JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 86

10 01 2024

Final report

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. 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. Section 2 of this report presents in detail the mandate and background to the final daft RTS which is included in Section 3.

2. This report follows a consultation paper which presented a first draft of the RTS and 32 questions and was open to comments from the public from 19 June to 11 September 2023.

3. A total of 120 responses were received to the public consultation, covering all sectors. They included 17 responses from EIOPA stakeholders, 33 from EBA stakeholders, 23 from ESMA stakeholders, 33 shared stakeholders and 31 other stakeholders. The ESAs have also received input from the ESAs' Stakeholders Groups.

4. The ESAs assessed the concerns raised to decide which changes, if any, should be made to the draft RTS. In the light of the comments received, the ESAs agreed with some of the proposals and their underlying arguments and have introduced changes to the draft RTS. A summary of the comments received, and the ESAs' analysis are included hereafter in Section 2.

5. The main changes related to the introduction of further proportionality and where possible of a risk-based approach, the removal of the article on governance and information security awareness from the general regime requirements, the clarification of provisions, especially those included in the articles related to network security, encryption, access control and business continuity aspects. The inclusion of cloud computing specific aspects was controversial, and it was chosen not to introduce any technology specific requirement based on the principle of technological neutrality, and to identify requirements related to ICT assets or services provided by ICT third party service providers in general. The ESAs may consider developing further guidelines in the areas that have been removed from the RTS, being those very important, and also on cloud computing security aspects. More information on the feedback received and how this was taken on board by the ESAs is provided within section 2, and in the feedback table.

6. This feedback allowed the ESAs to prepare the final draft RTS included hereto as Section 3.

Next steps

7. The ESAs will submit the final draft RTS to the European Commission for adoption. Following its adoption in the form of a Commission Delegated Regulation, it will then be subject to scrutiny of the European Parliament and the Council before publication in the Official Journal of the European Union.

8. The expected date of application of these technical standards is 17 January 2025.

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)
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)
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)
Regulation (EU) No 1025/2012	Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316 14.11.2012, p. 12)
Regulation (EU) No 153/2013	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)
Regulation (EU) No 600/2014	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84)
Regulation (EU) 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1)
Regulation (EU) 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 (OJ L 65, 10.3.2017, p. 48)
Regulation (EU) 2017/565	Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (OJ L 87, 31.3.2017, p. 1)

Regulation (EU) 2017/571	Commission Delegated Regulation (EU) 2017/571 of 2 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers (OJ L 87, 31.3.2017, p. 126)
Regulation (EU) 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 (OJ L 87 du 31.3.2017, p. 350)
Regulation (EU) 2019/881	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
Directive (EU) 2019/1937	Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17)
MiFID II	Directive 2014/65 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349)
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)

Abbreviations, acronyms

APA	Approved Publication Arrangements
ARM	Approved Reporting Mechanisms
BCBS	Basel Committee on Banking Supervision
BIA	Business Impact Analysis
BIS	Bank for International Settlements
CCP	Central counterparty, as defined under EMIR
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payments and Settlement Systems
CSD	Central securities depositories, as defined under CSDR
DRSP	Data reporting service providers, as defined in MiFID II
ENISA	European Union Agency on Cybersecurity
ESCB	European System of Central Banks
FSB	Financial Stability Board
ICT	Information and Communication Technologies
IOSCO	International Organization of Securities Commissions
ISO	International Organisation for Standardisation
NCA	National Competent Authority
NIST	National Institute of Standards and Technology
PFMIs	Principles for Financial Market Infrastructures, published by the Committee on Payment and Settlement Systems of the BIS and the Technical Committee of the IOSCO in 2012
RTS	Regulatory Technical Standards
SG	ESA Stakeholder Group
TPP	Third-party service provider

