JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 39

13 06 2023

Consultation Paper

on Draft Regulatory Technical Standards

to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Responding to this consultation

The three European Supervisory Authorities (ESAs) invite comments on all matters in this paper and on the specific questions summarised in Annex II.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 11.09.2023. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with the ESAs' rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESAs' Boards of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of EBA, EIOPA and ESMA websites respectively.

2. Executive Summary

Reasons for publication

1. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter 'DORA') tasks the ESAs, under its Article 15, to develop draft regulatory technical standards ('RTS') aiming at *'further harmonisation of ICT risk management tools, methods, processes and policies'* and under its Article 16, to develop a simplified ICT risk management framework for certain financial entities.

2. The ESAs have prepared this Consultation Paper (CP) to consult interested parties for the purpose of elaborating its draft RTS to be submitted to the European Commission (EC). Respondents to this consultation are encouraged to provide the relevant background information, and qualitative and quantitative data on costs and benefits, as well as concrete redrafting proposals, to support their arguments where alternative ways forward are called for. If respondents envisage any technical difficulties in implementing the proposed requirements, they are encouraged to provide details regarding the specific technical and operational challenges and specify the costs involved, which are important for the cost-benefit analysis.

Contents

3. Section 3 presents the background to our proposal and questions for your consideration and Section 4 includes our proposed draft RTS. Annex I includes a preliminary impact assessment and Annex II lists all questions formulated in this consultation.

Next steps

4. The ESAs will consider the feedback received to this consultation in Q3/Q4 2023 and should publish a Final Report and the submission of the draft RTS to the European Commission by 17 January 2024.

5. The ESAs will finalise the impact assessment regarding the proposed measures, to be included in the Final Report to be submitted to the EC. Due to the limitation of the information available, a more in-depth cost-benefit analysis will be provided after input of stakeholders. The input from stakeholders will help the ESAs in finalising the RTS and the relevant impact assessment. Therefore, respondents to this consultation are strongly encouraged to provide solutions for any problems raised and to support the drafting proposals with relevant data.

Legislative references

CSDR	Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1–772)
CSDR RTS 2017/392	Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (JO L 65 du 10.3.2017, p. 48–115)
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1–79)
EMIR	Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1–59)
EMIR RTS 2013/153	Commission Delegated Regulation (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties (JO L 52 du 23.2.2013, p. 41–74)
MIFID 2 RTS 2017/584	Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues (JO L 87 du 31.3.2017, p. 350–367)
NIS2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80–152)

Acronyms used

BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
ESCB	European System of Central Banks
NCA	National Competent Authority
NIST	National Institute of Standards and Technology
RTS	Regulatory Technical Standards

3. Background

2.1 Introduction

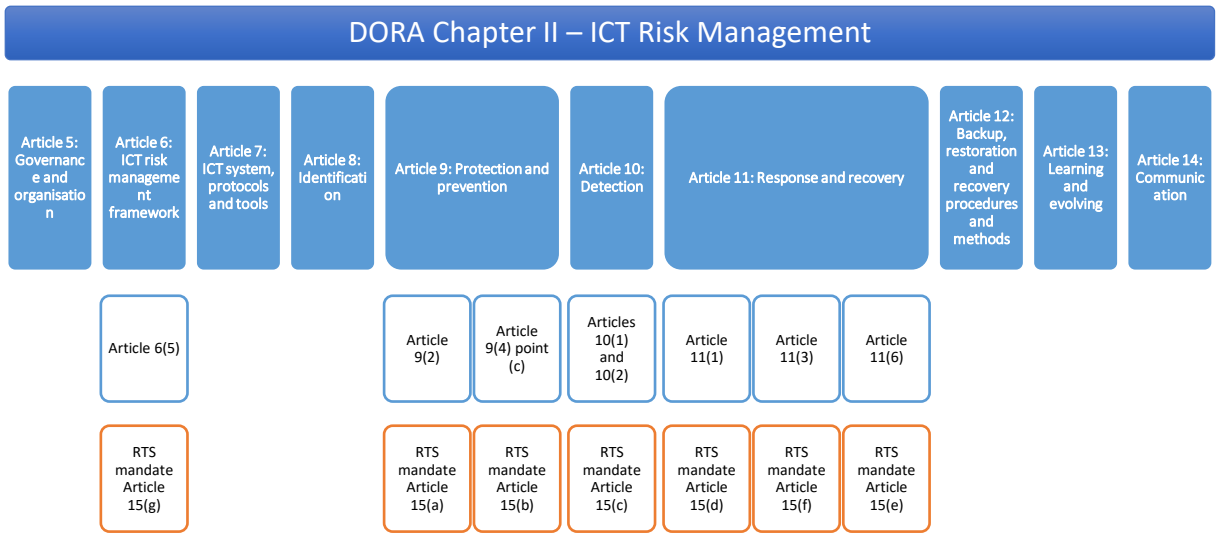
1. DORA sets out uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information and Communication Technologies) services to them, such as cloud computing or data analytics services. DORA creates a regulatory framework on digital operational resilience, whereby all financial entities need to make sure they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across the EU, with the core aim to prevent and mitigate cyber threats.

2. The ESAs, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA) were empowered to deliver two draft RTSs on certain aspects of the ICT risk management under Articles 15 and 16 of DORA.

3. To do so, the ESAs have duly considered the following existing European and international standards on ICT risk management: EBA Guidelines on ICT and security risk management (2019), EIOPA Guidelines on ICT security and governance (2020), NIS2 Directive and the NIST cybersecurity framework components, as well as ISO-IEC 27000 family standards, 2020 FSB CIRR toolkit, the G7 Fundamental Elements of Cyber security in the financial sector, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, the BCBS principles for operational resilience and sound management of operational risk, effective risk data aggregation and risk reporting.

4. The draft RTSs developed under Article 15 and Article 16(3) of DORA need to be understood as **complementary to the requirements set out in DORA itself.**

5. It is important to note that the mandate given to the ESAs pursuant to Article 15 of DORA is limited to the identification of further elements in certain areas of: ICT risk management framework (Article 6), Protection and Prevention (Article 9), Detection (Article 10), and Response and recovery (Article 11), as presented in the graph below. This means that, for the financial entities that are not subject to Article 16 of DORA, the implementation and supervision of their compliance with the Chapter II of DORA (ICT risk management) will consider requirements set out in DORA Articles 1 to 14, alongside with those of the RTS mandated under Article 15 of DORA.



6. DORA and the draft RTS developed under Articles 15 and 16(3) of the same Regulation together are carrying over several provisions related to ICT and security risk management/digital operational resilience from existing relevant sectoral EU guidelines (EBA Guidelines on ICT and security risk management (2019), EIOPA Guidelines on ICT security and governance (2020). Therefore, it will be assessed in due course how the existing sectoral EU regulatory framework will need to be amended to align with DORA and its respective RTS, and to supplement it with further convergence tools, if deemed necessary.

7. The draft RTS contained in this CP deals with specific requirements that are part of the broader framework on ICT risk management and digital operational resilience as designed in DORA. The ESAs attach a lot of importance to ensuring strong ICT risk management and control frameworks in financial entities, and would like to ensure that any elements identified provide a clear and coherent picture towards the effective implementation of these frameworks. To this effect, the ESAs are currently considering whether, how and what further guidance to provide to the market on the interaction between the requirements to be included in the draft RTS and the other requirements relating to the ICT risk management framework that are contained in DORA and are directly applicable (and whether there is a need for further specification outside of the Delegated Regulations).

8. In that respect, the ESAs welcome feedback on this point, identifying any bespoke areas for such consideration. They then will assess carefully the responses to the CP in order to: (i) ensure that the requirements of the draft RTS are clear and proportionate, and (ii) identify and prioritise the areas on which further guidance to the market would be appropriate, if any.

2.2 Architecture of the proposed draft RTS

2.2.1 One joint RTS on ICT risk management, two titles

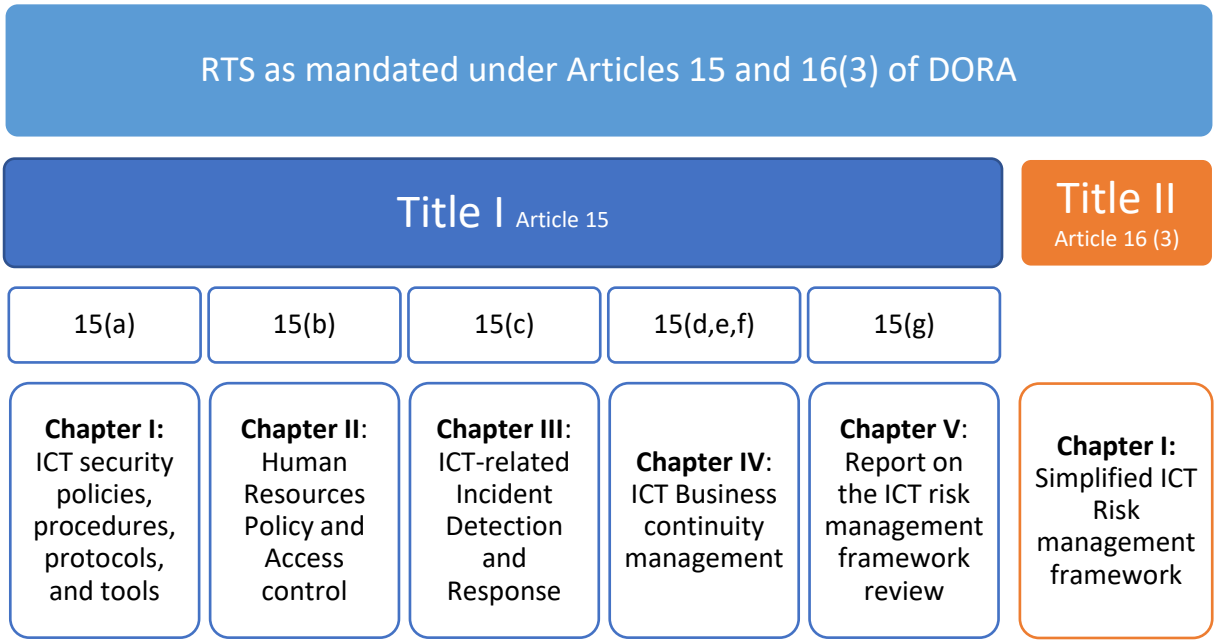
9. The ESAs' mandates under Article 15 and Article 16(3) of DORA both relate to the area of ICT risk management framework by detailing specific elements applicable to the financial entities in accordance with Article 15 of DORA or by designing the simplified ICT risk management framework for the financial entities set out in Article 16(1) of the same regulation.

10. To ensure coherence between those provisions, which should enter into force at the same time, it is proposed to include all the regulatory technical standards required by Article 15, fourth subparagraph, and Article 16(3), fourth subparagraph of DORA, into a single RTS.

11. The proposed RTS is therefore divided into two titles, respectively addressing each of the mandates.

2.2.2 Structure of the proposed RTSs

12. The structure of the proposed RTSs largely follows the empowerments granted to the ESAs under Article 15 and Article 16(3) of DORA. At the same time, to facilitate the implementation and supervision of the requirements, the RTS has been structured in a way to allow for the integration of existing European or international frameworks on ICT and information security already widely used, acknowledged and tested by the industry and supervised by the CAs to ensure alignment with said standards (please refer to point 3 for those). The following graph presents a high-level mapping of the structure of the proposed RTSs with the structure of the empowerments under Articles 15 and 16(3) of DORA.



2.3 General drafting principles

2.3.1 Technology-neutral

13. The ESAs consider that the RTS should remain technology-neutral and should not identify specific products or technologies. Such approach should ensure that the legal text remains future-proof to the extent possible, thus avoiding the need of frequent revisions.

2.3.2 Cross-sectoral

14. Given the wide scope of DORA in terms of entities in scope, and in order to keep the framework as simple as possible, the proposed RTS tends to include requirements applicable to all the entities within the scope of DORA (i.e. sector-agnostic and principle-based requirements).

15. This does not however exclude that, where needed, entity-specific requirements would be included. In particular, recital 103 of DORA states that '*the scope of the relevant articles related to operational risk, upon which empowerments laid down in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 had mandated the adoption of delegated and implementing acts, should be narrowed down with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those Regulations*'.

16. This is the basis for the introduction of certain requirements specific to CCPs, CSDs and trading venues in the proposed RTS which are more stringent than DORA requirements and are considered appropriate to keep in DORA Level 2. More details on these requirements are provided below in the relevant chapters or sections incorporating them.

2.3.3 Proportionality

17. The proposed draft RTS includes the proportionality principle, both with reference to the part based on the mandate in Article 15 of DORA and to the part based on Article 16 of DORA, which itself already embeds proportionality considerations as it designs a simplified regime for certain entities.

18. The ESAs, in line with mandate in Articles 15, second paragraph, and 16(3), second paragraph of DORA, have to take into consideration the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations when developing the draft RTSs.

19. In the case of the RTS developed under Article 16(3), the approach chosen by the ESAs to ensure the principle of proportionality has been to identify areas on which specific elements of complexity may require adapting the relevant policies and procedures.

20. In order to ensure a correct adaptation of the RTS to the different typologies of financial entities and to obtain adequate feedback on this point, it will be extremely useful to receive feedback during the consultation process both for the draft RTS based on Article 15 and for the draft RTS based on

Article 16 of DORA, from the largest number of financial entities, in particular from those that could be linked to a possible reduction of the requirements based on their size, risk profile, nature, scale and complexity of their services, activities and operations.

Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (*Complexity and risks considerations*)? If not, please provide detailed justifications and alternative wording as needed.

Q2. Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

2.4 Title I: Further harmonisation of ICT risk management tools, methods, processes and policies (Article 15)

Mandate under Article 15 of DORA

The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards in order to:

(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2), with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays;

(b) develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;

(c) develop further the mechanisms specified in Article 10(1) enabling a prompt detection of anomalous activities and the criteria set out in Article 10(2) triggering ICT-related incident detection and response processes;

(d) specify further the components of the ICT business continuity policy referred to in Article 11(1);

(e) specify further the testing of ICT business continuity plans referred to in Article 11(6) to ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;

(f) specify further the components of the ICT response and recovery plans referred to in Article 11(3);

(g) specifying further the content and format of the report on the review of the ICT risk management framework referred to in Article 6(5);

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors.

21. This mandate is covered under the first title of the proposed draft RTS. Its scope is limited to a coherent harmonisation of some of the requirements already identified in the DORA Chapter II, Section II, ICT Risk Management framework. It is important to note that, unlike the Guidelines on ICT risk management issued by the EBA and EIOPA, the purpose of this RTS is not to design a complete ICT risk management framework; **rather, it is focused on introducing only certain specific elements**.

