Boulevard de Berlaimont 14 – BE-1000 Brussels
Phone +32 2 221 48 66
Company number: 0203.201.340
RPM (Trade Register) Brussels
www.nbb.be

BanqueNationaleBank
DE BELGIQUE VAN BELGIË
Eurosystem

Circular

Brussels, 6 July 2021

Reference: NBB_2021_15

Contact person:
Thomas Plomteux
Phone +32 2 221 21 97
thomas.plomteux@nbb.be

Guidelines on information and communication technology security and governance

Scope

- *Insurance and reinsurance companies governed by Belgian law that are subject to the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (hereafter "Solvency II Law") (excluding the insurance companies referred to in Articles 275, 276 or 294 of the aforementioned Solvency II Law);*
- *Authorised branches in Belgium of insurance companies of which the registered office is established in a third country (a country that is not a party to the European Economic Area (EEA) Agreement);*
- *Entities that are responsible for an insurance or reinsurance group governed by Belgian law within the meaning of Articles 339, 2°, and 343 of the Solvency II Law, or for a financial conglomerate governed by Belgian law within the meaning of Articles 340, 1°, and 343 of the Solvency II Law.*

Summary/Objectives

This Circular implements the Guidelines of the European Insurance and Occupational Pensions Authority (hereinafter referred to as "EIOPA") on information and communication technology security and governance (EIOPA-BoS-20/600)[1] and applies from 6 July 2021.

1 https://www.eiopa.europa.eu/content/guidelines-information-and-communication-technology-security-and-governance_en.

Dear Madam,
Dear Sir,

I. Introduction and motivation

Through this Circular, the National Bank of Belgium (hereinafter referred to as the "NBB") indicates that the EIOPA Guidelines on information and communication technology security and governance have been integrated in its supervisory practices. These Guidelines aim to establish adequate ICT and security management in the insurance sector in the European Union and to ensure a level playing field in this regard. Among other things, these Guidelines include provisions on governance and strategy, ICT and security risk management, information security, ICT operations management, ICT project and change management, and business continuity management.

Thus, this Circular clarifies, in the context of ICT and security risk management, the NBB's expectations regarding the implementation of the following provisions:

- the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (hereinafter referred to as the "Solvency II Law"), and in particular Article 42, § 1 regarding an appropriate governance system[2];
- Commission Delegated Regulation 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance, and in particular articles 258-260, 266, 268-271 and 274[3] of the aforementioned Commission Delegated Regulation.

2 Among other things, this Article mentions:
- an appropriate management structure which is based, at the highest level, on the existence of a clear division between the senior management of the insurance or reinsurance company and the supervision of this management and which ensures that there is an adequate separation of functions within the company and a clear, transparent and coherent structure for allocating responsibilities;
- effective procedures for the identification, measurement, administration, monitoring and internal reporting of risks that the company is or might be exposed to and for the prevention of conflicts of interest;
- independent control functions, namely appropriate independent key staff for internal audit, risk management, etc.;
- appropriate IT control and security measures for the company's activities;
- the introduction of appropriate measures for business continuity to guarantee that the data and critical functions can be preserved or restored as quickly as possible and that the normal activities can be resumed within a reasonable timescale.

3 Among other things, these articles mention:
- general governance requirements for insurance and reinsurance companies, including employing personnel with the necessary skills, knowledge and expertise; establishing information systems which produce complete, reliable, clear, consistent, timely and relevant information; safeguarding the security, integrity and confidentiality of information (Article 258(1));
- establishing, implementing, and maintaining a business continuity policy (Article 258(3));
- characteristics of the risk management system, including a clearly defined risk management strategy, procedures on the decision-making process, written policies and reporting procedures and processes (Article 259(1));
- risk management areas, including operational risk management (Article 260(1)(f));
- characteristics of the internal control system (Article 266);
- specific provisions on functions, reporting lines and organisational structure (Article 268);
- the tasks and responsibilities of the risk management function (Article 269), compliance function (Article 270) and internal audit function (Article 271);
- establishing a written outsourcing policy (Article 274(1)), the tasks and responsibilities when choosing a service provider for any critical or important operational functions or activities (Article 274(3)), the written agreement between the insurance or reinsurance company and the service provider (Article 274(4)), and the requirements

II. Clarifications on the scope and implementation

References to "undertakings" in the EIOPA Guidelines should be understood as references to the institutions within the scope defined above.

This Circular applies from 6 July 2021.

