulars; therefore, EIOPA does not intend to provide such details.
§ 10	
We invite EIOPA to specify that the ICT strategy should also be aligned with the undertaking's overall risk strategy.	**EIOPA notes the concerns raised by the respondent** Undertakings should develop as defined by Level 2 a risk management strategy (Article 259 COMMISSION DELEGATED REGULATION (EU) 2015/35). This strategy needs to be consistent with and is based on the undertakings' overall business strategy but should be considered as part of the undertaking's risk management system. As both the ICT strategy and the risk management strategy should be aligned / consistent with the overall business strategy by definition, the suggested alignment of this Guideline is not deemed necessary.
§ 13	
We suggest specifying that the ICT strategy should be periodically reviewed and that undertakings should also monitor the alignment of the ICT strategy with their overall business and risk strategies.	**EIOPA agrees with the concerns raised by the respondent** Guideline was amended accordingly; also in line with Guideline 6 of the Guidelines on System of governance (EIOPA BoS 14/253 EN). **EIOPA has updated the Guidelines accordingly**
§ 15	
Paragraph 15(e) seems unduly prescriptive considering that the term "major changes" may be subject to different interpretations from national supervisors, whereas the undertakings should be fully responsible of identifying the appropriate time to carry out a thorough assessment. Therefore, we suggest	**EIOPA notes the concerns raised by the respondent** EIOPA is of the opinion the undertakings should determine by themselves what a major change is.

Response to the public consultation question	EIOPA's comments
maintaining the general obligation of assessing the ICT and security risks on a regular basis and deleting the second part of this paragraph.	
§ 21	
We suggest removing the reference to the "information security function" as Guideline 5 deals with policy and measures. See out comments below on the establishment of the information security function.	**EIOPA agrees with the concerns raised by the respondent** The reference to "information security function" was removed from this paragraph. **EIOPA has updated the Guidelines accordingly**
§ 22	
We suggest replacing "information security function" with the "ICT and security risk management framework" and deleting the following wording "with the responsibilities assigned to a designated person". The obligation to establish a new information security function – structurally separated from the other corporate functions – seems inappropriate and too prescriptive from an organisational point of view. According to the principle of proportionality, undertakings should be in charge of identifying and implementing the appropriate organisational measures to achieve the outcomes required by the regulation. In this regard, it is worth noting that EBA shared the stakeholders' concerns and deleted the provision of the new information security function in the final report of EBA Guidelines on ICT and security risk management.	**EIOPA notes the concerns raised by the respondent** Establishing an information security function is a vital and necessary function for a sound information security management. Therefore, its establishment is essential. Further this requirement takes the principle of proportionality into account as the actual implementation of this function within the undertakings structure is not specified further; but its independence and objectivity needs to be considered in this respect. EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) still specify an information security function (cf Background and Rationale, no. 5 on page 7).
§ 23	
The responsibilities conferred to the new information security function seem in contrast with the best practice according to which the risk mitigation should be carried out by three lines of defense (3LoD), given that the new function would group together competencies typical of the first line of defence (e.g. the coordination of operational or security incident examination) with others typical of the second line of defence (e.g., monitor the implementation of the information security measures). Therefore, we invite EIOPA to replace "information security function" with "ICT and security risk management framework".	**EIOPA notes the concerns raised by the respondent** The information security function tasks does not encompass analysing ICT and security risks. This is primarily the responsibility of the risk management and should be embedded within the undertaking's risk management (cf. Guideline 4). Nonetheless, a close cooperation between the information security function and the risk management might be advisable. Regarding the three lines of defence model, EIOPA would like to stress that this model is, not part of the Solvency II regulation; therefore, EIOPA can only stress that the organisational position of the information security function needs to be in line with the requirement specified under §. 23, 2nd sentence. This requirement takes the principle of proportionality into account as the actual implementation of this function within the undertakings structure is not specified further. The reference to "direct" reporting to AMSB was delete but

Response to the public consultation question	EIOPA's comments
	reporting to AMSB is still required and its independence and objectivity needs to be considered in this respect.
§ 29	
The provisions about encryption seem vague as it is not clear if all network traffic (point c)) and data (point f)) shall be encrypted, which would be disproportionate. Therefore, in order to avoid interpretative uncertainties, we suggest rephrasing the provisions as follows: "c) implementation of network segmentation, data leakage prevention system and the encryption of network traffic, in accordance with a risk-based approach; […] f) encryption of critical or sensitive data at rest and in transit, according with a risk-based approach". In this respect, it is worth considering that EBA also narrowed the scope of the provisions related to encryption in the final version of EBA Guidelines on ICT and security risk management.	**EIOPA partially agrees with the concerns raised by the respondent** These guidelines are subject to the principle of proportionality. To underline this principle, EIOPA has added an additional guideline focusing solely on this principle. Please also refer to general consideration (2). However, based on the suggestion and in order to serve the clarity of this document, § 30 is amended as follows, to underline the validity of the principle of proportionality: '... ~~These procedures should include, at least, the following measures:~~ These procedures should appropriately include the following measures:... ' On top of this, regarding c) and f) - based on the suggestions - the following amendments are made in line with the respective EBA guidelines, whereby instead of 'data classification', used by EBA, the term 'information asset classification' is used, as the term 'information asset' is covered by the definitions: 'c) implementation of network segmentation, data leakage prevention systems and the encryption of network traffic (in accordance with the information asset classification) ... f) encryption of data at rest and in transit (in accordance with the information asset classification).' **EIOPA has updated the Guidelines accordingly.**
§ 36	
The current provision could be interpreted as if penetration tests should be mandatory. If so, such provision would be disproportionate considering that performing penetration tests on an annual basis would be highly demanding for undertakings (in terms of budget, time and personnel). Although penetration tests are generally considered as a best practice, in first instance it could be more appropriate relying on thorough gap analysis and, only after that, the undertaking may assess if it is worth performing a penetration test. Besides, without prejudice to the provision according to which "tests should be performed on a regular basis", it is recommended that undertakings should autonomously assess which is the appropriate periodicity for testing the ICT	**EIOPA partially agrees with the concerns raised by the respondent** Refer to general considerations (2) Based on the feedback in the consultation § 36 has been changed. Security incidents and their consequences are observed as the operational risk with biggest economic consequence. To oblige a minimum measure for identifying possible vulnerabilities in the undertakings ICT infrastructure (HW and SW) EIOPA GL require a yearly vulnerability scan. These GL also require that critical ICT systems should be tested annually to ensure operational