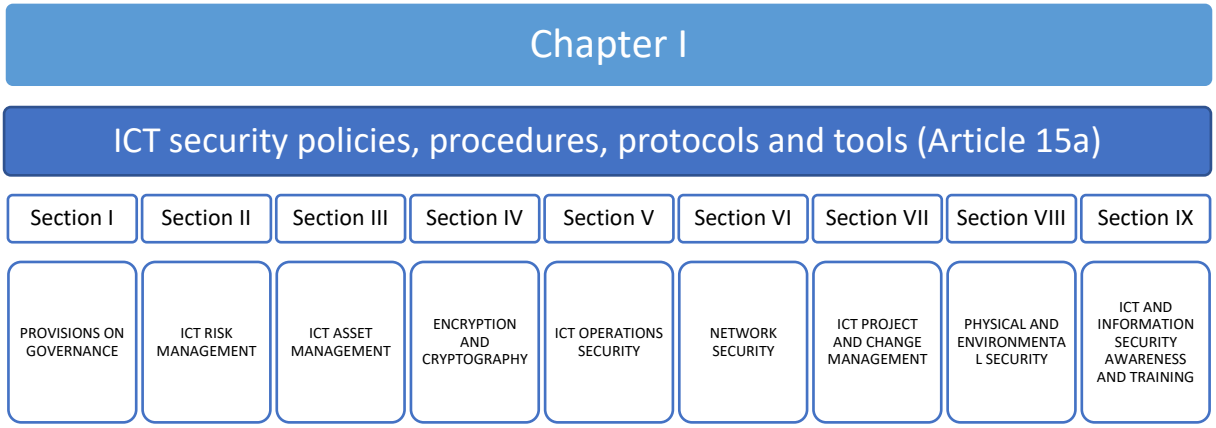
22. In addition, the mandate also requires in certain areas to provide **more detailed information on some aspects than those covered in the existing ESAs Guidelines** (e.g. detection mechanisms for anomalous activities, criteria triggering ICT-related incident detection and response, etc.). This also means that some articles will include more details than others.

23. Title I is divided into five chapters: ICT security, human resources policy and access control, ICT-related incident detection and response, ICT business continuity management, and report on the ICT risk management framework review.

24. The approach followed for each of these chapters is presented below.

2.4.1 Chapter I: ICT security policies, procedures, protocols and tools

25. The purpose of this chapter is to cover the mandate established in Article 15 (a) of DORA, which requires specifying further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2) of DORA. The latter requires financial entities to "*design, procure and implement ICT security policies, procedures, protocols and tools that that aim to ensure the resilience, continuity and availability of ICT systems, in particular those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit*".



26. The objective, therefore, of the ESAs is to identify elements additional to the above-mentioned in Article 9(2) of DORA ensuring the security of networks, safeguards against intrusions and data misuse, preserving the availability, authenticity, integrity and confidentiality of data, and guaranteeing an accurate and prompt data transmission without major disruptions and undue delays.

27. Based on this mandate, the ESAs have identified key elements of the ICT risk management framework that would assist in achieving the above objective. As the mandate is for the development of additional elements, the different articles included in this chapter complement the requirements already included in DORA.

28. For ease of reading and implementation, and considering the standards referred to in paragraph 3, the chapter has been divided into 9 different sections, which are detailed below.

2.4.1.1 Section I: Provisions on governance

29. This section is divided in two articles: Article 1 presents general elements of ICT security policies, making the link between ICT security policies, procedures, protocols and tools and the ICT risk management framework defined by the financial entities.

30. This article elaborates on the main ICT security policies, procedures, protocols and tools that shall be considered and which are detailed in the rest of the chapter, as an integral part of the ICT Risk management framework. The focus is on ensuring the security of networks, enabling adequate safeguards against intrusion and misuse of data, preserving the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and ensuring accurate and prompt data transmission without major interruptions or undue delays, in line with the provisions of Article 15(a) of DORA.

31. Article 2 of the proposed draft RTS details the minimum list of tasks and responsibilities to be assigned to the control function referred to in Article 6(4) of DORA.

Q3. Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

2.4.1.2 Section II: ICT risk management

32. The purpose of this section is to outline the minimum requirements applicable to financial entities regarding the development and documentation of their ICT risk management policy and procedures. The ICT risk management policy is essential for ensuring the preservation of data and systems availability, authenticity, integrity, and confidentiality and should be embedded in the overall ICT risk management framework of financial entities. The ESAs consider the financial entities' ICT risk management policy should include all elements specified in Article 3 of the proposed draft RTS.

33. Financial entities should be obligated to establish an ICT risk management policy that includes the necessary measures and procedures for effectively managing ICT risk. This policy should clearly define the approved risk tolerance levels for each type of risk identified. By establishing risk tolerance levels, financial entities can assess and manage their exposure to ICT risk effectively.

34. By adhering to the provisions outlined in this Section in conjunction with the provisions on ICT risk management outlined in DORA itself, financial entities can establish a robust ICT risk management policy that enables them to proactively address and mitigate ICT risk, safeguard data, and maintain the overall security and resilience of their operations.

35. In particular, financial entities should establish a process and a methodology to conduct the ICT risk assessment. The process and the methodology must identify vulnerabilities and threats that affect or may affect business functions, ICT systems, and supporting ICT assets. They must also include quantitative or qualitative indicators to measure the impact and likelihood of occurrence of these vulnerabilities and threats. It should be noted that the requirements on the ICT risk assessment should be read and implemented in conjunction with Article 8 of DORA on identification.

36. Financial entities should have a comprehensive and systematic approach to treating ICT risk identified through the ICT risk assessment. By identifying and implementing appropriate measures and regularly monitoring their effectiveness, financial entities can mitigate and manage ICT risk in line with their risk tolerance levels. This contributes to the overall resilience and security of their ICT systems and operations.

37. Also, financial entities should have a structured approach to identify, accept, document and review residual risks. The residual risks should be integrated within the broader risk management process of financial entities so that they can maintain a comprehensive understanding of their risk profile and make informed decisions regarding risk acceptance and mitigation. Financial entities should also identify who is responsible to accept the residual risks. The structured approach put in place contributes to the overall effectiveness of their ICT risk management efforts and strengthens their resilience against potential threats.

38. As part of their ICT risk management process, financial entities are responsible for monitoring any changes occurring within their ICT environment. This includes monitoring internal and external vulnerabilities and threats that may pose risks to their ICT systems and operations. By actively monitoring these factors, financial entities can stay vigilant and identify any changes that may increase or alter their ICT risk profile.

39. Furthermore, financial entities are expected to monitor their ICT risk to ensure they have an up-to-date understanding of their risk landscape. This involves tracking and assessing the various risks associated with their ICT systems, applications, and infrastructure. By doing so, financial entities can identify emerging risks and take proactive measures to mitigate or manage them effectively.

40. Another crucial aspect of the ICT risk monitoring is its alignment with ICT risk monitoring with changes in the business strategy and digital operational resilience strategy. Financial entities are required to verify at least once a year that any changes to their business strategy and digital operational resilience strategy are appropriately considered in their ICT risk monitoring efforts. This ensures that the monitoring activities remain relevant and aligned with the evolving objectives and priorities of the organization.

41. Finally, in addition to the reviews of their ICT risk management framework mandated under Article 6(5) of DORA, to ensure the ongoing effectiveness of the ICT risk management process, financial entities shall conduct additional reviews when triggered by significant changes to the cyber threat landscape, ICT services, ICT assets supporting business functions and update their ICT risk management policies and procedures.

Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

2.4.1.3 Section III: ICT asset management

42. One of the basic and initial steps in ensuring that the availability, authenticity, integrity and confidentiality of data is preserved, is the correct identification and classification of ICT assets and information assets. Without a correct identification and classification, it is very difficult to have a correct knowledge of these assets and a correct adaptation of the rest of the elements of the ICT risk management framework to them. In this line, Article 8(1) of DORA establishes that as part of the ICT risk management framework, financial entities shall identify, classify and adequately document, among others, their information assets and ICT assets.

43. Section III elaborates on the requirements of Article 8 of DORA through two articles. The first article requires financial entities to establish a policy for the management of ICT assets, complementing the elements already included in Article 8(6) of DORA with respect to the inventory of the ICT assets and information assets.

44. The second article focuses on the additional elements to be considered by financial entities when defining and implementing a procedure to perform the criticality assessment of the information and ICT assets.

Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

Q6. Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?

2.4.1.4 Section IV: Encryption and cryptography

45. Encryption plays a critical role in safeguarding sensitive data and protecting the integrity, confidentiality, and availability of ICT systems and data. By employing strong encryption algorithms and implementing cryptographic controls, financial entities can significantly reduce the risk of data breaches and unauthorized data manipulation. Encryption also ensures the confidentiality and privacy of communications and information within the financial entity. It prevents unauthorized interception and eavesdropping, ensuring that sensitive data remains confidential and only accessible to authorized individuals.

46. Under the first article of this section, Article 6 (*Encryption and cryptography*), financial entities are required to establish a comprehensive policy on encryption and cryptographic controls, incorporating key elements to effectively manage these security measures. When determining encryption requirements, they should consider data classification and ICT risk assessment results. This policy should also cover the encryption of internal network connections and traffic with external parties, considering data criticality and classification.

47. Proposed Article 6 uses the term "leading practices" on purpose, acknowledging that there may be multiple approaches that are effective and that organizations should strive to identify and adopt the most effective practices for their specific circumstances. Such terminology also suggests a forward-looking perspective, emphasizing the importance of innovation and continuous improvement. This term implies that the identified practices are not static, but rather are constantly evolving, and that organizations need to keep abreast of new developments to maintain their effectiveness.

48. The second article of this section, Article 7 (*Cryptographic key management*), further requires financial entities to establish and document a cryptographic key management policy as an integral part of the overall encryption policy. The cryptographic key management policy should establish guidelines for the correct use, protection, and lifecycle management of cryptographic keys, ensuring their secure generation, storage, distribution, and disposal.

49. When selecting cryptographic technologies and usage practices, financial entities should consider leading practices, reliable techniques, and the classification of involved ICT assets. If they cannot adhere to leading practices or use the most reliable techniques, financial entities should implement

and keep records of mitigation and monitoring measures to maintain resilience against cyber threats.

50. Monitoring developments in cryptanalysis is crucial, and financial entities must update or change their cryptographic technology when necessary to remain resilient. If updating or changing cryptographic technology is not feasible, alternative mitigation and monitoring measures should be adopted.

Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

Q8. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

2.4.1.5 Section V: ICT operations security

51. ICT operations security is vital for financial entities to ensure the secure and reliable operation of their ICT systems and services. By developing and documenting ICT operating procedures, financial entities can effectively manage their ICT assets and mitigate the risk of unauthorized access, intrusions, and data misuse.

52. This section contains five articles on (i) ICT operating procedures, (ii) capacity and performance management, (iii) vulnerability and patch management, (iv) data and system security and (v) logging.

53. ICT operating procedures shall cover key elements such as installation, maintenance, configuration, and deinstallation of ICT assets, as well as controls and monitoring of ICT systems, error handling, and recovery procedures. ICT operating procedures help maintain the availability, authenticity, integrity, and confidentiality of data, while also addressing legacy systems and interdependencies among ICT systems. By adhering to these procedures, financial entities can minimize disruptions to business operations, detect and respond to security incidents promptly, and ensure the continuity and security of their services.

54. In order to preserve the availability, authenticity, integrity, and confidentiality of data, mitigate ICT risk, and ensure the security and integrity of network, financial entities should develop, document and implement procedures on the capacity and performance management, as well as vulnerability and patch management.

55. In terms of capacity and performance management, financial entities need to identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures. The aim is to maintain and enhance the availability and efficiency of ICT systems while preventing capacity shortages. Specific attention should be given to systems with long or complex procurement processes or those that are resource intensive.

56. Regarding vulnerability and patch management, financial entities must establish procedures to detect vulnerabilities and update relevant information resources accordingly. Regular automated vulnerability scanning and assessments, typically using specialized software tools, of ICT assets are required, especially for critical or important functions. Also, ICT third-party service providers should handle any vulnerabilities and report them to the financial entities. The tracking of ICT third-party libraries (including tracking patches and updates), disclosure of vulnerability-related information, and deployment of patches are also vital. Financial entities need to prioritize patch deployment based on vulnerability criticality and risk profiles, while monitoring and verifying remediation.

57. Regarding the automated vulnerability scans, and considering that the main purpose of these scans is to cover the widest range possible of assets in an automated way, ESAs are considering mandating these requirement for all ICT assets, with independence of their classification and overall risk profile, and with the same weekly frequency already included for those ICT assets supporting critical or important functions.

58. Additionally, financial entities should record detected vulnerabilities, evaluate software and hardware patches and updates, test and deploy them in a controlled environment, and establish emergency procedures and deadlines for installation.

59. Another important aspect to ensure the security of networks against intrusions and data misuse, and to preserve the availability, authenticity, integrity and confidentiality of data is the data and system security. To this end, financial entities should implement various security measures outlined in Article 15 of DORA.

60. Finally, developing and implementing logging procedures, protocols, and tools allow financial entities to secure networks, preserve data integrity, and detect anomalies. By identifying events to be logged, setting retention periods, and securing log data, entities can effectively monitor and investigate ICT security incidents. The level of detail in logs should align with their purpose and the usage of the ICT asset producing the log, facilitating accurate analysis.

61. Logging events related to access control, capacity management, change management, and network traffic activities enhances monitoring capabilities. Protecting logging systems and information from tampering ensures data integrity, while clock synchronization aids incident response and forensic analysis. These measures collectively strengthen the security posture of financial entities.

62. Regarding cloud computing resources, ESAs may consider introducing additional requirements to those already included in Article 11(2) point (k). For example, preventive and detective measures to ensure the security in the cloud environment, including tenant security and further resilience model.

Q9. Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

Q10. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q11. What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.

Q12. Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.

2.4.1.6 Section VI: Network security

63. Network security measures are vital for the financial entities overall digital and operational resilience as they establish policies, procedures, protocols, and tools to protect networks, prevent unauthorized access, maintain data confidentiality, integrity, and availability, and ensure secure data transfer. They help financial entities mitigate risks, detect vulnerabilities, and establish a secure network infrastructure that aligns with industry standards and leading practices. This section is split in two articles covering two types of network security measures: network security management and securing information in transit.

64. In terms of network security management, financial entities are required to develop policies, procedures, protocols, and tools to ensure the security of networks. This includes segregation and segmentation of ICT systems and networks based on their criticality, classification, and risk profile. The mapping and visualization of networks provide an overview for effective management. A separate and dedicated network for ICT asset administration, along with strict prohibition of direct internet access, helps mitigate unauthorized access risks. Implementing network access controls prevents connection of unauthorized devices or systems. Encryption of network connections across various networks ensures the confidentiality, integrity, and availability of communication.

65. Designing networks in accordance with security requirements and industry leading practices protects the confidentiality, integrity, and availability of the network. Securing network traffic between internal networks and external connections safeguards against external threats. Regular reviews of connection filters and network architecture help identify potential vulnerabilities. Secure configuration baselines, network hardening, and session termination after inactivity limit potential attack vectors. Additionally, inclusion of ICT and information security measures in network service agreements ensures that security requirements are met for both in-house and outsourced services.