2. Background and rationale

2.1 Background and rationale

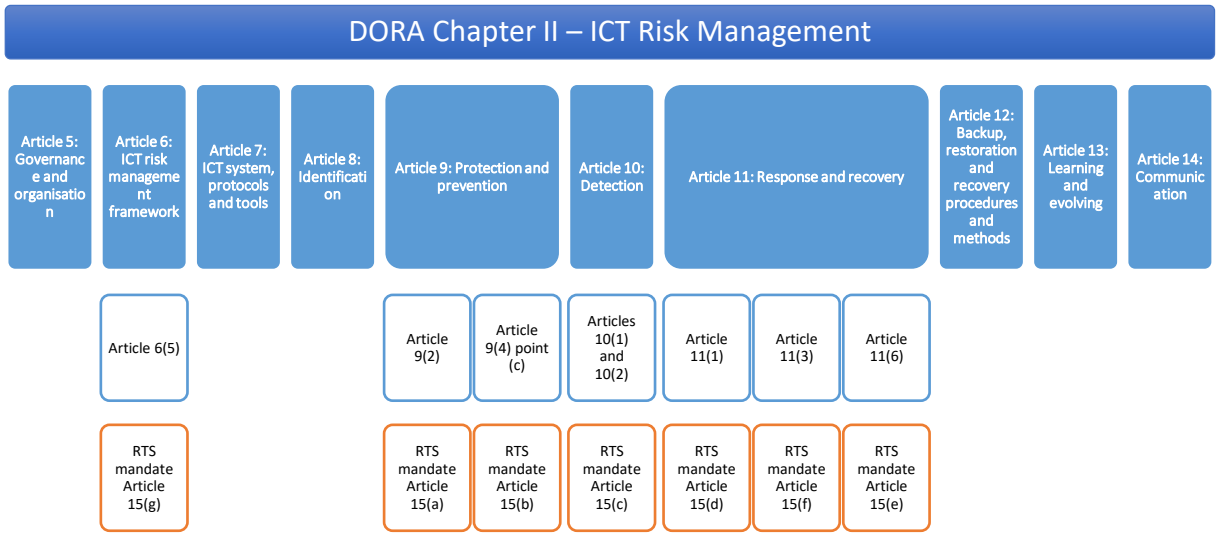
1. DORA sets out uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector (the 'financial entities'). It thus creates a regulatory framework on digital operational resilience, whereby all financial entities need to make 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 required to deliver draft RTSs on selected topics of the ICT risk management under distinct mandates included in Articles 15 and 16 of DORA.

3. In delivering the mandates, the ESAs have duly considered existing European and international standards on ICT risk management, such as 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, and the BCBS principles for operational resilience and sound management of operational risk, effective risk data aggregation and risk reporting. Further to that, the proposed regulation uses common industry terms as defined in ISO standards in order to ease financial entities' understanding and implementation of its requirements. Examples of common industry terms derived from industry standards include 'information processing facilities', derived from the standard ISO 27000 or 'clear screen policy' and 'protection of unattended ICT assets', derived from standards ISO 27002.

4. The draft RTS 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 development of specific regulatory requirements on the following selected aspects: 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 subject to Article 15 of DORA, the assessment of their compliance with the Chapter II of DORA (ICT risk management) will consider requirements set out in Articles 5 to 14 of DORA, alongside with those of the RTS mandated under Article 15 of DORA.



6. A similar consideration is valid for the mandate contained in Article 16(3) of DORA, according to which the ESAs are required to specify certain elements of the simplified ICT risk management framework (while other elements, required in Article 16, are not included in the mandate of the draft RTS).

7. 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.

8. The draft RTS deal with specific requirements that are intended to be part of the broader framework on ICT risk management and digital operational resilience designed in DORA. The ESAs attach a lot of importance to ensuring strong ICT risk management and control frameworks in financial entities and aim at ensuring 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 needs to be provided to the market with respect to the interaction between the requirements included in the draft RTS and the other directly applicable requirements relating to the ICT risk management framework that are contained in DORA (and whether there is a need for further clarification outside of the draft RTS). Finally, the ESAs wish to clarify that, in order to ensure the necessary adherence to the fundamental objectives enshrined within the draft RTS while reducing administrative burden and complexity, the financial entities covered by DORA can adjust their existing policies without having to create brand new ones, if not needed.

2.2 Architecture of the proposed draft RTS

One joint draft RTS on ICT risk management, two main parts

9. The mandates granted to the ESAs pursuant to 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 become applicable at the same time, it is proposed to include all the draft regulatory technical standards required by Article 15, fourth subparagraph, and Article 16(3), fourth subparagraph of DORA, into a single draft RTS.