Response to the public consultation question	EIOPA's comments
systems. Therefore, we suggest rephrasing paragraph 36 as follows: "The tests should include vulnerability scans and/or 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". In this regard, it is worth noting that in the final report of EBA Guidelines on ICT and security risk management, EBA specified that penetration tests are not mandatory but a good practice.	stability and security. EIOPA made this decision after evaluating consequences for budget, time and personnel. The requirement to test critical systems annually do not specify what to test. As explained in §. 3 of the Introduction, 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. **EIOPA has updated the Guidelines accordingly.**
§ 52	
We suggest deleting the second sentence of paragraph 52 and the subsequent points as it is overly prescriptive and incompatible with the agile software/ICT development, which is based on delivering the outcome iteratively and incrementally and favours a dynamic and flexible approach over detailed plans and procedures established ex ante. The adoption of the agile approach (which is also based on the collaboration between small self-organising teams) is especially suited when there is need of adapting quickly the scope and features of software/ICT development to new needs and requirements. The current provision seems instead more suitable for the so-called "waterfall"/traditional approach, according to which the scope of work is defined ex-ante and the ICT development is carried out following pre-determined steps. Insurance undertakings should be able to choose autonomously the most suitable approach for ICT development.	**EIOPA notes the concerns raised by the respondent** The guidelines aim to be methodologically agnostic and to provide the facility for a risk-based approach; therefore, EIOPA has amended this paragraph as follows: "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 be designed using a risk-based approach."
§ 60	
The second sentence of the provision and its subsequent points seem disproportionate as it prescribes analytically how insurance undertakings are supposed to achieve the outcomes set forth by the regulatory provision. On the contrary, a proportionate regulation should be principle-based by providing the desired outcomes and leaving the insurance undertakings in charge of assessing the most suitable way to manage and mitigate the risks. Therefore, we suggest deleting the second sentence of paragraph 60. Should EIOPA keep the provision – notwithstanding the above reasoning and the fact that EBA deleted an analogous provision in the final version of its guidelines on ICT and security risk management – we advocate the following amendments: - Letter b), removal of the provision "following approval, the process should	**EIOPA partially agrees with the concerns raised by the respondent** Based on the feedback from the consultation EIOPA GL has been adjusted in line with the EBA guidelines. **EIOPA has updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
include a formal acceptance of any new residual risks", which would be totally disproportionate in most cases, considering that it would entail a formal and thorough risk assessment for any change in ICT systems, including minor software updates that sometimes could also be automated, and - Letter c), specifying that the rollback procedure can be carried out only when it is feasible and proportionate.	
§ 65	
Although the provision of paragraph 65 may be appropriate for credit institutions and payment service providers, it seems too wide and disproportionate for insurance undertakings, which are less exposed to systemic and contagion risks. Therefore, in order to take into account the specific nature of insurance business, we suggest narrowing the scope of the provision by specifying that undertakings should put BCPs in place in accordance with the proportionality principle, the Business Impact Analysis results and with the assessment of IT and security risk carried provided by Guideline 3.	**EIOPA notes the concerns raised by the respondent.** The paragraph contains the generic, very basic concepts of business continuity, and contains the basics of business continuity. Also, § 69 (old 67) states the following: "Based on the BIA and plausible scenarios undertakings should develop response and recovery plans" as well as "The response and recovery plans should aim to meet the recovery objectives of undertakings' operations."
§ 71	
In order to avoid possible interpretative uncertainties and heterogeneous supervisory practices across Member States, we suggest rewording the provision as follows "[…] are tested regularly through suitable methods based on overall risk tolerance of the undertakings and on the criticality assigned to the relevant activities and assets". Otherwise, the risk is that certain supervisory authorities may adopt an overly restrictive approach imposing de facto the most expensive testing method (e.g. full recovery test) for all the insurance undertakings and with reference to the full scope of activities and assets, in spite of the principle of proportionality.	**EIOPA notes the concerns raised by the respondent.** The requirement refers to critical business processes and activities for which BCPs shall be regularly tested, and in addition in line with the risk profile of the undertakings. Hence the requirement is sufficiently proportionate to allow undertakings to decide which processes and activities are critical, and also allows them to perform the regular testing thereof according to their risk profiles.
§ 76	
Given that both "primary service" and "ancillary service" have not been defined, these two concepts may lead to interpretative uncertainties and do not seem to add much value to the provision. Therefore, we suggest deleting the sentence between the indents.	**EIOPA partially agrees with the concerns raised by the respondent.** Accordingly we will delete "- irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service -". **EIOPA has updated the Guidelines accordingly.**