66. Regarding securing information in transit, financial entities must develop policies, procedures, protocols, and tools to protect data transfer. This includes ensuring the availability, authenticity, integrity, and confidentiality of data during network transmission. Measures to prevent data leakage and secure information transfer with external parties are also essential. Confidentiality and non-disclosure arrangements, along with compliance assessments, protect sensitive information. Financial entities should also comply with data protection laws is required for the transfer of personal data.

Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

Q14. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

2.4.1.7 Section VII: ICT project and change management

67. Often, poor ICT project management significantly impacts the achievement of business objectives especially in terms of cost, quality and time in all sizes of firms. Similarly, the lack of proper management of projects and other changes in the ICT domain can be seen as a common source of ICT related incidents.

68. Having an appropriate ICT project and change management framework in place therefore serves two purposes, it helps to maximise the benefits associated with projects, acquisitions and changes and on the other hand it reduces or minimises the negative impacts that can result from such actions.

69. Section VII elaborates on these aspects through three articles. The first one focuses on the relevance of having a project management policy as a basic mechanism for ensuring the security of networks, against intrusions and data misuse and, in order to preserve the availability, authenticity, integrity and confidentiality of data. This article is based on the EBA Guidelines on ICT and security risk management, in particular Section 3.6.1, notably with regard to the elements to be included in the policy.

70. The second article, with the same objectives, establishes the need for a policy regarding ICT systems acquisition, development, and maintenance, focused fundamentally on the testing of these systems and on the security implications that can be derived from these processes.

71. Finally, the third article in this section focuses on procedures related to change management. It has been decided to include change management in the same section as project management, although under certain approaches it can be considered as another element of the ICT operational management area. In any case, regardless of which heading it falls under, proper change management has a similar impact to proper project management, and poor change management is often behind incidents in the ICT field. Once again, the focus is on resilience, and in this line, requirements are established on the testing and approval of changes, on the governance of such changes and on the procedures for making urgent changes or reversing changes made if necessary.

72. These two latter articles both include specific provisions for CCPs and CSDs, replicating the existing EMIR and CSDR L2 provisions requiring them to test their ICT systems (i) prior to their use and (ii) after significant changes[1], to include the minimal list of external stakeholders that CCPs and CSDs should involve in such tests.

[1] respectively, Articles 9(2) of EMIR RTS 2013/153 and Article 75(6) of CSDR RTS 2017/392.

Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

Q16. Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

2.4.1.8 Section VIII: Physical and environmental security

73. Section VIII is focused on covering the requirements related to physical and environmental security as a fundamental part of the ICT risk management framework. Both physical and environmental security are key aspects in the process of ensuring the availability, authenticity, integrity and confidentiality of data and ICT systems.

74. A single article establishes the implementation of a policy in this area, aimed at specifying the elements of this policy with respect to Secure premises, data centres, sensitive designated areas and hardware equipment.

75. The main elements of this policy include measures such as the protection of these ICT assets against unauthorised access, attacks, accidents and from environmental threats and hazards, and the proper maintenance of these assets. It also establishes the need for a clear desk policy for papers and a clear screen policy for information processing facilities.

Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

Q19. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

2.4.1.9 Section IX: ICT and information security awareness and training

76. This section focuses on elaborating on the requirements related to the ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of DORA. These programmes are considered fundamental in order to preserve the availability, authenticity, integrity and confidentiality of data.

77. Thus, requirements are established with respect to elements to be included, the periodicity of such programmes, their review and effectiveness.

Q20. Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

2.4.2 Chapter II: Human resources policy and access control

78. This chapter is intended to cover the mandate set out under Article 15(b) of DORA: "*develop further components of the controls of access management rights referred to in Article 9(4), point (c) [of*

DORA] and associated human resources policy (…)". The chapter covers three firmly related but distinct elements, human resources policy, identity management and access control.

79. DORA, primarily in its Article 9(4)(c), already sets out a requirement to "*implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of controls that address access rights and ensure a sound administration thereof*".

80. Article 20 of the proposed draft RTS focuses, through a single article, on Human resources policy, in particular on the main requirements related to the employment cycle. This article specifies requirements on contracts, covering the pre-employment phase, on communication and awareness, the employment period and on requirements to be considered after the termination of the contractual relationship. In identifying these requirements, controls and measures identified in the ISO/IEC 27001 and ISO/IEC 27002 standards have been considered.

81. Articles 21 and 22 introduce requirements relating to Identity and Access management.

82. Access controls, as part of the ICT risk management framework, help to protect unauthorised access to information and systems, ensure the integrity of information and systems and preserve the confidentiality of data, both internally and externally. The relevance of access control requirements is therefore, for obvious reasons, particularly relevant in the financial sector.

83. Article 21 on Identity Management elaborates on the elements to be included by financial entities, as part of their controls on access management rights, in the policies and procedures to ensure the unique identification of natural persons and systems accessing the financial entities' information. Provisions related to the management of user accounts and linked identities are also included.

84. Article 22 on Access Control sets out the main elements to be included in this policy, which address the following topics: governance, authentication methods, strategy, access rights and physical access.

Q21. Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

Q22. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

2.4.3 Chapter III: ICT-related incident detection and response

85. The management of ICT-related incidents is one of the core elements of DORA. Numerous articles of DORA elaborate on specific aspects linked to ICT-related incidents, such as incident detection (Article 10), incident response (Article 11) or the learning process linked to incidents (Article 13) as well as the whole chapter III of DORA which covers aspects related to ICT-related incident management, classification and reporting.

86. The mandate set out in Article 15(c) of DORA is intended to complement the requirements already included in Level 1, by specifying further the steps that precede the application of Chapter III by identifying the anomalous activities that can develop into ICT-related incidents. It requires to develop further the mechanisms (specified in Article 10(1) of DORA) enabling a prompt detection of anomalous activities and the criteria (set out in Article 10(2) of DORA) triggering ICT-related incident detection and response processes.

87. The latter part of the mandate is covered in Article 23 of the proposed draft RTS (*ICT-related incident management policy*). It includes the requirement to document the ICT-related incident management process referred to in Article 17 of DORA and complements the elements to be included in this process. Further, other elements considered key to help in fulfilling this objective are added, such as the retention of evidence related to ICT-related incidents and the review of the policy.

88. The former part of the mandate is covered under Article 24 of the proposed RTS (*Anomalous activities detection and criteria for ICT-related incidents detection and response*), which provides for more granular requirements for the mechanisms to be established by financial entities to allow the correct detection of anomalous activities that can result in ICT network performance issues and ICT-related incidents and on establishes criteria for the activation of the processes linked to the ICT-related incident detection and subsequent response.

Q23. Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.

2.4.4 Chapter IV: ICT business continuity management

89. ICT systems and services have become essential to the operation of the financial sector, and any disruption to such systems or services can result in a significant impact on business continuity and the provision of critical services to customers and stakeholders.

90. Article 11 of DORA already emphasises the need to ensure adequate response and recovery of ICT systems, requiring the implementation of a business continuity policy and response and recovery plans, as well as adequate testing of these plans.

91. The mandate set out in Article 15, points (d), (e) and (f) of DORA is aimed to elaborate further on these three elements and has been covered through three articles.

92. Article 25 of the proposed draft RTS details the expected components of the ICT business continuity policy. DORA establishes through its Article 11(1) the obligation to implement, as part of the ICT risk management framework, a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity. The proposed article elaborates on the main objectives and

characteristics of this policy and further specifies the minimum elements to be included in the business continuity policy as well as the requirements related to its communication (to be aligned with the relevant requirements already set out in Articles 11 and 14 of DORA).

93. In addition, this article also includes specific provisions for CCPs, CSDs and trading venues, replicating certain requirements from EMIR, CSDR and MIFID 2 Level 2 regulations[2] in place, in particular the maximum two-hour time-recovery objective for their critical functions, the need to consider links and interdependencies with external stakeholders when defining it and, for CCPs, the establishment and maintenance of a secondary site.

94. Article 11(4) of DORA establishes the need to maintain and periodically test ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers. DORA also elaborates on the obligation to conduct a business impact analysis (BIA) and the periodicity of the testing of the plans. Article 26 of the proposed RTS further elaborates on the assumptions to be taken into account, the main elements to be considered in relation to the planning and execution of such tests, as well as the scenarios to be considered and the objectives that testing should help to achieve. For the elaboration of this article the EBA Guidelines on ICT and security risk management (in particular its section 3.7.4) has been largely used.

95. Here also specific provisions have been included to replicate the requirements existing for CCPs and CSDs under EMIR and CSDR L2 regulations[3] to make sure certain selected external stakeholders are involved in this testing.

96. As a fundamental part of the ICT response and recovery mechanisms, financial entities shall implement ICT response and recovery plans in line with the provisions of Article 11 (3) of DORA. Article 27 of the proposed draft RTS further specifies the components of these ICT response and recovery plans. It elaborates on the minimum elements to be considered for the development of the plans and the scenarios to be considered, which include additional scenarios to those already contemplated in Article 11(6), second subparagraph, and Article 15(e) of DORA.

Q24. Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

Q25. Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

2.4.5 Chapter V: Report on the ICT risk management framework review

97. Article 6(5) of DORA establishes the obligation to document and review the ICT risk management framework. This article also establishes proportionality mechanisms, limiting the minimum periodicity for such a review for micro-enterprises. The review should ensure continuous

[2] Cf. Article 17(3) of EMIR RTS 2013/153, Article 78(2) of CSDR RTS 2017/392 and Article 15(2) of MIFID2 RTS 2017/584.

[3] Cf. Article 20(2)(b) of EMIR RTS 2013/153 and Article 79(c) of CSDR RTS 2017/392.

improvement of the ICT risk management framework. As part of the review process, a report on the outcome of the review shall also be generated, which should be sent to the competent authority upon request. The format and content of such a report is the subject of this chapter, which addresses the mandate set out in Article 15(g) of DORA.

98. Such a report should assist, internally, in the proper documentation and implementation of modifications or revisions made and should serve as a basis for a periodic and ongoing review of the ICT risk management framework. As the report should also be submitted, upon request, to the relevant competent authority, it is also important to harmonise the format and content of the document, so that the different stakeholders, both internal and external, are aware of the minimum elements to be included and can access it in an appropriate manner.

99. Both elements, the format and the content, are covered in a unique article. In terms of format requirements, paragraph 1 of this article only requires the report to be in a searchable electronic format. The ESAs believe that whatever format is chosen, it must guarantee the basic aspects of any information flow, but that no unique format for the file that contains it should be mandated, to leave some flexibility to the financial entities.

100. Paragraph 2 of the article elaborates on the content that is expected from such report and cover the minimum elements that shall be included in it. It is not intended to be an exhaustive list for the final report and entities may, as long as they include the information contained in the article, include in the report other elements that they consider useful.

Q26. Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.

2.5 Title II: Simplified ICT risk management framework

Article 16(3) of DORA

The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards in order to:

(a) specify further the elements to be included in the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a);

(b) specify further the elements in relation to systems, protocols and tools to minimise the impact of ICT risk referred to in paragraph 1, second subparagraph, point (c), with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data;

(c) specify further the components of the ICT business continuity plans referred to in paragraph 1, second subparagraph, point (f);

(d) specify further the rules on the testing of business continuity plans and ensure the effectiveness of the controls referred to in paragraph 1, second subparagraph, point (g) and ensure that such

testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails;

(e) specify further the content and format of the report on the review of the ICT risk management framework referred to in paragraph 2.

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations.

101. Financial entities covered by Article 16 of DORA are: small and non-interconnected firms, payment institutions exempted pursuant to Directive (EU)2015/2366, institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation, electronic money institutions exempted pursuant to Directive 2009/110/EC and small institutions for occupational retirement provision. Recital 42 explains the reasons why these categories of entities benefit from lighter ICT risk management requirements. The ESAs understand that in principle, these entities usually are small or very small firms, and when they have, sometimes counting only a handful of employees.

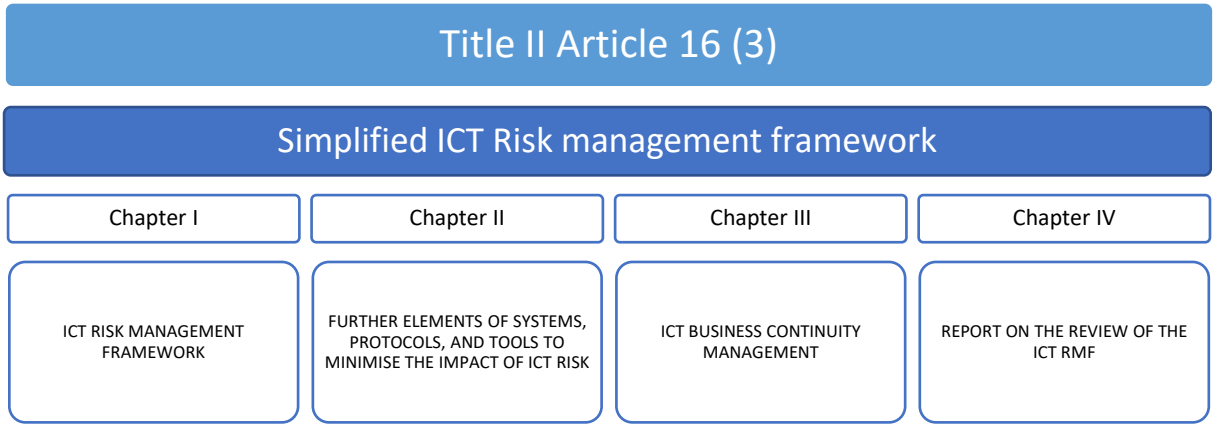
102. To specify the requirements that should apply to these financial entities, the ESAs have considered two sets of provisions in DORA:

a. On the one hand, Article 16(1), first subparagraph of DORA which lists requirements that shall not apply to the financial entities subject to the simplified ICT risk management framework, Articles 5 to 15 of DORA, i.e. the 'general' ICT risk management requirements, as well as Recital 43 of DORA, which details these excluded requirements; and

b. On the other hand, Article 16(1), second subparagraph and Article 16(2) of DORA, which set out a list of 'positive' obligations applicable to those entities.

103. This mandate is covered under the second title of the proposed draft RTS and is divided into 4 chapters: ICT risk management framework, further elements of systems, protocols, and tools to minimise the impact of ICT risk, ICT business continuity management and report on the ICT risk management framework review.

104. This title has been designed in accordance with the principle of proportionality already embedded in Article 16 of DORA, meaning that it is tailored to fit the specific needs and characteristics of these entities. The objective is to strike a balance between ensuring the security of their ICT systems and that of other financial entities, while avoiding excessive regulatory burdens.



105. Below is presented the suggested approach for each of these chapters.

2.5.1 Chapter I – Simplified ICT risk management framework

106. The purpose of this chapter is to cover the mandate established in Article 16(3)(a) of DORA, which requires specifying further the elements to be included in the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a) of the same article. To maintain a high level of digital operational resilience and considering sector-specific Union law, some financial entities are subject to lighter requirements or exemptions for reasons associated with their size and the nature, scale and complexity of the services, activities and operations they provide. These financial entities mentioned in Article 16 of DORA are required to establish and maintain a simplified ICT risk management framework. This framework serves as a comprehensive set of requirements that outlines the necessary mechanisms and measures to effectively manage ICT risk, while also safeguarding the physical components and infrastructures involved.

