13.03.2020

AMICE Response to EIOPA consultation on the proposal for guidelines on Information and Communication Technology security and governance

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

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

13. EIOPA identified the need to develop specific guidance on Information and Communication Technology (ICT) security and governance in relation to Articles 41 and 44 of Directive 2009/138/EC in the context of the analysis performed to answer to the European Commission FinTech Action plan (COM(2018) 109 final), the EIOPA Supervisory Convergence Plan 2018-20192 and following interactions with several other stakeholders.

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

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

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

17. In addition, across the insurance sector, including both traditional and innovative business models, there is an increasing reliance on ICT in the provision of insurance services and in the undertakings' normal operational functioning, e.g. digitalisation of the insurance sector (InsurTech, IoT, etc.) as well as interconnectedness through telecommunications channels (internet, mobile and

wireless connections and wide area networks). This makes undertakings' operations vulnerable to security incidents including cyber attacks. It is therefore important to ensure that undertakings are adequately prepared to manage their ICT and security risks.

18. Furthermore, recognising the need for being prepared for cyber risk and the a sound cyber security framework by undertakings, these Guidelines also cover cyber security as a part of the undertaking's information security measures. Whilst these Guidelines recognise that cybersecurity should be addressed as part of an undertaking's overall ICT and security risk management, it is important to point out that cyber attacks have some specific characteristics, which should be taken into account to ensure that information security measures adequately mitigate cyber risk:

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

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

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

AMICE feedback: We invite EIOPA to correct the typo in the first sentence ("*the a sound cyber security framework by undertakings")* and delete "the".

19. The objective of these Guidelines is to:

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

b) avoid potential regulatory arbitrage;

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

INTRODUCTION AND DEFINITIONS

1. In accordance with Article 16 of Regulation (EU) No 1094/20105 EIOPA issues these Guidelines addressed to the supervisory authorities to provide guidance on how insurance and reinsurance undertakings should apply the governance requirements foreseen in Directive 2009/138/EC6 ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/357 ("Delegated Regulation") in the context of ICT security and governance. To that end, these Guidelines build on the provisions on governance provided by Articles 41, 44, 46, 47, 93, 132 and 246 of the Solvency II Directive and Article 258 to 260, 266, 268 to 271 and 274 of the Delegated Regulation. Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on system of governance (EIOPA-BoS-14/253) and by EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-19/270).

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

AMICE feedback: 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.

3. Supervisory authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality. The proportionality principle aims at ensuring that governance arrangements are consistent with the nature, scale and complexity of respective risks undertakings face or may face.

AMICE feedback: 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.

4. These Guidelines should be read in conjunction with and without prejudice to the Solvency II Directive, the Delegated Regulation, EIOPA Guidelines on system of governance and EIOPA Guidelines on outsourcing to cloud service providers.

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

Asset owner - Person or entity with the accountability and authority for an information and ICT asset.

Availability - Property of being accessible and usable on demand (timeliness) by an authorised entity.

Confidentiality - Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.

Cyber attack - Any type of hacking leading to an offensive / malicious attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorised use of an information asset that targets ICT systems

Cyber security - Preservation of confidentiality, integrity and availability of information and/or information systems through the internet.

ICT asset - An asset of either software or hardware that is found in the business environment.

ICT projects - Any project, or part thereof, where ICT systems and services are changed, replaced or implemented.

ICT and security risk - As a sub component of operational risk; the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change ICT within a reasonable time and costs when the environment or business requirements change (i.e. agility).

This includes cyber risks as well as information security risks resulting from inadequate or failed internal processes or external events including cyber attacks or inadequate physical security.

Information security- Preservation of confidentiality, integrity and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

ICT services - Services provided through ICT systems and service providers to one or more internal or external users.

ICT systems - Set of applications, services, information technology assets, ICT assets or other information-handling components, which includes the operating environment.

Information asset - A collection of information, either tangible or intangible, that is worth protecting.

Integrity - Property of accuracy and completeness.

Operational or security incident - A singular event or a series of linked unplanned events which have or will probably have an adverse impact on the integrity, availability and confidentiality of ICT systems and services.

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

Threat Led Penetration Testing - A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.