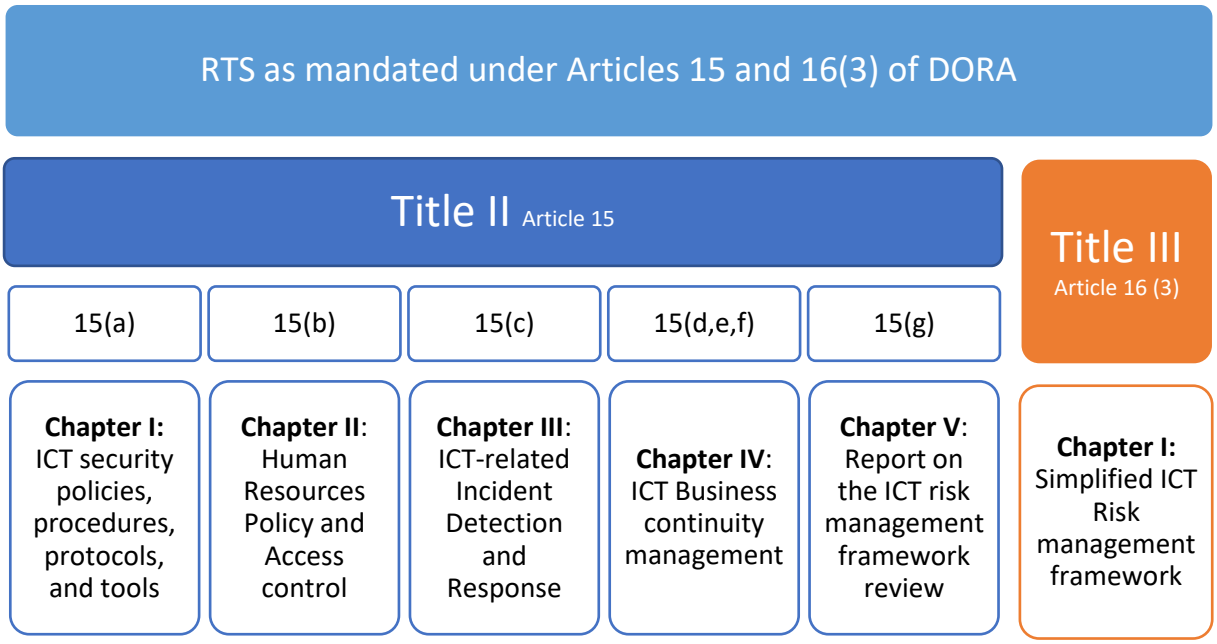
11. In the draft RTS two titles (Title II and Title III) respectively address each of the mandates. Title II is appliable to the financial entities, as defined in Article 2(2) of DORA, with the exception of the entities referred to in Article 16(1), to which the Title III applies[1].

Structure of the draft RTS

12. The structure of the draft RTS largely follows the mandates in 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).

13. The following graph presents a high-level mapping of the structure of the draft RTSs against the structure of the empowerments listed under Articles 15 and 16(3) of DORA.

[1] Namely, small and non-interconnected investment 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.



2.3 General drafting principles

Technology-neutral

14. The ESAs consider that the draft 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. This approach has been confirmed by respondents to the consultation.

Cross-sectoral and sector-agnostic

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

16. Nonetheless, where needed, entity-specific requirements have been included. Indeed, 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*'.

17. This is the basis for the introduction of certain requirements specific to CCPs, CSDs and trading venues in the draft RTS. More details on these requirements are provided below in the relevant chapters or sections incorporating them, namely: ICT project and change management (testing of ICT systems before use and after significant changes) and ICT business continuity management (components of the ICT business continuity policy and testing of the ICT business continuity policy).

18. This is particularly important for CCPs and CSDs, in respect of which such requirements were introduced in EMIR and CSDR to comply with the applicable international standards of the Principles for Financial Market Infrastructures issued in April 2012 by the Committee on Payments and Settlement Systems (CPSS) of the Bank of International Settlements (BIS) and the International Organisation of Securities Commissions (IOSCO).

2.4 Title I: General principles

19. Although DORA itself already embeds a general proportionality principle in its Article 4, and specific proportionality considerations through the exemptions granted to microenterprises and the simplified regime defined in Article 16 for certain types of entities, the mandates in Articles 15, second paragraph, and 16(3), second paragraph of DORA, required the ESAs 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 RTS.