107. To achieve this, the ESAs believe the framework should encompass various key elements. Firstly, governance and organization provide the foundation for effective ICT risk management by establishing clear roles, responsibilities, and accountability within the organization. This ensures that decision-making processes are defined and that risk management is embedded throughout the entity.

108. Note that the reference in the proposed provisions to 'management body' is not an issue given the broad definition given to that concept in Article 2(30) of DORA, which includes management bodies as they are defined for financial entities in each sectorial legislation and also "*the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law*", which should cater for the situation of the smallest entities.

109. The information security policy is a crucial component as it sets out the overall objectives, principles, and guidelines for protecting the availability, authenticity, integrity and confidentiality of information. It outlines the entity's commitment to safeguarding its data and ICT assets, ensuring compliance with relevant laws and regulations.

110. Classification of information assets and ICT assets allows financial entities to prioritize their resources and efforts by categorizing and understanding the value, sensitivity, and criticality of their information and technology. This classification enables the application of appropriate security measures based on the risk profiles of different assets.

111. The ICT risk management process forms the core of the framework, involving the identification, assessment, mitigation, and monitoring of ICT risk. It ensures that potential risks are identified, analysed, and managed proactively to minimize their impact on operations

112. ICT-related incident management is essential for promptly responding to and recovering from any ICT incidents or breaches that may occur. It establishes procedures and protocols to detect, respond, and mitigate the effects of incidents, reducing potential damage and enhancing resilience.

113. Finally, physical and environmental security addresses the protection of physical components and infrastructures supporting ICT systems. It includes measures to secure data centres, servers, networks, and other critical assets from unauthorized access, theft, natural disasters, or environmental hazards.

114. Including these elements within the simplified ICT risk management framework is crucial as they provide a comprehensive and structured approach to managing ICT risk. They enable financial entities to establish a robust governance framework, protect information assets, assess and mitigate risks effectively, respond to incidents, and safeguard the physical environment supporting ICT systems. By implementing these elements, financial entities can enhance their overall security posture and ensure the continuity and reliability of their ICT operations.

Q27. Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

2.5.2 Chapter II – Further elements of systems, protocols, and tools to minimise the impact of ICT risk

115. To mitigate the impact of ICT risk, financial entities referred to in Article 16 of DORA should employ robust and up-to-date ICT systems, protocols, and tools that are specifically tailored to support their operations and services. These measures are essential in ensuring the security of networks, defending against intrusions, preventing data misuse, and maintaining the availability, authenticity, integrity, and confidentiality of critical data and cover different areas.

116. Access control is vital for financial entities to prevent unauthorized access to their ICT systems and sensitive information. Financial entities should define and implement procedures for logical and physical access control. These procedures should include granting access based on need-to-know and least privileges, ensuring user accountability, managing account rights, using appropriate authentication methods, and regularly reviewing access rights. By following these measures, organizations can restrict access to authorized personnel, minimize unauthorized activities, and

protect data integrity, reducing the risk of breaches and unauthorized manipulation of systems and information.

117. ICT operations security ensures the secure functioning of ICT systems throughout their lifecycle. Financial entities should monitor and manage ICT assets supporting critical functions, assess capacity requirements, perform vulnerability scanning, manage outdated assets, log events, monitor logs for anomalies, stay informed about cyber threats, and implement measures to detect security threats and vulnerabilities. These actions contribute to maintaining the availability, reliability, and continuity of critical systems and services, protecting against unauthorized access, information leakage, malicious code, and other security risks. In addition, considering that the security level of the financial entity is as secure as its weakest point ESAs are considering mandating these requirements for all ICT assets, and not only for those supporting critical or important functions.

118. Ensuring the security of data, systems, and networks is crucial for safeguarding the integrity, confidentiality, and availability of financial information. Financial entities should incorporate various security measures to protect data at all stages, including in use, in transit, and at rest. This involves implementing security measures for software, data storage media, systems, and endpoint devices, as well as preventing and detecting unauthorized connections to networks. Measures are also needed to ensure the secure transmission, deletion, and disposal of data, as well as to address teleworking and cloud computing security. Compliance with data protection regulations and the implementation of strong security measures are essential in maintaining a secure environment.

119. In addition to those requirements ESAs are considering introducing further bespoke requirements for example, secure configuration baseline for ICT systems to minimise the exposure to cyber risk and segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification and overall risk profile of ICT assets using them.

120. Financial entities should also prioritize ICT security testing to proactively identify vulnerabilities and weaknesses within their systems. By conducting comprehensive assessments, penetration testing, and vulnerability scans, they can uncover potential risks and promptly address them. This includes establishing and implementing an ICT security testing plan that considers threats and vulnerabilities specific to the financial entity. Reviews, assessments, and tests should align with the overall risk profile of the entity, and the results should be carefully monitored and evaluated. Any necessary updates to security measures should be implemented promptly, particularly for critical ICT systems. This proactive approach is crucial for maintaining the resilience and security of ICT systems.

121. Financial entities should adhere to secure practices in the acquisition, development, and maintenance of ICT systems. A procedure should be implemented, following a risk-based approach, which includes clearly defining functional and non-functional requirements, obtaining approval

from relevant business management, conducting testing and approval before first use, and identifying measures to mitigate risks during development and implementation. By following these practices, financial entities can mitigate potential vulnerabilities, ensuring the overall security and reliability of ICT systems.

122. Finally, financial entities need robust ICT project and change management processes. They should develop documented procedures covering project initiation to closure, defining roles and responsibilities. Additionally, an ICT change management procedure ensures controlled recording, testing, assessment, approval, implementation, and verification of system changes, preserving digital operational resilience. Proper governance, risk assessment, and control mechanisms reduce the likelihood of introducing vulnerabilities or disruptions, ensuring secure project implementation and system modifications.

123. The requirements contained in the articles included in this chapter have been conveniently adjusted taking into account the size and the overall risk profile of the financial entities subject to the simplified regime, and the nature, scale and complexity of its services, activities and operations compared to the analogous elements included in Title I, such is the case of the articles on Access Control, ICT Operations Security, ICT systems acquisition, development, and maintenance. On the other hand, certain related articles that were presented separately in Title I and with a greater number of requirements, such as Project and change management or Data System and Network Security, have been merged. Finally, requirements related to encryption and cryptography or specific provisions related to human resources, among others, disappear.

124. Regarding cloud computing resources, ESAs may consider introducing additional requirements to those already included in Article 37(2)(h). For example, preventive and detective measures to ensure the security in the cloud environment, including tenant security and further resilience model.

Q28. Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

Q29. What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.

Q30. Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.

2.5.3 Chapter III – ICT business continuity management

125. Financial entities referred to in Article 16 of DORA should also ensure the continuity of their critical functions, especially in case of severe disruptions. By incorporating the components identified under this chapter and conducting regular testing, financial entities enhance their

resilience and minimize disruption impacts. The ICT business continuity plans enable them to safeguard critical operations, protect information assets, and ensure service continuity, even in unforeseen circumstances.

126. The identified components should include conducting a business impact analysis (BIA) to assess potential risks and vulnerabilities, identifying scenarios that ICT assets may face, and developing plans based on the business impact analysis (BIA) and scenario assessment.

127. The ICT business continuity plans should be approved by the management body, documented for easy access, and allocate sufficient resources for execution. They should establish recovery levels and timeframes, specify activation triggers and actions, and outline restoration and recovery measures. Backup policies, alternative options, communication arrangements, insurance arrangements, and plan updates are also included.

128. Financial entities should also test their business continuity plans regularly to ensure their effectiveness. Testing covers backup and restore procedures and occurs at least once a year or during major plan changes. The tests should verify the ability to sustain operations until critical functions are re-established and identify any deficiencies, which are documented, analysed, addressed, and reported.

129. In this chapter, the complexity has been reduced compared to the Business Continuity articles of Title I, among others, the scenarios to be considered or the requirements related to the testing of the plans have been reduced. In general terms, the requirements related to business continuity are maintained but with less granularity, since, for example, no specific requirements are established with respect to Response and Recovery plans.

Q31. Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

2.5.4 Chapter IV – Report on the ICT risk management framework review

130. Financial entities referred to in Article 16 of DORA should submit a report on the review of their ICR risk management framework to the competent authority upon its request. This chapter defines the format and content of the said report trying to strike a balance between the level of details to be included in the report and the size or service provided by these entities. It notably requires financial entities to provide less details on the measures taken to address weaknesses, planned developments, past reports and sources of information used to prepare this report than under the general regime. Finally, as under the general regime, financial entities should send the report in a searchable electronic format.

Q32. Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.

4. Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying further elements to be included in ICT security policies, procedures, protocols and tools, developing further components of the controls of access management rights, developing the mechanisms to detect anomalous activities and the criteria triggering ICT-related incident detection and response processes, specifying further the components of the ICT business continuity policy, the testing of ICT business continuity plans, the components of the ICT response and recovery plans and the content and format of the report on the review of the ICT risk management framework as well as specifying certain elements of the simplified ICT risk management framework

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011[4] and, in particular Articles 15, fourth subparagraph and 16(3), fourth subparagraph thereof,

Whereas:

(1) Financial entities vary widely in their size, structure, and internal organisation and in the nature and complexity of their activities. It is therefore necessary to take into account that diversity while imposing certain fundamental regulatory requirements which are appropriate for all financial entities under the scope of DORA when designing, documenting and implementing the elements specified in this Regulation.

(2) To ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays, financial entities should design, document and implement ICT security policies, procedures, protocols and tools containing elements on governance, ICT risk management process, ICT and information asset management, cryptography, ICT operation security, network security, ICT system acquisition, development and maintenance, physical and environmental security, ICT and information security awareness and training. The abovementioned policies, procedures,

[4] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

protocols and tools related to ICT security should be embedded in and be consistent with the overall ICT risk management framework of the financial entity, which includes all the further policies, procedures, strategies set out in Articles 6 to 14 of Regulation (EU) 2022/2554 and that are not within the scope of this Regulation.

(3) Considering leading practices and, where applicable, relevant international standards, financial entities should develop and implement consistent and up-to-date ICT security policies that support the financial entity's digital operational resilience strategy and the related information security objectives. To ensure compliance, enhance the overall information security awareness and culture of the financial entity and prevent unintentional security breaches, the ICT security policies should be approved by the management body of the financial entity, and should be made available to all stakeholders, including, where necessary, the one outside the financial entity such as ICT third-party service providers.

(4) To ensure accountability, compliance and in order to improve the efficiency of the overall ICT security of the financial entity, financial entities other than microenterprises should specify in their ICT security policy specific tasks and responsibilities of their ICT risk management function referred to in Article 6(4) of Regulation (EU) 2022/2554. The ICT risk management function should be responsible to manage and monitor the ICT risk management process and report on the outcome of the risk assessment to the management body of the financial entity without undue delay. The ICT risk management function and the management body should agree on the format of these reports ensuring that these are clear and can be understood by the management body. The reports should also consider the overall risk management framework of the financial entity. The ICT risk management function should also identify document and review ICT securities policies, procedures, protocols and tools to ensure they are up-to-date and adequate to achieve the ICT an information security objective that the same function should define.

(5) To assess potential risks to their operations and take steps to mitigate or eliminate them and to address ICT risk quickly, efficiently and comprehensively, and to ensure a high level of digital operational resilience, financial entities should have an ICT risk management process in place

(6) The provisions of this Regulation are linked to each other, since they relate to the area of the ICT risk management framework, by detailing specific elements applicable to the financial entities in accordance with Article 15 of Regulation (EU) 2022/2554 or by designing the simplified ICT risk management framework for the financial entities set out in Article 16(1) of the same Regulation. To ensure coherence between those provisions, which should enter into force at the same time, is appropriate to include all the regulatory technical standards required by Article 15, fourth subparagraph, and Article 16(3), fourth subparagraph, into a single Regulation.

(7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority (European Supervisory Authorities), in consultation with ENISA.

(8) The Joint Committee of the European Supervisory Authorities has conducted open public consultations on the draft regulatory technical standards on which this Regulation is

based, analysed the potential related costs and benefits and requested the advice of the of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[5], the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council[6] and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[7],

HAS ADOPTED THIS REGULATION:

[5] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

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

[7] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

TITLE I - FURTHER HARMONISATION OF ICT RISK MANAGEMENT TOOLS, METHODS, PROCESSES AND POLICIES

CHAPTER I

ICT SECURITY POLICIES, PROCEDURES, PROTOCOLS, AND TOOLS

SECTION I

PROVISIONS ON GOVERNANCE

Article 1

General elements of ICT security

1. Financial entities shall ensure that their ICT policies including information security and related procedures, protocols and tools are embedded in the ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols and tools in Chapter I with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays.

2. Financial entities shall ensure that the ICT security policies referred to in paragraph 1:

(a) are aligned to the financial entity's information security objectives included in the digital operational resilience strategy referred to in Article 6 (8) of Regulation (EU) 2022/2554;

(b) contain the indication of the date of approval by the management body;

(c) include control measures to monitor their implementation and to record exceptions in the implementation of the policies. In case of exceptions the digital operational resilience of the financial entity shall be ensured;

(d) set out the responsibilities of staff at all levels to ensure the financial entity's ICT security;

(e) set out the consequences of non-compliance with the policies from staff of the financial entity and ICT third-party service providers accessing the information assets and ICT assets of the financial entity;

(f) list the documentation to be maintained;

(g) specify the segregation of duties arrangements to avoid conflicts of interest, in the context of the three lines of defence model or other internal risk management and control model, as applicable;

(h) consider leading practices and, where applicable, relevant international standards;

(i) identify the roles and responsibilities for their development, implementation and maintenance;

(j) are reviewed in accordance with the requirements set out in in Article 6(5) of Regulation (EU) 2022/2554 and take into account material changes concerning the financial entity, including material changes to activities or processes of the financial entity, or to the cyber threat landscape or to applicable legal obligations.

Article 2

Provisions on governance

1. As part of their ICT security policies, financial entities other than microenterprises shall assign to the control function referred to in Article 6(4) of Regulation (EU) 2022/2554 all of the following tasks and responsibilities:

(a) reporting to and advising the management body, to which the control function shall be accountable, including reporting of the outcome of the risk assessment required by Article 3(1), point (b);

(b) managing and monitoring the financial entity's ICT risk in accordance with requirements laid down in Section II of this regulation and Chapter II of Regulation (EU) 2022/2554;

(c) defining the ICT and information security objectives and setting the qualitative and quantitative measures of their attainment, key performance indicators and key risk metrics referred to in Article 6(8), point (c) of Regulation (EU) 2022/2554;

(d) remaining independent from the function or functions in charge of the ICT development, management, changes and operations;

(e) monitoring the accuracy of classification of information assets and ICT assets referred to in Article 8(1) of Regulation (EU) 2022/2554;

(f) developing and monitoring the effective implementation of ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of Regulation (EU) 2022/2554.