The EIOPA Guidelines should be read and applied in conjunction with the provisions of the following circulars:

- overarching Circular NBB_2016_31 on the system of governance, in its amended version of 5 May 2020;
- Circular NBB_2020_018 of 5 May 2020 on the recommendations of the Bank on outsourcing to cloud service providers;
- Circular NBB_2015_32 of 18 December 2015, which applies specifically to significant institutions and groups;
- Circular CBFA_2009_17 of 7 April 2009, which contains additional provisions regarding financial services provided via the internet;
- Circular PPB 2005/2 of 10 March 2005, which contains additional provisions regarding business continuity management.

III. Guidelines on information and communication technology security and governance

Definitions

If not defined in these Guidelines, the terms have the meaning defined in the Solvency II Directive.

For the purposes 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 unauthorised access to or make unauthorised use of an information asset that targets ICT systems.

for insurance or reinsurance companies outsourcing critical or important operational functions or activities (Article 274(5)).

Cyber security	Preservation of confidentiality, integrity, and availability of information and/or information systems through the cyber medium.
ICT asset	An asset of either software or hardware that is found in the business environment.
ICT projects	Any project, or part thereof, where ICT systems and services are changed, replaced, or implemented.
ICT and security risk	As a sub-component of operational risk; the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change ICT within a reasonable time and costs when the environment or business requirements change (i.e. agility). This includes cyber risks as well as information security risks resulting from inadequate or failed internal processes or external events including cyber attacks or inadequate physical security.
Information security	Preservation of confidentiality, integrity, and availability of information and/or information systems. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
ICT services	Services provided through ICT systems and service providers to one or more internal or external users.
ICT systems	Set of applications, services, information technology assets, ICT assets or other information-handling components, which includes the operating environment.
Information asset	A collection of information, either tangible or intangible, that is worth protecting.
Integrity	Property of accuracy and completeness.
Operational or security incident	A singular event or a series of linked unplanned events which have or will probably have an adverse impact on the integrity, availability and confidentiality of ICT systems and services.
Service provider	Means a third-party entity that is performing a 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.

Guideline 1 – Proportionality

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

Guideline 2 – ICT within the system of governance

2. 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.

3. 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 ensure the implementation of their ICT strategy. Furthermore, staff should receive adequate training on ICT and security risks, including information security, on a regular basis, as set out in Guideline 13.

4. The AMSB should ensure that the allocated resources are appropriate to fulfil the above requirements.

Guideline 3 – ICT strategy

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

6. The ICT 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;

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

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

8. Undertakings should establish a process to monitor and measure the effectiveness of the implementation of the ICT strategy. That process should be reviewed and updated on a regular basis.

Guideline 4 – ICT and security risks within the risk management system

9. 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.

10. 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 their importance 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 ahead of 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.

11. The results of the ICT and security risk management process should be approved by the AMSB and included in the process of operational risk management as part of the undertakings' overall risk management.

Guideline 5 - Audit

12. Undertakings' governance, systems and processes for its ICT and security risks should be audited on a periodic basis in line with the undertakings' audit plan[4] 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 6 – Information security policy and measures

13. Undertakings should establish a written information security policy approved by the AMSB 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.

14. 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.

15. 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.

16. Based on the policy, undertakings should establish and implement more specific information security procedures and information security measures to, *inter alia*, mitigate the ICT and security risks they are exposed to. These procedures and information security measures should include every process described in these Guidelines, as applicable.

Guideline 7 - Information security function

17. 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 to the AMSB.

4 Article 271 of the Delegated Regulation.

18. The tasks of the information security function are typically to:

a) support the AMSB when 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 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;

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

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

Guideline 8 – Logical security

19. 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 4. These procedures should be implemented, enforced, monitored, and periodically reviewed, and should also include controls for monitoring anomalies. These procedures 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, at a minimum, privileged users' activities. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate 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 revoked;

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, revocation of access rights should be documented in a way that facilitates comprehension and analysis;

i) authentication methods: undertakings 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 process being accessed. This should, at a minimum, include strong passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

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

Guideline 9 – Physical security

21. 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.

22. Physical access to ICT systems should be permitted only to authorised individuals. Authorisation should be assigned in accordance with the individuals' tasks and responsibilities and 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.

23. 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 10 – ICT operations security

24. Undertakings should implement procedures to ensure 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 appropriately include 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 (in accordance with the information asset classification);

    d) implementation of protection of endpoints including servers, workstations, and mobile devices. Undertakings should evaluate whether an endpoint meets the security standards defined by them 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 (in accordance with the information asset classification).