Vulnerability - A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.

AMICE feedback: 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.

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. These Guidelines shall apply from XX.XX.XXXX

AMICE feedback: 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.

GUIDELINES

Guideline 1 - ICT within the system of governance

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

AMICE feedback: 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).

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

9. The AMSB should ensure that the budget allocated to fulfilling the above is continually appropriate, according to the defined risk appetite (or risk tolerance). Furthermore staff should receive appropriate training on ICT and security risks, including information security, on a regular basis.

AMICE feedback: 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”.

Guideline 2 - ICT strategy

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

AMICE feedback: We invite EIOPA to specify that the ICT strategy should also be aligned with the undertaking's overall risk strategy.

11. The strategy should define at least:

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

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

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

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

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

AMICE feedback: 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.

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

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

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

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

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

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

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

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

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

AMICE feedback: 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 maintaining the general obligation of assessing the ICT and security risks on a regular basis and deleting the second part of this paragraph.

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

Guideline 4 - Audit

17. Undertakings' governance, systems and processes for its ICT and security risks should be audited on a periodic basis in line with the undertakings' audit plan12 by auditors with sufficient knowledge, skills and expertise in ICT and security risks to provide independent assurance of their effectiveness to the AMSB. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

Guideline 5 - Information security policy and measures

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

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

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

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

AMICE feedback: 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.

Guideline 6 - Information Security Function

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

AMICE feedback: 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.

23. The information security function is typically:

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

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

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

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

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

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

AMICE feedback: 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 defense (*e.g.* the coordination of operational or security incident examination) with others typical of the second line of defense (*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".

Guideline 7 - Logical security

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

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

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

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

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

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

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

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

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

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

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

Guideline 8 - Physical security

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

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

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

Guideline 9 - ICT operations security

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

a) identification of potential vulnerabilities which should be evaluated and remediated by ensuring that ICT systems are up-to-date, including the software provided by undertakings to its internal and external users, by deploying critical security patches including antivirus definitions updates or by implementing compensating controls;

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

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

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

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

f) encryption of data at rest and in transit.

AMICE feedback: 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.

Guideline 10 - Security monitoring

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

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

c) potential internal and external threats.

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

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

Guideline 11 - Information security reviews, assessment and testing

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

34. Undertakings should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and the ICT and security risk assessment process.

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

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

AMICE feedback: 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, 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.

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

Guideline 12 - Information security training and awareness

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

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

Guideline 13 - ICT operations management

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

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

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

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

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

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

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

Guideline 14 - ICT incident and problem management

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

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

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

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

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

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

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

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

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

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

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

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

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

Guideline 15 - ICT project management

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

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

Guideline 16 - ICT systems acquisition and development

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

a) setting objectives during the development phase;

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

c) quality assurance standards; and

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

AMICE feedback: 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.

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

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

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

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

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

58. Undertakings should implement measures to protect the integrity of source code (where available) of ICT systems. They should also document the development, implementation, operation, and/or configuration of the ICT systems in a comprehensive manner to reduce unnecessary dependency on subject matter experts.

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

Guideline 17 - ICT change management

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

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

b) an evaluation, testing, and approval process for all change requests to ICT systems. Specifically, undertakings should evaluate the impact of the proposed changes and the potential implementation

risks (e.g. compatibility and security). Following approval, the process should include a formal acceptance of any new residual risks;

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

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

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

AMICE feedback: 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 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.

Guideline 18 - Business continuity management

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

Guideline 19 - Business impact analysis

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

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

Guideline 20 - Business continuity planning

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

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

AMICE feedback: 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.

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

Guideline 21 - Response and recovery plans

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

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

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

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

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

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

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

Guideline 22 - Testing of plans

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

AMICE feedback: 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.

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

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

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

Guideline 23 - Crisis communications

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

Guideline 24 - Outsourcing of ICT systems and ICT services

76. Without prejudice to the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-19/27014) undertakings should ensure that in cases where ICT services and systems are

outsourced - irrespective of whether this relates to the primary service or to an additional ancillary service for another primary service - the relevant requirements for the service or system should be met.

AMICE feedback: 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.

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

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

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

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

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

General comments

AMICE feedback: 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.