SECTION II

Article 3

ICT risk management

1. Financial entities shall develop, document and implement ICT risk management policy and procedures with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delay. The ICT risk management policy and procedures shall include all of the following:

(a) the indication of the approved risk tolerance levels for ICT risk established according to Article 6(8), point (b) of Regulation (EU) 2022/2554;

(b) the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators to measure impact and likelihood of occurrence of those vulnerabilities and threats;

(c) the procedure to identify, implement and document ICT risk treatment measures for the ICT risk assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance levels of ICT risk of the financial entity. The procedure shall ensure the monitoring of the effectiveness of the measures implemented, the assessment of whether the established risk tolerance levels of the financial entity have been attained and that actions are taken to correct or improve the measures where necessary;

(d) with reference to the ICT risk that are still present following the implementation of the ICT risk treatment measures:

i. the identification of residual ICT risk. The residual ICT risk shall be integrated into the overall risk management process;

ii. the assignment of roles and responsibilities regarding the acceptance of the residual ICT risk that exceed the financial entity's risk tolerance levels for ICT risk established according to Article 6(8), point (b) of Regulation (EU) 2022/2554, and for the review process referred to in point (iii);

iii. the development of an inventory of the accepted residual ICT risk, including an explanation of the reasons for which they were accepted;

iv. provisions on the review of the accepted residual ICT risk at least once a year, including the identification of any changes to the residual ICT risk, the assessment of

available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risk are still valid and applicable.

(e) provisions on the monitoring of any changes to their ICT landscape, internal and external vulnerabilities and threats and of ICT risk to promptly detect changes that could affect the overall ICT risk profile. Financial entities shall verify at least once a year that changes to their business strategy and the digital operational resilience strategy, if any, are taken into account in the overall ICT risk profile.

3. Financial entities shall update the ICT risk management policies and procedures where material changes to the cyber threat landscape, to ICT services, or to ICT assets supporting the business functions occur.

SECTION III

ICT ASSET MANAGEMENT

Article 4

ICT asset management policy

1. As part of the ICT security policies, financial entities shall develop, document and implement a policy on management of ICT assets, with a view to preserving the availability, authenticity, integrity and confidentiality of data.

2. The policy on management of ICT assets shall:

(a) prescribe the monitoring and management of the life cycle of ICT assets identified and classified as required by Article 8(6) of Regulation (EU) 2022/2554, including exceptions, to ensure that they meet and support business and risk management requirements;

(b) prescribe that the financial entity keeps records of all of the following:

i. unique identifier of each ICT asset;

ii. information on the location, either physical or logical, of all ICT assets;

iii. the classification of ICT assets, as specified in Article 8 of Regulation (EU) 2022/2254;

iv. the identity of ICT asset owner;

v. apart from microenterprises, the information needed to perform specific ICT risk assessment on all legacy ICT systems;

vi. business functions or services supported by the ICT asset;

vii. the ICT business continuity requirements, including recovery time objectives and recovery points objectives

viii. whether the ICT asset can be or is exposed to external networks, including the internet;

ix. the links and interdependencies among ICT assets and the business functions using each ICT asset.

Article 5

ICT asset management procedure

1. Financial entities shall develop, document and implement an ICT asset management procedure, with a view to preserve the availability, authenticity, integrity and confidentiality of data.

2. Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. The assessment shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities.

SECTION IV

ENCRYPTION AND CRYPTOGRAPHY

Article 6

Encryption and cryptographic controls

1. As part of their ICT security policies, financial entities shall develop, document and implement a policy on encryption and cryptographic controls, with a view to preserve the availability, authenticity, integrity, and confidentiality of data.

2. The policy on encryption and cryptographic controls shall include all the following elements:

(a) rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification and ICT risk assessment processes to protect the availability, authenticity, integrity and confidentiality of data. If encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment to ensure the confidentiality, integrity and availability of data.

(b) rules for the encryption of internal network connections and traffic with external parties, which shall protect availability, authenticity, integrity and confidentiality of data, taking into account the criticality and the approved data classification and ICT risk assessment processes.

(c) a cryptographic key management policy establishing the correct use, protection and lifecycle of cryptographic keys, in accordance with Article 7;

3. Financial entities shall include in the policy on encryption and cryptographic controls criteria to select cryptographic techniques and use practices taking into account leading practices, appropriate techniques referred to in international standards and the classification of ICT assets involved established according to Article 8(1) of Regulation (EU) 2022/2554. Where the financial entity cannot adhere to the leading practices or use the most reliable techniques, it shall adopt mitigation and monitoring measures to ensure resiliency against cyber threats.

4. Financial entities shall include in the policy on encryption and cryptographic controls provisions to monitor developments in cryptanalysis and, where necessary, update or change the cryptographic technology to ensure they remain resilient against cyber threats. Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats.

5. Financial entities shall include in the policy on encryption and cryptographic controls the requirement to record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4 and the reasons for doing so.

Article 7

Cryptographic key management

1. Financial entities shall lay out in the cryptographic key management policy referred to in Article 6(2), point (d) the requirements for managing cryptographic keys through their whole lifecycle, including generating, storing, backing up, archiving, retrieving, transmission, retiring, revoking and destroying keys.

2. Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification. The controls shall be designed taking into account the results of the approved data classification and the ICT risk assessment processes.

3. Financial entities shall develop and implement methods to recover the cryptographic keys in the case of lost, compromised or damaged keys.

4. Financial entities shall create and maintain a register for all certificates and certificate storing devices. The register shall be kept up-to date.

SECTION V

ICT OPERATIONS SECURITY

Article 8

ICT operating policies and procedures

1. As part of the ICT security policies and procedures, financial entities shall develop, document and implement ICT operating policies and procedures to manage the operations of ICT assets, with a view to ensuring the security of networks, against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data. These procedures shall define how financial entities operate, monitor, control and restore their ICT assets, including the documentation of ICT operations.

2. The ICT operating policies and procedures referred to in paragraph 1 shall cover all of the following elements:

(a) ICT systems description, including all of the following:

i. secure installation, maintenance, configuration and deinstallation of ICT assets;

ii. management of information assets used by ICT assets, including their processing and handling, automated and manual;

iii. identification and control of legacy ICT systems.

(b) Controls and monitoring of ICT systems, including all of the following:

i. backup and restore requirements of ICT systems;

ii. scheduling requirements, taking into consideration interdependencies among the ICT systems;

iii. protocols for audit-trail and system log information;

iv. requirements to ensure that the performance of internal audit and other testing minimises disruptions to business operations.

v. requirements on the segregation of ICT production environments from development, testing and other non-production environments. The segregation shall consider all the components of an environment, such as accounts, data or connections, in accordance with Article 13(1) point (a);

(c) Error handling concerning ICT systems, including all of the following:

i. guidelines for handling errors;

ii. support and escalation contacts, including external support contacts in case of unexpected operational or technical issues;

iii. ICT system restart, rollback and recovery procedures for use in the event of ICT system disruption.

Article 9

Capacity and performance management

1. As part of the ICT security procedures financial entities shall develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve availability and efficiency of ICT systems and prevent ICT capacity shortages before they materialise.

2. The capacity and performance management procedures shall ensure that appropriate measures are taken to cater for the specificities of ICT systems with long or complex procurement or approval processes or that are resource-intensive.

Article 10

Vulnerability and patch management

1. As part of the ICT security procedures, financial entities shall develop, document and implement vulnerability management procedures, with a view to ensuring the security of networks, against intrusions and data misuse, in order to preserve the availability, authenticity, integrity and confidentiality of data.

2. These procedures shall:

(a) identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities;

(b) ensure the performance of automated vulnerability scanning and assessments on ICT assets commensurate to their classification and overall risk profile of the ICT asset. For those supporting critical or important functions it shall be performed at least on a weekly basis.

(c) ensure that ICT third-party service providers handle any vulnerabilities related to the ICT services provided to the financial entity and report them to the financial entity. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root cause and implement appropriate solutions;

(d) track the usage of third-party libraries, including open source, monitoring the version and possible updates;

(e) establish procedures for responsible disclosure of vulnerabilities to clients and counterparts as well as to the public, as appropriate;

(f) deploy patches to address identified vulnerabilities. If no patches are available for a vulnerability, financial entities shall identify and implement other mitigation measures;

(g) prioritise the deployment of patches and of the other mitigation measures, where applicable pursuant to point (f). For the purposes of the prioritisation, financial entities shall consider the criticality of the vulnerability, the classification and risk profile of the ICT assets affected by the identified vulnerabilities;

(h) monitor and verify the remediation of vulnerabilities;

(i) prescribe the recording of any detected vulnerabilities affecting ICT systems and the monitoring of their resolution.

3. As part of the ICT security procedures, financial entities shall develop, document and implement patch management procedures, with a view to ensuring the security of networks, against intrusions and data misuse, in order to preserve the availability, authenticity, integrity and confidentiality of data.

4. These procedures shall:

(a) identify and evaluate available software and hardware patches and updates using automated tools, to the extent possible.;

(b) identify emergency procedures for the patching and updating of ICT assets;

(c) test and deploy software and hardware patch and updates in an environment, which replicates the production one, to avoid adverse consequences and disruption before their deployment to production environments;

(d) set deadlines for the installation of software and hardware patches and updates and escalation procedures if case the deadline cannot be met.

Article 11

Data and system security

1. As part of the ICT security procedures, with a view to ensuring the security of networks and information systems, against intrusions and data misuse, in order to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a data and system security procedure.

2. The data and system security procedure shall include all of the following elements related to data and ICT system security, in accordance with the classification performed pursuant to Article 8(1) of Regulation (EU) 2022/2554:

(a) the access restrictions, in line with Chapter II Section II of this Regulation, supporting the protection requirements for each level of classification;

(b) identification of secure configuration baseline for ICT assets taking into account leading practices, appropriate techniques referred to in international standards that will minimise their exposure to cyber threats, and measures to verify regularly that these baselines are those that are effectively deployed;

(c) identification of security measures so that only authorised software is installed in ICT systems and end point devices;

(d) identification of security measures against malicious code;

(e) identification of security measures to ensure the use of only authorised data storage media, systems and endpoint devices to transfer and store data of the financial entity;

(f) requirements to secure the use of portable endpoint devices and private non-portable endpoint devices as follows:

i. the use of a centralised management solution to remotely manage the endpoint devices and remotely wipe the financial entity's data;

ii. the use of security mechanisms that cannot be modified, removed or bypassed by staff members or ICT third-party service providers;

iii. the authorisation to use removable data storage devices only where the residual ICT risk remains within the financial entity's risk tolerance levels;

(g) the process to securely delete data on-premises or stored externally that the financial entity no longer needs to collect or to store;

(h) the process to securely dispose or decommission of data storage devices on premises or stored externally containing confidential information;

(i) the identification and implementation of security measures to prevent data loss and leakage for systems and endpoint devices;

(j) the implementation of security measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the ICT security of the financial entity.

(k) for cloud computing resources:

i. the requirement that the individual in charge of using the cloud client interface to manage the cloud computing resource shall have adequate competences and training in the management and security of cloud computing resources that are specific to the cloud service used;

ii. implement technical and organisational security measures on the credentials used to access the cloud client interface to manage the cloud computing resource.

Article 12

Logging

1. As part of the safeguards against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement logging procedures, protocols and tools.

2. The logging procedures, protocols and tools shall include all the following:

(a) the identification of the events to be logged, the retention period of the logs and the measures to secure and handle the log data, considering the purpose for which the logs are created;

(b) Alignment of the level of detail of the logs with their purpose and usage to enable effective detection of anomalous activities as specified under Article 24 of this Regulation

(c) the requirement to log events related to all of the following:

i. logical and physical access control and identity management;

ii. capacity management;

iii. change management;

iv. ICT operations, including ICT system activities;

v. network traffic activities, including ICT network performance;

(d) the indication of the retention period of the logs. The retention period shall be defined taking into account the business and information security objectives, the reason for recording the event in the logs and the results of the ICT risk assessment.

(e) measures to protect logging systems and log information against tampering, deletion, and unauthorised access at rest, in transit, and, where relevant, in use;

(f) measures to detect failure of logging systems;

(g) the synchronisation of the clocks of all the financial entity's ICT systems upon a single reliable reference time source.

SECTION VI

NETWORK SECURITY

Article 13

Network security management

1. As part of the safeguards to ensuring the security of networks, against intrusions and data misuse and, in order to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement policies, procedures, protocols and tools on network security management, including all of the following:

(a) segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification and overall risk profile of ICT assets using them;

(b) mapping and visual representation of all the financial entity' networks and data flows;

(c) use of a separate and dedicated network for the administration of ICT assets and prohibition of direct internet access from and to devices or servers used for information system administration;

(d) identification and implementation of network access controls to prevent and detect connection to the financial entity's network by any unauthorised device or system, or any endpoint not meeting financial entity's security requirements;

(e) encryption of network connections passing over corporate networks, public networks, domestic networks, third party networks and wireless networks, for all communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment and in accordance with the rules set out in Article 6(2);

(f) design of networks in accordance with ICT security requirements and taking into account leading practices to ensure the confidentiality, integrity and availability of the network;

(g) securing the network traffic between the internal networks and the internet and other external connections;

(h) identification of the roles and responsibilities for the definition, implementation, approval, change and review of firewall rules and connections filters. Financial entities shall perform the review on a regular basis according to the classification and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions, the financial entities shall perform this review at least every six months;

(i) performance of reviews of the network architecture and of the network security design once a year to identify potential vulnerabilities;

(j) measures to temporarily isolate, where necessary, subnetworks and network components and devices;

(k) implementation of a secure configuration baseline of all network components and hardening the network and network devices according to vendor instructions, industry standards and leading practices;

(l) procedures to limit, lock, and terminate system and remote sessions after a predefined period of inactivity;

(m) with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services, whether these services are provided in-house or outsourced;

Article 14

Securing information in transit

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect information in transit. In particular, financial entities shall ensure all of the following:

(a) the availability, authenticity, integrity and confidentiality of data during network transmission, as well as the establishment of procedures to assess compliance with these requirements;

(b) the prevention and detection of data leakage and the secure transfer of information between the financial entity and external parties;

(c) that requirements on confidentiality or non-disclosure arrangements reflecting the financial entity's needs for the protection of information are implemented, documented and regularly reviewed, for both staff of the financial entity and of third parties, in line with the requirements included under article 28 of Regulation (EU) 2022/2554;

SECTION VII

ICT PROJECT AND CHANGE MANAGEMENT

Article 15

ICT project management

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement an ICT project management policy.

2. The ICT project management policy shall define the elements to ensure effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the financial entity's ICT systems.

3. The ICT project management policy shall include all of the following elements:

(a) project objectives

(b) project governance, including roles and responsibilities;

(c) project planning, timeframe and steps;

(d) project risk assessment;

(e) key milestones;

(f) change management requirements;

(g) testing of all requirements, including security requirements, and respective approval process when deploying an ICT system in the production environment.