20. The draft RTS submitted to public consultation included one article requiring taking into account elements on increased complexity and risk when implementing ICT risk management elements defined under the mandate established in Article 15 of DORA (i.e., for the general regime only). This approach on proportionality attracted many comments from the respondents to the consultation. Although most respondents approved of this article, suggestions were made to: make this assessment go both ways (taking into account not only elements of increased complexity but also elements of reduced complexity and risk, so that requirements could be either strengthen or lessen); take into account more elements and in particular the risk profile of the entities; have a more sectoral approach, taking into account the particularities of certain entities including to explicitly waive certain requirements; include more proportionality at the level of each requirement or to the contrary make the requirements in the draft RTS less detailed, to make them less prescriptive and more flexible.

21. Following from this, the ESAs have reviewed their approach to embed more proportionality in the text. The final draft RTS now includes as first article in its first title a general provision applying to Title II and Title III, i.e., in the context of both the general and the simplified regimes, and requiring that, when defining and implementing their ICT risk management frameworks, financial entities shall take into account elements of increased or reduced complexity and their overall risk profile.

22. This should allow financial entities to tailor to a certain extent the requirements established in this draft RTS to their specific situation, subject to being able to evidence the assessment performed to that purpose.

2.5 Title II: 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.

23. This mandate is covered under the second title of the 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 draft RTS is not to design a complete ICT risk management framework; **rather, it is focused on introducing only certain specific elements**, namely those required by the mandate.

24. 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.

25. Title II is divided into five chapters: ICT security policies, procedures, protocols and tools, 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.

26. The table below provides an overview of the policies and procedures mandated under Title II. There are in total 20 policies and procedures: in 8 areas only policies are required, in 3 areas specific elements for policies and specific elements for procedures are required, in 5 areas specific elements for procedures and finally in 4 areas policies and procedures are required, without specifying which elements should go in policies and which procedures.

ONLY POLICIES	ONLY PROCEDURES	POLICIES AND PROCEDURES
• ICT asset management • Encryption & cryptographic controls • ICT project management • Acquisition, development and maintenance of ICT systems • Physical and environmental security • Human resources • Identity management • Access control • ICT-related incident management • ICT business continuity	• ICT asset management • Capacity and performance management • Vulnerability and patch management • Data and system security • Logging • Acquisition, development, and maintenance of ICT systems • ICT change management • Identity management	• ICT risk management • ICT operations • Network security management • Security information in transit

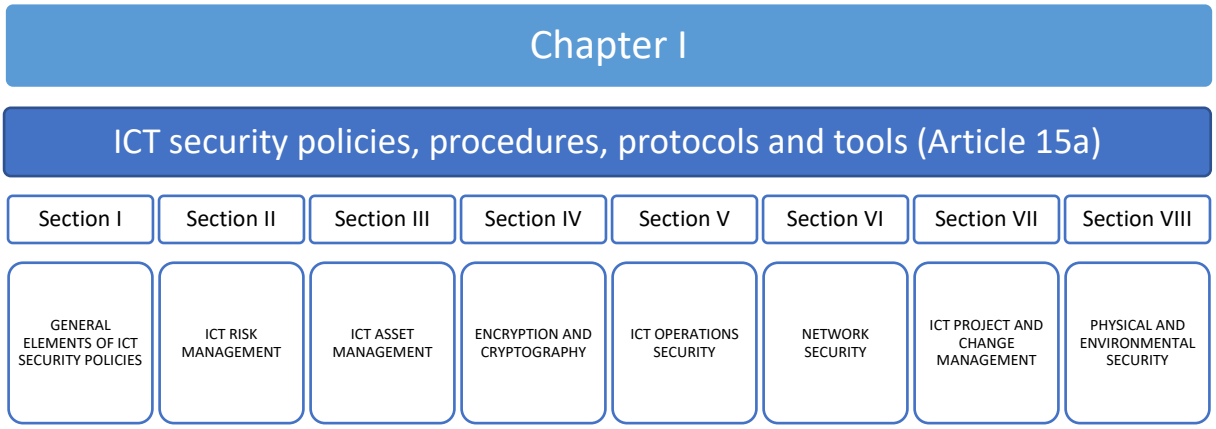
27. This approach was deemed appropriate to balance the need to provide maximum clarity to the industry on the requirements, while providing sufficient leeway to the financial entities to identify their own as it fits their environment. In this context, the draft RTS acknowledges that some elements are more principles and fit for policies and other are more elements of practical / technical implementation and thus more fit for procedures. In doing so, the draft RTS also provides the required leeway for financial entities to choose those elements for the areas in which both policies and procedures are needed.