Guideline 11 – Security monitoring

25. Undertakings should establish and implement procedures and processes to continuously monitor activities that impact the undertakings' information security. The monitoring should cover, at least:

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

    b) transactions by service providers, other entities, and internal users;

    c) potential internal and external threats.

26. Based on the monitoring the undertakings should implement appropriate and effective capabilities for detecting, reporting and responding to anomalous activities and threats, like physical or logical intrusion, breaches of confidentiality, integrity and availability of information assets, malicious code and publicly known vulnerabilities for software and hardware.

27. The reporting from the security monitoring should help the undertakings to understand the nature of both operational or security incidents, to identify trends and to support the undertakings' internal investigations and enable them to make appropriate decisions.

Guideline 12 – Information security reviews, assessment, and testing

28. 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.

29. 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.

30. 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.

31. 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 commensurate with the level of risk identified. Testing of critical ICT systems and vulnerability scans should be performed annually.

32. 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 13 – Information security training and awareness

33. Undertakings should establish information security training programmes 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.

34. 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 14 – ICT operations management

35. 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 processes, procedures, and operations.

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

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

38. 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 processed and disposed of.

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

40. 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.

41. 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 15 - ICT incident and problem management

42. 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.

43. 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.

44. 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 ensure that the root causes are identified, treated, and corrective actions/measures are taken to prevent the incident from happening again. 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, and 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, relevant (supervisory) authorities, as appropriate and in line with applicable regulation).

Guideline 16 – ICT project management

45. Undertakings should implement an 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.

46. 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 17 - ICT systems acquisition and development

47. 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 secured and the defined protection requirements are met. This process should be designed using a risk-based approach.

48. Undertakings should ensure that before system acquisitions or development activities take place, the functional and non-functional requirements (including information security requirements), and technical objectives are clearly defined.

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

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

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

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

53. 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.

54. 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) using a risk-based approach. The undertakings should maintain a register of these applications that support critical business functions or processes.

Guideline 18 - ICT change management

55. Undertakings should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, assessed, tested, approved, authorised, and implemented in a controlled manner. Changes during urgent or emergency ICT changes should be traceable and notified ex-post to the relevant asset owner for ex-post analysis.

56. Undertakings should determine whether changes in the existing operational environment impact the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the undertakings' formal change management process.

Guideline 19 – Business continuity management

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

Guideline 20 – Business impact analysis

58. As part of a sound business continuity management, undertakings should conduct a business impact analysis to assess the undertakings' exposure to severe business disruptions and their potential impact, quantitatively and qualitatively, using internal and/or external data and scenario analysis. The business impact analysis 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 4.

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

Guideline 21 – Business continuity planning

60. The overall Business Continuity Plans (BCPs) of the undertakings 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 the undertakings' 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.

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

62. 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 of such scenarios. Based on these scenarios, undertakings should describe how continuity of ICT systems and services, as well as undertakings' information security, is ensured.

Guideline 22 – Response and recovery plans

63. Based on the business impact analysis and plausible scenarios undertakings should develop response and recovery plans. These plans should specify the conditions that may require activation of the plan and actions to 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 the undertakings' operations.

64. The response and recovery plans should consider both short-term and, where 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;

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

65. 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.

66. 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 23 – Testing of plans

67. 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 regularly tested based on the undertakings' risk profile.

68. 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 Recovery Time Objective and Recovery Point Objective) and/or changes in business processes and activities, business functions, roles, and assets (e.g. information assets and ICT assets) should also be included.

69. BCP testing should demonstrate that they are capable of sustaining the viability of the business until critical operations are re-established at a predefined service level or impact tolerance.

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

Guideline 24 - Crisis communications

71. 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 relevant supervisory authorities, when required by national regulation, as well as relevant service providers, are informed in a timely and appropriate manner.

Guideline 25 – Outsourcing of ICT services and ICT systems

72. Without prejudice to EIOPA Guidelines on outsourcing to cloud service providers undertakings should ensure that where ICT services and ICT systems are outsourced the relevant requirements for the ICT service or ICT system are met.

73. In case of outsourcing of critical or important functions undertakings should ensure that contractual obligations of the service provider (e.g. contract, service level agreements, termination provisions in the relevant contracts) 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 ICT systems and performance targets under normal circumstances as well as those provided by contingency plans in the event of service interruption;

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

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

IV. Distribution

A copy of this Circular will be sent to your institution's accredited statutory auditor(s).

Yours faithfully,

p.p. Pierre Wunsch
Governor

Steven Vanackere
Vice-governor