4. Financial entities shall ensure that the staff dedicated to an ICT project includes staff from business activities or functions impacted by that ICT project and that it has the necessary knowledge to ensure the secure and successful project implementation.

5. The establishment and progress of ICT projects impacting critical or important functions and their associated risks shall be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, periodically and, where necessary, on an event-driven basis, in accordance with ICT project risk assessment included in paragraph 3, point (d).

Article 16

ICT systems acquisition, development, and maintenance

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development and maintenance of ICT systems. This policy shall:

(a) identify security practices and methodologies relating to acquisition, development and maintenance of ICT systems;

(b) require the identification of functional and non-functional requirements relating to acquisition, development and maintenance of ICT systems, including ICT security requirements and their approval by the relevant business function and ICT asset owner according to the financial entity's internal governance arrangements;

(c) define measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development, maintenance and deployment in the production environment.

2. Financial entities shall develop, document and implement an ICT systems acquisition, development, and maintenance procedure, for testing and approval of all ICT systems prior to their use and after maintenance. The level of testing shall be commensurate to the criticality of the concerned business procedures and ICT assets. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. Financial entities shall use test data and environments that adequately represent the production environment. In addition:

(a) a CCP shall involve, as appropriate, in the design and conduct of these tests, clearing members and clients, interoperable CCPs and other interested parties;

(b) a CSD shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other CSDs, other market infrastructures, and any other institutions with which interdependencies have been identified in its business continuity policy.

3. Financial entities shall conduct the development and testing in environments which are segregated from the production environment.

4. Financial entities shall perform source code review covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and applications. Financial entities shall identify and analyse anomalies in the source code, adopt an action plan to address them and monitor their implementation.

5. Financial entities shall perform security testing of software packages not later than the integration phase.

6. Financial entities shall protect the integrity and confidentiality of data in non-production environments. Non-production environments shall only store anonymized, pseudonymized or randomized production data.

7. By way of derogation from the first subparagraph, financial entities may store production data only for specific testing occasions, for limited periods of time and following the approval by the relevant function and the reporting of such occasions to the ICT risk management function.

8. Financial entities shall implement controls to protect the integrity of the source code of ICT systems that are developed in-house or by an ICT third-party service provider and delivered to the financial entity by an ICT third-parties service provider.

9. The source code and proprietary software provided by ICT third-party service providers or coming from open-source projects shall be analysed and tested for vulnerabilities and for absence of malicious codes in accordance with paragraph 4 prior to the deployment in the production environment.

10. Financial entities' procedures referred in this article shall also apply to ICT systems developed or managed by users outside the ICT function, using a risk-based approach. Financial entities shall establish and maintain a register of these applications that support their critical or important functions, in line with requirements under Article 5.

Article 17

ICT change management

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement ICT change management procedures.

2. Financial entities shall include in the ICT change management procedures, in respect of all changes to software, hardware, firmware components, systems or security parameters, all of the following elements:

(a) verification that ICT security requirements have been met;

(b) mechanisms to ensure independence between the functions that approve changes and those responsible for requesting and implementing them;

(c) definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is an effective quality assurance;

(d) documentation and communication of change details, including purpose and scope of the change, the timeline for implementation and the expected outcomes;

(e) identification of fall-back procedures and responsibilities, including procedures and responsibilities for aborting changes or recovering from changes not successfully implemented;

(f) procedures, protocols and tools to manage emergency changes that provide adequate safeguards;

(g) procedures to document, re-evaluate, assess and approve after their implementation emergency changes, including workarounds and patches;

(h) identification of potential impact of a change on existing ICT security measures and assessment of whether it requires the adoption of additional ICT security measures.

3. After making significant changes to its systems, CCPs and CSDs shall submit their ICT systems to stringent testing by stimulating stressed conditions:

(a) a CCP shall involve, as appropriate, in the design and conduct of these tests: clearing members and clients, interoperable CCPs and other interested parties;

(b) a CSD shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other CSDs, other market infrastructures, and any other institutions with which interdependencies have been identified in its ICT business continuity policy.

SECTION VIII

Article 18

Physical and environmental security

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall define, document and implement a physical and environmental security policy, which shall be designed according to the threat landscape and to the classification and overall risk profile of ICT assets and information assets that can be accessed.

2. The physical and environmental security policy shall include all of the following:

(a) measures to protect the premises, data centres of the financial entity and sensitive designated areas identified by the financial entity where ICT assets and information assets reside from unauthorised access, attacks, accidents and from environmental threats and hazards. The measures to protect from environmental threats and hazards shall be commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there;

(b) measures to secure ICT assets, both within and outside the premises of the financial entity, taking into account the results of the ICT risk assessment related to the relevant ICT assets. The physical and environmental security policy shall include measures to provide appropriate protection to unattended ICT assets;

(c) measures to ensure the availability, authenticity, integrity and confidentiality of ICT assets, information assets and physical access control devices of the financial entity through the appropriate maintenance;

(d) measures to preserve availability, authenticity, integrity and confidentiality of the data, including a clear desk policy for papers and a clear screen policy for information processing facilities.

SECTION IX

Article 19

ICT and information security awareness and training

1. Financial entities shall include in specific ICT security awareness programmes and digital operational resilience training elements regarding the security of networks, the safeguards against intrusions and data misuse and the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, including the cryptographic techniques used. The ICT security awareness programmes and digital operational resilience training shall be aligned to the overall ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of Regulation (EU) 2022/2554.

2. The programmes and training shall be conducted at least yearly and financial entities shall implement processes to regularly evaluate and review their effectiveness and to incorporate lessons learned from their analysis of the ICT-related incidents and cyber threat information into their ICT security awareness programmes and digital operational trainings.

CHAPTER II

HUMAN RESOURCES POLICY AND ACCESS CONTROL

Article 20

Human resources policy

1. As part of their human resource policy, financial entities shall include all the following ICT security related elements:

(a) identification and assignment of any specific information security responsibilities;

(b) requirements for staff and ICT third-party service providers to:

i. be informed about, and adhere to, the financial entity's ICT security policies, procedures and protocols;

ii. be aware of the reporting channels put in place by the financial entity for the purpose of detection of anomalous activities, including those established according to Directive (EU) 2019/1937:

iii. upon termination of employment, requirements for the staff to return to the financial entity all ICT assets and information assets that belong to the financial entity.

Article 21

Identity management

2. As part of their control of access management rights, financial entities shall develop, document and implement identity management policies and procedures to ensure the unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights, in accordance with Article 22.

3. These policies and procedures shall include all of the following elements:

(a) A unique identity corresponding to a unique user account shall be assigned to each staff member of the financial entity or staff of the third-party service providers accessing the information assets and ICT assets of the financial entity. These identities shall be linked to a specific natural person also in the case of reorganisation or after the contractual relationship has ended without prejudice to the retention requirements set out in EU and national law. Financial entities shall maintain records containing every identity assignment.

(b) A lifecycle management process for identities and accounts managing the creation, change, recertification, temporary deactivation and termination of user accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process.

Article 22

Access control

1. As part of their control of access management rights, financial entities shall develop, document and implement a policy that includes all of the following elements:

(a) access rights to ICT assets based on need-to-know, need-to-use and least privilege principles, including for remote and emergency access;

(b) segregation of duties designed to prevent unjustified access to critical data or to prevent the allocation of combinations of access rights that may be used to circumvent controls;

(c) user accountability, by limiting as much as possible the use of generic and shared user accounts and ensuring that users can be identified for the actions performed in the ICT systems at all times;

(d) restrictions of access to ICT assets, setting out controls and tools to block unauthorised access;

(e) account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. The procedures shall include all the following:

i. the assignment of roles and responsibilities for granting, reviewing, and revoking access rights. Retention period for logs shall be defined in accordance with Article 12(2), point (d).

ii. assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Whenever possible, for the performance of administrative tasks on ICT systems, dedicated accounts shall be used. Where applicable, financial entities shall deploy automated solutions for the privilege access management.

iii. withdrawal of access rights upon termination of employment or when the access is no longer required, without undue delay.

iv. review of access rights, at least once a year for all ICT systems, other than critical ICT systems and at least every six months for ICT systems supporting critical or important functions. Review of access rights shall be performed also whenever a change is necessary at user level.

(f) authentication methods including all the following:

i. the use of authentication methods commensurate to the classification and overall risk profile of ICT assets and considering leading practices;

ii. the use of strong authentication methods in accordance with leading practices and techniques for remote access to the financial entity's network, for privileged access, for access to ICT assets supporting critical or important functions or that are publicly accessible.

(g) physical access controls measures including:

i. identification of natural persons who are authorised to enter the critical locations of operation of the financial entity and the recording of every entry to its premises;

ii. granting of physical access rights to critical ICT assets to authorised persons only according to the need-to-know, least privilege principles and on an ad-hoc basis.

iii. monitoring of physical access to premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. The monitoring should be commensurate to the classification of the assets and the criticality of the area accessed.

iv. review of physical access rights to ensure that unnecessary access rights are promptly revoked.

CHAPTER III

ICT-RELATED INCIDENT DETECTION AND RESPONSE

Article 23

ICT-related incident management policy

1. As part of the mechanisms to detect anomalous activities and ICT-related incidents, the financial entities shall develop, document, and implement an ICT-related incident policy through which they shall:

(a) document the ICT-related incident management process referred to in Article 17 of Regulation (EU) 2022/2554;

(b) establish a list of contacts with internal functions and external stakeholders that are directly involved in ICT operations security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management;

(c) establish, implement and operate technical, organisational, and operational mechanisms to support the ICT-related incident policy, including mechanisms to enable a prompt detection of anomalous activities and behaviours in accordance with Article 24 of this Regulation;

(d) retain all evidence relating to ICT-related incidents for a period no longer than necessary for the purposes for which the data is collected and commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets. This evidence shall be retained in a secure manner and in accordance with the relevant provisions on personal data.

(e) establish and implement mechanisms to analyse recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents;

(f) review and update at least once a year the ICT-related incident management policy, its procedures, protocols, and tools. The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios.

Article 24

Anomalous activities detection and criteria for ICT-related incidents detection and response

1. Financial entities shall set clear roles and responsibilities to effectively detect and respond to ICT-related incidents and anomalous activities.

2. To detect anomalous activities that can result in ICT network performance issues and ICT-related incidents in accordance with Article 10(1) of Regulation (EU) 2022/2554, financial entities shall implement detection mechanisms allowing them to:

(a) collect and analyse all the following information on:

i. internal and external factors, including business and ICT administrative functions;

ii. potential internal and external threats, including usual scenarios of detection used by threat actors and scenarios based on threat intelligence activity

(b) identify and implement tools generating alerts of anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. This shall include tools that provide automated alerts based on pre-defined rules to identify any anomalies with the completeness and the integrity of the data sources, monitor the log collection and issue an alert if the log collection failed;

(c) define the alerts referred to in point (b), to allow the detection of ICT-related incidents to be managed within the expected recovery time, both during and outside working hours

(d) proactively monitor and analyse the logs collected in accordance with Article 12 ensuring that all scenarios identified under point 2(a)(ii), and the alerts specified in point (b) of this paragraph;

(e) record, analyse and evaluate all information on all anomalous activities and behaviours automatically where possible, or manually by staff;

3. Any recording of the anomalous activities shall be protected against tampering and unauthorised access at rest, in use, where relevant, and in transit.

4. The financial entity shall log all relevant information for each detected anomalous activity, to enable identification of the data, time of occurrence and detection and the type of the anomalous activity.

5. Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes:

(a) indications that malicious activity may have been carried out in an ICT system or network or that such ICT system or network may have been compromised;

(b) data losses detected, in relation to availability, authenticity, integrity and, confidentiality of data;

(c) adverse impact detected on financial entity's transactions and operations;

(d) ICT Systems and network unavailability;

(e) problems reported by users of the financial entity;

(f) ICT-related incident notification from an ICT third-party service provider of the financial entity detected in the ICT systems and networks of the ICT third-party service provider and which may affect the financial entity.

(g) for the response processes financial entities shall also consider the criticality of the services affected;

CHAPTER IV

ICT BUSINESS CONTINUITY MANAGEMENT

Article 25

Components of the ICT business continuity policy

1. Financial entities shall include in the ICT business continuity policy all of the following:

(a) definition of the objectives, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA) referred to in Article 11(5) of Regulation (EU) 2022/2554;

(b) definition of the scope, including limitations and exclusions, to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;

(c) definition of the timeframe to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;

(d) description of the criteria to activate ICT business continuity plans, ICT response and recovery plans and crisis communications plans;

(e) provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the ICT business continuity policy and to ensure that sufficient resources are available;

(f) provisions on the alignment between the ICT business continuity plans and the overall business continuity plans. The alignment shall concern at least all of the following:

i. potential failure scenarios, including those listed in Article 27(2);

ii. recovery objectives, specifying that the financial entity shall be able to recover the operations of its critical or important functions after disruptions within a recovery time objective and a recovery point objective;

(g) provisions on the development of specific ICT business continuity plans for severe business disruptions, prioritising ICT business continuity actions using a risk-based approach;

(h) provisions on the development, testing and review of ICT response and recovery plans, in accordance with Articles 26 and 27;

(i) provisions on the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26;

(j) provisions to align the ICT business continuity policy to the communication policy referred to in Article 14 (2) and to communication and crisis communication actions referred to in Article 11(2)(e) of Regulation (EU) 2022/2554.

2. In addition to the requirements referred to in paragraph 1, central counterparties shall ensure that their ICT business continuity policy:

(a) includes a maximum recovery time for its critical functions that is not higher than two hours. End of day procedures and payments shall be completed on the required time and day in all circumstances.

(b) takes into account external links and interdependencies within the financial infrastructures including trading venues cleared by the central counterparty, securities settlement and payment systems and credit institutions used by the central counterparty or a linked central counterparty;

(c) requires that arrangements are in place to:

i. ensure continuity of their critical or important functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions, and fail over and recovery to a secondary site;

ii. maintain a secondary processing site capable of ensuring continuity of their critical or important functions identical to the primary site. The secondary processing site shall have a geographical risk profile which is distinct from that of the primary site;

iii. maintain or have an immediate access to a secondary business site, at least, to allow staff to ensure continuity of the service if the primary location of business is not available;

iv. consider the need for additional processing sites, in particular if the diversity of the risk profiles of the primary and secondary sites does not provide sufficient confidence

that the central counterparty's business continuity objectives will be met in all scenarios.

3. In addition to the requirements referred to in paragraph 1, central securities depositories shall ensure that the ICT business continuity policy:

(a) takes into account any links and interdependencies to at least users, critical utilities and critical service providers, other central securities depositories and other market infrastructures.

(b) requires its ICT business continuity arrangements to ensure that the recovery time objective for their critical or important functions shall not be longer than two hours.

4. In addition to the requirements referred to in paragraph 1, trading venues shall ensure that its ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is close to zero.