28. At the same time, it is important to highlight that the inclusion of elements in specific policies and/or procedures does not imply that the financial entities should develop and implement only these policies and / or procedures and only in these areas. Financial entities should consider articles 6 to 14 of DORA together with this draft RTS and in that context consider the integration of these policies and procedures in their ICT risk management framework.

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

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

30. 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*".



31. The ESAs identified 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.

32. 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 further elements, the different articles included in this chapter complement the requirements already included in DORA.

33. 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.

Section I: General elements of ICT security

34. This section contains only one article which 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.

35. This article elaborates on the main ICT security policies, procedures, protocols and tools 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, first subparagraph, point (a) of DORA.

36. The ESAs consider that governance is a fundamental aspect of any ICT risk management framework, and that this is an element where introducing certain provisions could provide greater clarity in the process of implementing the requirements, and for these reasons the inclusion of governance requirements in draft RTS included in the CP (in particular the minimum list of tasks and responsibilities to be assigned to the control function referred to in Article 6(4) of DORA) was considered.

37. However, in view of the feedback received from the consultation and in line with the scope of the mandate set out in DORA, the proposed provisions on governance have been deleted entirely. The ESAs will assess the need to provide additional guidance on this issue in the future.

Section II: ICT risk management

38. 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 policies and procedures. An ICT risk management framework is essential for ensuring the preservation of data and systems availability, authenticity, integrity, and confidentiality and should be based on a robust ICT risk management policy. The ESAs consider the financial entities' ICT risk management policy should include the elements specified in Article 3 of the proposed draft RTS.

39. Financial entities are required to establish an ICT risk management policy that includes the necessary measures and procedures for effectively managing ICT risk. To that end, this policy should clearly define the approved risk tolerance levels for each type of risk identified and enable them to proactively address and mitigate ICT risk, safeguard data, and maintain the overall security and resilience of their operations.

40. In particular, financial entities should establish a process and a methodology to conduct their 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.

41. 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.

42. Also, financial entities should have a structured approach to identify, accept, document and review residual risks. These residual risks should be integrated within the general 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 should contribute to the overall effectiveness of their ICT risk management efforts and strengthens their resilience against potential threats.

43. 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.

44. 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.

    Another crucial aspect of the ICT risk monitoring is its alignment with changes in the business strategy and digital operational resilience strategy to ensure that it remains relevant for the evolving objectives and priorities of the organization.

Section III: ICT asset management

45. 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 should identify, classify and adequately document, among others, their information assets and ICT assets.

46. Section III elaborates on the requirements of identification and classification of ICT assets through two articles. Article 4 (*ICT asset management policy*) requires financial entities to establish a policy

for the management of ICT assets, complementing the elements included in Article 8(6) of DORA with respect to the inventory of the ICT assets and information assets. The feedback from the public consultation showed that stakeholders considered important to keep record of the end date of the provider's support or the date of the extended support of ICT assets.

The ESAs agreed with the feedback received and included new point (ix) under Article 4(2)(b) of the final draft RTS. However, as explained in the proposed Recital (7), financial entities should focus specifically on those ICT assets or systems necessary for the business operation, considering their criticality and potential impact in case of the loss of their confidentiality, integrity and availability.

47. Article 5 of the draft RTS (*ICT asset management procedure*) 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.

Section IV: Encryption and cryptography

48. 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.

49. Under the first article of this section, Article 6 (*Encryption and cryptographic controls*), 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.

50. Proposed Article 6 uses the term "leading practices or standards" as defined in Regulation (EU) 1025/2012[2], 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

[2] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, OJ L 316, 14.11.2012, p. 12–33

importance of innovation and continuous improvement to keep abreast of new developments to maintain their effectiveness.