Article 26

Testing of the ICT business continuity plans

1. Financial entities shall test the ICT business continuity plans taking into account the financial entity's BIA and the ICT risk assessment referred to in Article 3(1) point (b) of this Regulation.

2. Financial entities shall assess through the testing of their ICT business continuity plans whether they are able to sustain the viability of their business until critical operations are re-established. The testing of the ICT business continuity plan shall:

(a) be performed on the basis of realistic test scenarios that simulate potential disruption, including an adequate set of severe but plausible scenarios. The testing scenarios considered for the development of the business continuity plans shall always be included in the testing;

(b) include the testing of ICT services provided by ICT third-parties service providers, where applicable;

(c) include the successful switchover of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;

(d) be designed to challenge the assumptions on which business continuity plans rest, including governance arrangements and crisis communication plans;

(e) include procedures to verify the ability of the financial entities staff, of ICT third-party service providers, of ICT systems and ICT services to respond adequately to the scenarios defined in Article 27(2).

3. In addition to the requirements referred to in paragraph 2, for central counterparties the testing of their ICT business continuity plans shall include the involvement of clearing members, external providers and relevant institutions in the financial infrastructure with which interdependencies have been identified in its business continuity policy.

4. In addition to the requirements referred to in paragraph 2, for central securities depositories the testing of their ICT business continuity plans shall include the participation of, as appropriate, users of the central securities depositories, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in its business continuity policy.

5. Test results shall be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.

6. Financial entities shall review ICT business continuity plans at least once a year taking into account the results of the tests, the most recent threat intelligence and lessons derived from previous events, and, where relevant, any changes in the recovery objectives, including recovery time objectives and recovery point objectives, and/or changes in the business functions, supported by ICT processes and information assets.

Article 27

ICT response and recovery plans

1. Financial entities shall develop ICT response and recovery plans taking into account the results of the BIA. The ICT response and recovery plans shall:

(a) specify the conditions prompting their activation and any exceptions;

(b) describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least the critical ICT systems and service of the financial entities;

(c) be designed to meet the recovery objectives of the operations of financial entities;

(d) be documented and made available to the staff involved in the execution of the plan and readily accessible in case of emergency. Financial entities shall clearly define roles and responsibilities to that extent;

(e) provide for both short-term and long-term recovery options including partial systems and recovery;

(f) lay down the objectives of the plan and the conditions to declare successful execution of the plan;

(g) be updated in accordance with lessons derived from ICT-related incidents, results of tests, newly identified risks and threats, and recovery objectives and priorities amended in accordance with recommendations stemming from audit checks or supervisory reviews.

2. The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios shall include all of the following:

(a) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities;

(b) scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider;

(c) partial or total failure of premises, including office and business premises, and data centres;

(d) substantial failure of ICT assets or of the communication infrastructure;

(e) the non-availability of a critical number of staff or key staff members;

(f) natural disasters, pandemic situations and physical attacks, including intrusions and terrorist attacks;

(g) insider attack;

(h) political and social instability, including, where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed;

(i) widespread power outage.

3. The ICT response and recovery plans shall consider alternative options where the primary recovery measures may not be feasible in the short term because of cost, risks, logistics or unforeseen circumstances.

4. As part of the response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers which are of key importance for a financial institution’s ICT service continuity.

CHAPTER V

REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW

Article 28

Format and content

1. Financial entities shall develop and document the report referred to in Article 6(5) of Regulation (EU) 2022/2554 in a searchable electronic format.

2. Financial entities shall include all of the following information in the report:

(a) an introductory section which:

i. clearly identifies the financial entity which is the subject of the report, and describes its group structure where relevant;

ii. describes the purpose of the report;

iii. describes the context of the report in terms of the nature, scale and complexity of the financial entity's services, activities and operations, its organisation, identified critical functions, strategy, major ongoing projects or activities, relationships and its dependence on in-house and contracted ICT services and systems (or the implications of the total loss or severe degradation of such systems would mean in terms of critical or important functions and market efficiency);

iv. summarises major changes in the ICT risk management framework since the previous report;

v. provides an executive level summary of the current and near-term ICT risk profile, threat landscape, the assessed effectiveness of its controls and hence security posture of the financial entity;

(b) date of the approval of the report by the management body of the financial entity;

(c) description of the reason for the review of the ICT risk management framework in accordance with Article 6 (5) of Regulation (EU) 2022/2554. Where the review was initiated following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes, the report shall contain explicit references to such documents or instructions, allowing the identification of the reason for initiating the review. Where the review was initiated following ICT-related incidents, the report shall contain the list of all ICT-related incidents with incident root-cause analysis;

(d) start and end dates of the review period;

(e) indication of the function responsible for the review;

(f) description of the major changes and improvements to the ICT risk management framework since the previous review. This description shall include an analysis of the impact of the changes on the financial entity's digital operational resilience strategy, on the financial entity's ICT internal control framework and on the financial entity's ICT risk management governance;

(g) summary of the findings of the review and detailed analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period;

(h) description of the measures to address identified weaknesses, deficiencies and gaps, including all of the following:

i. summary of measures taken to remediate to identified weaknesses, deficiencies and gaps;

ii. expected date for implementing the measures and dates related to the internal control of the implementation, including information on the state of progress of their implementation as at the date of drafting of the report, explaining where applicable if there is a risk that deadlines may not be respected;

iii. tools to be used and identification of the staff in charge for carrying out the measures, detailing whether they are internal or external;

iv. description of the impact of the changes envisaged in the measures on the financial entity's budgetary, human and material resources, including resources dedicated to the implementation of corrective measures;

v. information on the process for informing the competent authority in case of major and immediate deficiency;

vi. if the weaknesses, deficiencies or gaps identified are not subject to remedial measures, a detailed explanation of the criteria used to analyse their impact, to evaluate the related residual risk and for the acceptance of such a risk;

(i) information on planned further developments;

(j) overall conclusions on the review of the ICT risk management framework;

(k) information on past reviews:

i. list of past reviews to date;

ii. if applicable, state of implementation of remedying measures identified by the last report;

iii. where applicable, description of whether the proposed remedying measures in past reviews have proven ineffective or created unexpected challenges, and how they could be improved;

(l) sources of information used in the preparation of the report, including all of the following but not limited to:

i. results from internal audit,

ii. results from compliance assessments,

iii. results from digital operational resilience testing, and advanced testing of ICT tools, systems and processes based on TLPT,

iv. external sources.

CHAPTER VI

PROPORTIONALITY PRINCIPLE

Article 29

Complexity and risk considerations

For the purposes of defining and implementing ICT risk management tools, methods, processes and policies referred to in Articles 1 to 28 elements of increased complexity or risk shall be taken into account, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management, and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and of the disruptions on the continuity and availability of the financial entity's activities.

TITLE II – SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK

CHAPTER I

SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK

Article 30

Governance and organisation

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall have in place an internal governance and control frameworks that ensure an effective and prudent management of ICT risk, to achieve a high level of digital operational resilience.

2. As part of their ICT risk management framework, the financial entities shall ensure that their management body:

(a) bears the overall responsibility for ensuring that the ICT Risk Management Framework enables the achievement of the financial entity's business strategy and risk appetite, and ensures that ICT risk is considered in this context;

(b) sets clear roles and responsibilities for all ICT-related tasks;

(c) sets out information security objectives and ICT requirements;

(d) approves, oversees, and periodically reviews the financial entity's:

i. information assets, list of main risks identified, business impact analysis and related policies;

ii. business continuity plans and response and recovery measures, referred to, in Article 16(1)(f) of Regulation (EU) 2022/2554 ;

(e) allocates and reviews at least yearly the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training , and ICT skills for all staff;

(f) defines and implements the policies and measures included in Article 31 to identify, assess and manage ICT risk the financial entity is exposed to;

(g) identify and implement procedures, ICT protocols and tools that are necessary to protect all information assets and ICT assets;

(h) keeps staff of the financial entity up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, commensurate to the ICT risk being managed;

(i) sets out reporting arrangements, including the frequency, form, and content of reporting to the management body on the information security and digital operational resilience.

3. Financial entities referred to in paragraph 1 may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requirements to intra-group or external undertakings. In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements.

4. Financial entities referred to in paragraph 1 shall ensure appropriate segregation and independence of control functions and internal audit functions.

5. Financial entities referred to in paragraph 1 shall ensure that the ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. Auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.

6. Based on the conclusions from the audit referred to in paragraph 5, financial entities referred to in paragraph 1 shall ensure the timely verification and remediation of critical ICT audit findings.

Article 31

Information security policy and measures

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and document an information security policy in the context of the ICT risk management framework. The information security policy shall define the high-level principles and rules to protect the confidentiality, integrity, availability and authenticity of data and the services financial entities provide.

2. Based on their information security policy, financial entities referred to in paragraph 1 shall establish and implement ICT security measures to mitigate their exposure to ICT risk, including mitigating measures implemented by third party providers.

3. These ICT security measures shall include:

(a) classification of information assets and ICT assets;

(b) ICT-related incident management;

(c) access control;

(d) physical and environmental security;

(e) ICT operations security;

(f) ICT security testing;

(g) ICT systems, acquisition, development, and maintenance;

(h) ICT project and change management

Article 32

Classification of information assets and ICT assets

1. As part of the ICT risk management framework referred to in Article 16(1)(a) of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify, classify, and document all critical or important functions, the information assets and ICT assets supporting them and their interdependencies. Financial entities shall review the identification and classification as needed.

2. Financial entities referred to in paragraph 1 shall identify all critical or important functions supported by ICT third-party service providers.

Article 33

ICT risk management

1. The ICT risk management framework of financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall include all of the following elements relating to the ICT management:

(a) determine the risk tolerance levels for ICT risk, in accordance with the risk appetite of the financial entity;

(b) identify and assess the internal and external ICT and information security risks to which the financial entity is exposed;

(c) define mitigation strategies at least for the ICT risk that are not within the risk tolerance levels of the financial entity;

(d) monitor the effectiveness of these measures;

(e) identify and assess whether there are any ICT and information security risks resulting from any major change in ICT system or ICT services, processes, or procedures, from ICT security testing results and after any major ICT-related incident.

2. The ICT risk assessment shall be carried out and documented periodically commensurate to the financial entities' overall risk profile.

3. Financial entities referred to in paragraph 1 shall ensure that they continuously monitor threats and vulnerabilities relevant to their critical or important functions, supporting information and ICT assets and shall regularly review the risk scenarios impacting them.

4. Financial entities referred to in paragraph 1 shall define alert thresholds and criteria to trigger and initiate ICT-related incident response processes as part of their ICT-related incident management process under Article 17(1) of Regulation (EU) 2022/2554.

Article 34

Physical and environmental security

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify and implement physical security measures, which shall be designed according to the threat landscape and to the classification and overall risk profile of ICT assets and information assets that can be accessed.

2. The measures referred to in paragraph 1 shall protect the premises and, where applicable, data centres of the financial entity where ICT assets and information assets reside, from unauthorised access, attacks, accidents and from environmental threats and hazards.

3. The protection from environmental threats and hazards shall be commensurate with the importance of the premises and, where applicable, the data centres, and the criticality of the operations or ICT systems located there.

CHAPTER II

FURTHER ELEMENTS OF SYSTEMS, PROTOCOLS, AND TOOLS TO MINIMISE THE IMPACT OF ICT RISK

Article 35

Access Control

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall define, document, and implement procedures for logical and physical access control and shall enforce, monitor, and periodically review these procedures. These procedures shall define the following logical and physical access control elements:

(a) access rights to information assets, ICT assets and their supported functions, critical locations of operation of the financial entity, shall be managed on a need-to-know, need-to-use and least privileges basis, including for remote and emergency access;

(b) user accountability, thereby ensuring that users can be identified for the actions performed in the ICT systems;

(c) account management procedures to grant, change or revoke access rights for use and generic accounts, including generic administrator accounts. Assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems and shall be logged in accordance with Article 36(f);

(d) the use of authentication methods commensurate to the classification and overall risk profile of ICT assets and considering leading practices. The use of strong authentication methods in accordance with leading practices for remote access to the financial entities' network, for privileged access, and for access to ICT assets supporting critical or important functions that are publicly available;

(e) access rights shall be periodically reviewed and shall be withdrawn when no longer required.

Article 36

ICT operations security

1. As part of their systems, protocols and tools, and for ICT assets supporting critical or important functions, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall:

(a) monitor and manage the life cycle of these ICT assets, to ensure that they continue to meet and support business and risk management requirements;

(b) monitor whether these ICT assets are supported by their external or internal vendors and developers, if applicable,

(c) identify capacity requirements of their ICT systems and measures to maintain and improve availability and efficiency of ICT systems and prevent ICT capacity shortages before they materialise;

(d) perform automated vulnerability scanning and assessments on ICT assets commensurate to their classification and overall risk profile of the ICT asset, and deploy patches to address identified vulnerabilities;

(e) manage the risks related to outdated or unsupported and legacy ICT assets;

(f) log events related to logical and physical access control, ICT operations, including system and network traffic activities, ICT change management. The level of detail of the logs shall be aligned with their purpose and usage of the ICT asset producing the logs;

(g) identify and implement measures to monitor and analyse logs to detect anomalies for critical or important ICT operations;

(h) implement measures to monitor relevant and up-to-date information about cyber threats;

(i) implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and shall check for corresponding new security updates.

Article 37

Data, System and Network Security

1. As part of their systems, protocols and tools, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and implement safeguards to ensuring the security of networks, against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data.

2. Financial entities referred to in paragraph 1 shall perform all of the following related to data, ICT system and network security, in accordance with the classification performed pursuant to Article 32:

(a) measures to protect data in use, in transit and at rest;

(b) identification of security measures regarding the use of software, data storage media, systems and endpoint devices transferring and storing data of the financial entity;

(c) identification and implementation of measures to prevent and detect unauthorised connections to the financial entity's network and to secure the network traffic between the financial entity’s internal networks and the internet and other external connections;

(d) identification of measures ensuring the availability, authenticity, integrity and, confidentiality of data during network transmission

(e) process to securely delete data on premises or stored externally that the financial entity no longer needs to collect or store;

(f) process to securely dispose or decommission of data storage devices on premises or stored externally containing confidential information;

(g) the implementation of measures to ensure that teleworking and the use of private endpoint devices, does not adversely impact the financial entity’s ability to carry out their critical activities in an adequate, timely and secure manner;

(h) where relevant, the implementation of strong technical and organisational security measures on the credentials used to access the cloud client interface to manage the cloud computing resource.

Article 38

ICT security testing

1. For the purposes of Article 16(3), first subparagraph, point (d) of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall establish and implement an ICT security testing plan to validate the effectiveness of their ICT security measures developed in accordance with Chapters II and III of this Title, and ensure that this plan considers threats and vulnerabilities, identified as part of the Article 33(3).

2. Financial entities referred to in paragraph 1 shall ensure that reviews, assessments, and tests of ICT security measures are conducted taking into consideration the overall risk profile of the financial entity.

3. Financial entities referred to in paragraph 1 shall monitor and evaluate the results of the security tests and update their security measures accordingly without undue delay in the case of critical ICT systems.

Article 39

ICT systems acquisition, development, and maintenance

1. Where applicable, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall implement a procedure governing the acquisition, development, and maintenance of ICT systems and shall design this procedure following a risk-based approach. The procedure governing the acquisition, development, and maintenance of ICT systems shall:

(a) ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements, including information security requirements, are clearly defined, and approved by the relevant business management;

(b) ensure the testing and approval of ICT systems prior to their first use and before introducing changes to the production environment;

(c) identify measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

Article 40

ICT project and change management

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document and implement an ICT project management procedure, and define the roles

and responsibilities for its implementation. The ICT project management procedure shall cover all stages of the ICT projects from its initiation to its closure.

2. Financial entities referred to in paragraph 1 shall develop, document and implement an ICT change management procedure to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner and with the adequate safeguards to preserve the financial entity's digital operational resilience.

CHAPTER III

ICT BUSINESS CONTINUITY MANAGEMENT

Article 41

Components of the ICT business continuity plan

1. As part of the overall business continuity policy, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall conduct a business impact analysis (BIA) of their exposures and potential impact to severe business disruptions. The BIA shall consider the criticality of identified business functions, supporting processes, information assets and ICT assets, third-party dependencies, and their interdependencies.
2. As part of the preparation of the ICT business continuity plan, financial entities referred to in paragraph 1 shall identify a range of scenarios to which its ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario, and the assessment of the potential impact that such scenarios might have.
3. Financial entities referred to in paragraph 1 shall develop the ICT business continuity plans considering the results of the BIA referred to in paragraph 1 and the scenarios referred to in paragraph 2.
4. The ICT business continuity plans shall:

   (a) be approved by the management body of the financial entity;

   (b) be documented and readily accessible in the event of an emergency or crisis,

   (c) allocate sufficient resources to execute the plan;

   (d) establish planned recovery levels and timeframes for recovery and resumption of functions and key internal and external dependencies including third party service providers;

   (a) specify what conditions may prompt activation of the plans and what actions shall be taken to ensure the availability, continuity, and recovery of the financial entities' ICT assets, supporting critical or important functions;

(e) identify restoration and recovery measures for critical or important business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial entities. These measures shall include mitigation of failures of critical third-party providers as well;

(f) identify backup policies and procedures specifying the scope of the data that is subject to the backup, and the minimum frequency of the backup, based on the criticality of the function using those data;

(g) consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances;

(h) specify the internal and external communication arrangements including escalation plans;

(i) identify insurance arrangements in place and insurance notification procedures to be followed in the event of loss from material interruptions;

(j) be updated in line with lessons learned from incidents, tests, new risks and threats identified, changed recovery objectives, major changes to the financial entity's organisation and to the ICT assets supporting critical or business functions.

Article 42

Testing of business continuity plans

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall test their business continuity plans referred to in Article 41, including the scenarios defined in paragraph 2, at least every year for the back-up and restore procedures or at every major change of the business continuity plan.
2. The testing of their business continuity plans shall demonstrate that the financial entities referred to in paragraph 1 are able to sustain the viability of their businesses until critical operations are re-established and identify any deficiencies in the business continuity plan.
3. Financial entities referred to in paragraph 1 shall document the test results of the testing of business continuity plans and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.

CHAPTER IV

REPORT ON THE REVIEW OF THE ICT RMF

Article 43

Format and content

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and document the report referred to in Article 16(2) of Regulation (EU) 2022/2554 in a searchable electronic format.

2. Financial entities referred to in paragraph 1 shall include the following information in the report:

(a) an introductory section which:

(i) describes the context of the report in terms of the nature, scale and complexity of the financial entity's services, activities and operations, its organisation, identified critical functions, strategy, major ongoing projects or activities, relationships and its dependence on in house and outsourced ICT services and systems (or the impact of the total loss or severe degradation of such systems on critical or important functions and market efficiency);

(ii) provides an executive level summary of the current and near-term ICT risk identified, threat landscape, the assessed effectiveness of its controls and hence security posture of the financial entity;

(iii) provides information about the reported area;

(iv) provides list of changes which were done in the reported area;

(v) summarises and specifies impact of major changes to the ICT risk management framework since the previous report;

(b) where applicable, date and evidence of the approval of the report by the management body of the financial entity in accordance with Article 16(2) of Regulation (EU) 2022/2554;

(c) description of the reason(s) for the review, including:

(i) in case the review has been initiated following supervisory instructions, evidence of such instructions;

(ii) in case the review has been initiated following the occurrence of ICT-related incidents, the list of all ICT-related incidents with related incident root-cause analysis;

(d) start and end date of the review period;

(e) the person responsible for the review;

(f) a summary of findings and a self-assessment of the severity of the weaknesses, deficiencies, and gaps identified in ICT risk management framework for the review period, including a detailed analysis;

(g) remedying measures identified to address weaknesses, deficiencies, and gaps in the ICT risk management framework and expected date for implementing these measures including follow-up of weaknesses, deficiencies, and gaps identified in previous reports, if they have not been remedied;

(h) overall conclusions on the review of the ICT risk management framework, including any further planned developments.

5. Annex I: Draft impact assessment

1. As per Article 15(1) of Regulation (EU) No 1093/2010 (EBA Regulation), of Regulation (EU) No 1094/2010 (EIOPA Regulation) and Regulation (EU) No 1095/2010 (ESMA regulation), any draft regulatory technical standards developed by the ESAs shall be accompanied by an Impact Assessment (IA) which analyses 'the potential related costs and benefits'.

2. This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on regulatory technical standards (RTS) to specify the detailed content of the policy in relation to the contractual arrangements on the further harmonisation of ICT risk management tools, methods, processes and policies and the simplified ICT risk management framework.

Problem identification

3. Complexity of information and communication technology (ICT) risk is increasing and frequency of ICT-related incidents, including cyber incidents, is rising together with their potential significant adverse impact on the financial institutions' operational functioning. Moreover, due to the interconnectedness between financial institutions, ICT related incidents risk causing potential systemic impact.

4. DORA introduces requirements for a minimum risk management framework for financial entities, in order to address the increasing complexity and evolving nature of cybersecurity threats they face, ensuring the protection of their critical systems, availability, authenticity, integrity and confidentiality of data, including their customers' data, and maintaining the stability and integrity of the financial sector.

5. DORA also introduces a simplified risk management framework recognising that smaller financial entities may have limited resources and capabilities to implement and maintain comprehensive risk management practices. By providing a simplified framework, DORA aims to facilitate the adoption of effective risk management measures and promote cybersecurity resilience among all financial entities, regardless of their size or complexity, ultimately contributing to a more secure and resilient financial ecosystem.

6. In this context, the ESAs have been mandated under Article 15 and 16(3) Regulation (EU) 2022/2554 to develop draft RTS to specify further details and components of ICT risk management framework referred to in Article 6(1) and of the simplified risk management framework referred to in Article 16 (1).

Policy objectives

7. The draft RTS specifying the further details and components of ICT risk management framework and of the simplified risk management framework aims to establish a common risk framework for all EU financial entities in a manner that is proportionate to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. The objective of these RTS is to enable financial entities to manage their ICT risk and information security risk.

Baseline scenario

8. With the entry into force of DORA, financial entities that are not subject to Article 16 of DORA must comply with Chapter II "ICT risk management", Section II of the same regulation. Financial entities subject to Article 16 of DORA must comply with this article.

9. The above legal requirements form the baseline scenario of the impact assessment, i.e. the impact caused by DORA is not assessed within this impact assessment, which focuses only on areas where further specifications have been provided in the regulatory technical standards.

10. The following overarching aspects have been considered when developing the proposed RTS.

POLICY ISSUE 1: TECHNOLOGY NEUTRALITY

Options considered

11. Option A: the RTS should adopt a technology-neutral approach to allow financial entities flexibility in selecting and implementing risk management measures, considering the evolving landscape of technologies.

12. Option B: The RTS should include specific provisions and references to certain technological standards addressing technology-related risks and controls, taking into account the unique challenges and vulnerabilities associated with different technologies used by financial entities.

13. Option C: The RTS should adopt a technology-neutral approach to allow financial entities flexibility in selecting and implementing risk management measures, considering the evolving landscape of technologies. At the same time, the RTS shall include some limited provisions related to the cloud computing paradigm, considering that (a) cloud computing is not a technology itself, (b) financial entities increasingly rely on cloud computing resources, and (c) there are some particularities in the model that need to be identified.

Cost-benefit analysis

14. By adopting a technology-neutral approach, the RTS can provide a framework that is adaptable to different technological advancements and avoids being outdated or restrictive.

15. By including technology-specific provisions, the RTS can provide clear guidance on recommended risk management practices tailored to the specific technologies employed, ensuring a higher level of security and resilience in the financial industry.

16. A balanced approach based on a technology-neutral stance while including limited provisions specific to cloud computing would allow the recognition of the increasing reliance on cloud computing resources acknowledging its unique characteristics. The RTS can provide targeted guidance on addressing the associated ICT risks. This approach enhances risk management practices, promotes regulatory compliance in cloud environments, and instils confidence in stakeholders.

Preferred option

Option C has been retained, and some questions have been included in the consultation paper in relation to the identification of specific provisions regarding cloud computing.

POLICY ISSUE 2: PRESCRIPTIVENESS OF THE RTS

Options considered

17. Option A: the RTS should take a rule-based approach i.e., mandate prescriptive requirements going into details on how to implement specific elements of the risk management framework or its simplified version.

18. Option B: the RTS should take a principle-based and objective-focused approach.

19. Option C: the RTS shall adopt a principle-based and objective-focused approach. At the same time, considering (a) the nature of the empowerment to cover in detail certain provisions, and (b) the need to be more specific in the requirements, to provide clarity to the industry and facilitate the implementation of the requirements, a combination of principle-based and rule-based approach have been followed, especially for the articles on network security, data and system security, encryption and cryptography, and access control.

Cost-benefit analysis

20. If the RTS is designed to be prescriptive, it will provide detailed and specific requirements, guidelines, and procedures for financial entities to follow in implementing their risk management framework. This approach aims to ensure consistency and uniformity in risk management practices across the industry, facilitating easier supervision and regulatory oversight by providing regulators with clear benchmarks against which to evaluate compliance.

21. On the other hand, if the RTS is principle-based, it will focus on providing high-level principles, and objectives for financial entities to develop and customize their risk management framework based on their specific circumstances. This approach allows for more flexibility and adaptability, enabling financial entities to tailor their risk management approach more specifically to their unique business models and risk profiles, while also promoting effective supervision as regulators can assess the soundness and effectiveness of the overall risk management framework rather than just compliance with specific requirements. The principle-based approach encourages financial entities to exercise judgment and take responsibility for their risk management decisions, while regulators can monitor the application of the principles and evaluate the effectiveness of the risk management framework in achieving its intended outcomes.

22. Combining the benefits of a principle-based approach with some rule-based provisions would strikes a balance between principle-based guidance and necessary rule-based provisions, leading to effective risk management practices across the financial sector. The principle-based approach allows for flexibility and adaptability, enabling financial entities to implement risk management measures tailored to their specific circumstances. This approach encourages innovation and enables financial entities to respond effectively to the evolving threat landscape. The inclusion of specific rule-based provisions for critical areas such as network security, data and system security, encryption and cryptography, and access control enhances clarity, facilitates implementation, and ensures a minimum level of security standards across the industry. While there may be initial costs associated with interpreting and implementing the combination approach, the benefits of flexibility, innovation, clarity, and standardized security measures justify the investment.

Preferred option

Option C has been retained.

POLICY ISSUE 3: DEFINITION OF LOGGING RETENTION PERIODS

Options considered

23. Option A: the RTS should define the logging retention periods for all logs it refers to.

24. Option B: the RTS should not define the logging retention periods and leave the decision about such periods to financial entities.

Cost-benefit analysis

25. On the one hand, if the RTS includes the definition of logging retention periods, it will establish clear and specific requirements for financial entities regarding the duration for which they must retain logs of their ICT activities. This approach provides clarity and consistency in record-keeping

practices, ensuring that relevant information is available for audit, investigation, and regulatory oversight purposes. On the other hand, a set duration in this RTS would introduce compliance concerns with existing regulations and standards at Union, national and international levels, that already have established logging or data retention periods (including personal data retention), and to which the financial entities may be subject to.

26. If the RTS does not define logging retention periods but the objective to be achieved, it allows financial entities to determine the most appropriate duration for retaining logs based on their individual risk profiles, business needs, and regulatory requirements. This approach acknowledges the diverse nature of financial entities and the varying factors that may influence their logging practices, including other Union or national regulations, promoting flexibility while still emphasizing the importance of maintaining sufficient logs to support risk management, incident response, and audit and compliance obligations.

Preferred option

Option B has been retained.

POLICY ISSUE 4: PROPORTIONALITY PRINCIPLE

Options considered

27. Option A: Introduce a principle-based proportionality article applicable to all financial entities under the scope of DORA but not subject to Article 16 of that regulation.

28. Options B: Identify specific requirements that could be applied in a differentiated manner to financial entities, based on their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations, e.g., frequency of the review or different details to be included in the ICT policies or procedures aspects.

Cost-benefit analysis

29. DORA already embeds proportionality in three ways: its Article 4 sets out general requirements on the proportionate application of its requirements, for both financial entities and for competent authorities, it exempts microenterprises from certain requirements, and it already foresees a simplified risk management framework for specific entities indicated in Article 16.

30. While somehow repeating level 1, including a general article on proportionality in the RTS would ensure that this principle is followed by both financial entities and supervisors reducing the overall costs for the implementation of the RTS and at the same time for the supervision of the said entities, while leaving them some flexibility in their assessment.

31. Identifying in the RTS specific ways to adapt the implementation of the RTS to certain categories of financial entities would give more guidance and possibly ensure a more harmonised application of DORA but would leave less flexibility to the financial entities and their supervisors.

Options considered

Both options have been considered by the ESAs to prepare their proposal. Option A has been retained for the part of the draft RTS based on Article 15 of DORA: Article 29 further specifies some of the criteria for the application of the proportionality principle that can be considered by financial entities and competent authorities when doing the proportionality assessment. Option B has been retained to approach the drafting of the whole part of the draft RTS based on Article 16(3) of DORA (Title II of the proposed draft RTS, on the simplified ICT risk management framework).

6. Annex II: Overview of the questions for consultation

Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (*Complexity and risks considerations*)? If not, please provide detailed justifications and alternative wording as needed.

Q2. Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.

Q3. Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.

Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.

Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.

Q6. Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?

Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.

Q8. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q9. Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.

Q10. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q11. What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.

Q12. Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.

Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.

Q14. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.

Q16. Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.

Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.

Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.

Q19. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q20. Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.

Q21. Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.

Q22. Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

Q23. Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.

Q24. Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.

Q25. Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.

Q26. Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.

Q27. Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.

Q28. Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

Q29. What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.

Q30. Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.

Q31. Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.

Q32. Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.