51. 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 standards, financial entities should implement and keep records of mitigation and monitoring measures to maintain resilience against cyber threats.

52. 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.

53. Article 7 (*Cryptographic key management*) of the draft RTS 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.

Section V: ICT operations security

54. 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.

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

56. ***Policies and procedures for ICT operations***. Financial entities' policies and procedures for ICT operations should 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 policies and 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.

57. Following the feedback received the ESAs acknowledged that there's been a noticeable shift in terminology and principles regarding the management of software development environments.

Earlier approaches highlighted strict compartmentalization of development, testing, and operational environments. Contemporary guidelines or international standards lean towards a more integrated approach, promoting the separation of these environments while acknowledging scenarios where overlaps and controlled testing in live environments might be necessary. This evolution reflects a balanced emphasis on both security and operational flexibility, acknowledging that real-world applications may require adaptable solutions while maintaining rigorous security protocols.

58. To this end, Article 8 of the draft RTS (*Policies and procedures for ICT operations*) has been amended substituting the word "segregation" with the word "separation" and adding additional requirements for cases where testing is conducted in production environments. Such controls are deemed important also in the area of vulnerability and patch management for testing and deploying software and hardware patches and updates, of ICT systems and acquisition, development and maintenance for testing and approval of all ICT systems prior to their use and after maintenance, security testing for internet-exposed systems and applications or for software packages.

59. ***Capacity and performance management***. Financial entities need to identify the capacity requirements of their ICT systems and implement resource optimization and monitoring procedures. Article 9 of the draft RTS aims at maintaining and enhancing 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.

60. ***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. Considering that the main purpose of these scans is to cover the widest range possible of assets in an automated way, these requirement concerns all ICT assets based on their classification and overall risk profile, and at least on a weekly basis for those ICT assets supporting critical or important functions. Also, ICT third-party service providers should handle any vulnerabilities and report them to the financial entities.

61. The tracking of ICT third-party libraries (including tracking patches and updates), disclosure of vulnerability-related information, and deployment of patches are also vital. Some respondents to the public consultation noted that the obligation to monitor the usage, versions, and updates of third-party libraries, including open source, is quite burdensome for financial entities. Considering the feedback received, Article 10(2)(d) of the draft RTS has been amended to make the requirement more flexible.

62. Financial entities need to prioritize patch deployment based on vulnerability criticality and risk profiles, while monitoring and verifying remediation.

63. 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.

64. ***Data and system security***. 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 the various security measures outlined in Article 15 of DORA.

65. In the version submitted to public consultation, the draft RTS included requirements explicitly referring to 'cloud computing resources', however, further to the responses received, the ESAs considered that the draft RTS should remain technology-neutral and should not identify specific products or technologies. Such approach should ensure that the text remains future-proof to the extent possible. At the same time, the ESAs acknowledge the relevance and the specificity of cloud-based resources in the current landscape of technological solutions and the increasing dependence of the financial entities on them.

66. In this context, and based on the received feedback, the ESAs changed the requirements previously associated with cloud computing resources, to ICT assets or services provided by ICT third party service providers.

67. ***Logging***. 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.

68. 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.

Section VI: Network security

69. 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.

70. 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.

71. 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 services provided either by an ICT intra-group service provider or by ICT third-party service providers.

72. 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. Further, the protection of information in transit should take into account the results of the approved data classification and the ICT risk assessment processes.

Section VII: ICT project and change management

73. 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 is commonly seen as a source of ICT related incidents.

74. 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 it reduces or minimises the negative impacts that can result from such actions.

75. Section VII elaborates on these aspects through three articles. Article 15 (*ICT project management*) 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 their Section 3.6.1, notably with regard to the elements to be included in the policy.

76. Article 16 (*ICT systems acquisition, development, and maintenance*) establishes the need to design a policy on the acquisition, development and maintenance of ICT systems by financial entities, focused fundamentally on the testing of these systems and on the security implications that can be derived from these processes.

77. Finally, Article 17 (*ICT change management*) 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.

78. These two latter articles both include specific provisions for CCPs and CSDs, considering the specific ICT risks relating to these types of entities and replicating the existing EMIR and CSDR delegated regulations' provisions which require them to test their ICT systems (i) prior to their use and (ii) after significant changes[3], and include the minimal list of external stakeholders that CCPs and CSDs should involve in such tests, if they consider such involvement appropriate.

Section VIII: Physical and environmental security

79. 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.

80. Article 18 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.

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

81. 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. In order to identify security measures to protect premises, data centers 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 hazard, financial entities should consider geographical and weather-related threats such as earthquakes, floods, hurricanes, wildfires, as well as civil unrest and other forms of natural or man-made disaster. With respect to bespoke hazards and measures, financial entities may use international standards, such as ISO 27002 as further guidance.

82. It also establishes the need for a clear desk policy for papers and a clear screen policy for information processing facilities.

83. The version of the draft RTS which was submitted to public consultation included an article on ICT and information security awareness. A group of stakeholders noted that this article might not be in scope of the mandate of the draft RTS and the ESAs agree with this feedback. The article has therefore been deleted. However, the ESAs will consider developing further guidance on this area, as it is considered vital to ensure an effective digital operational resilience.

Chapter II: Human resources policy and access control

84. 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.

85. 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*".

86. This chapter is split into three articles: Human resources policy, Identity management and Access control.

87. Article 19 (*Human resources policy*) focusses 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.

88. Article 20 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.

89. 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.

90. The proposed Article 21 (*Access control*) sets out the main elements to be included by financial entities in their access control policy, which should address the following topics: governance, authentication methods, strategy, access rights and physical access.

Chapter III: ICT-related incident detection and response

91. 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.

92. The mandate set out in Article 15(c) of DORA is intended to complement the requirements already included in the same Regulation, 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.

93. The latter part of the mandate is covered in Article 22 of the 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 fulfilling this objective are added, such as the retention of evidence related to ICT-related incidents and the review of the policy.

94. The former part of the mandate is covered under Article 23 of the draft 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.

Chapter IV: ICT business continuity management

95. 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.

96. 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.

97. 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.

98. Article 24 of the 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).

99. In addition, this article also includes specific provisions for CCPs, CSDs and trading venues, replicating already applicable requirements from EMIR, CSDR and MIFID 2 Level 2 regulations[4], 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. This is particularly important for CCPs and CSDs, to comply with the existing international standard in this area, which is set by the PFMIs.

100. 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.

[4] Cf. Article 17(3) of Regulation (EU) 2013/153, Article 78(2) of Regulation (EU) 2017/392 and Article 15(2) of Regulation (EU) 2017/584.

101. Article 25 (*Testing of the ICT business continuity plans*) 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 their section 3.7.4) have been largely used.

102. Here also specific provisions have been included to replicate the requirements existing for CCPs and CSDs under EMIR and CSDR Delegated Regulations[5] to make sure certain selected external stakeholders are involved in this testing, if appropriate.

103. As a fundamental part of the ICT response and recovery mechanisms, financial entities should implement ICT response and recovery plans in line with the provisions of Article 11 (3) of DORA. The last article of this chapter (Article 26 on *ICT response and recovery plans*) 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.

Chapter V: Report on the ICT risk management framework review

104. 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 improvement of the ICT risk management framework. As part of the review process, a report on the outcome of the review should also be generated, which should be sent by the financial entity to its competent authority upon request.

105. This report should assist the financial entity 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.

106. Article 15(g) of DORA established a mandate for the ESAs to define the format and content of that report. Both elements, the format and the content, are covered in a unique article. Article 27 of the draft RTS (*Format and content*).

[5] Cf. Article 20(2)(b) of Regulation (EU) 2013/153 and Article 79(c) of Regulation (EU) 2017/392.

107. 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.

108. Paragraph 2 of the article elaborates on the content that is expected from such report and cover the minimum elements that should 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. For sake of proportionality, the ESAs have limited the requirement of Article 43(2)(a)(iv), to major changes.

2.6 Title III: 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.

109. The financial entities benefitting from this simplified ICT risk management regime are listed in Article 16(1) of DORA: 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. It is important to note that this list is exhaustive and that the ESAs cannot extend it through the draft RTS.

110. Recital 42 of DORA explains that the reasons why these categories of entities benefit from lighter ICT risk management requirements are that in principle, these entities usually are small or very small firms, and when they have, sometimes counting only a handful of employees.

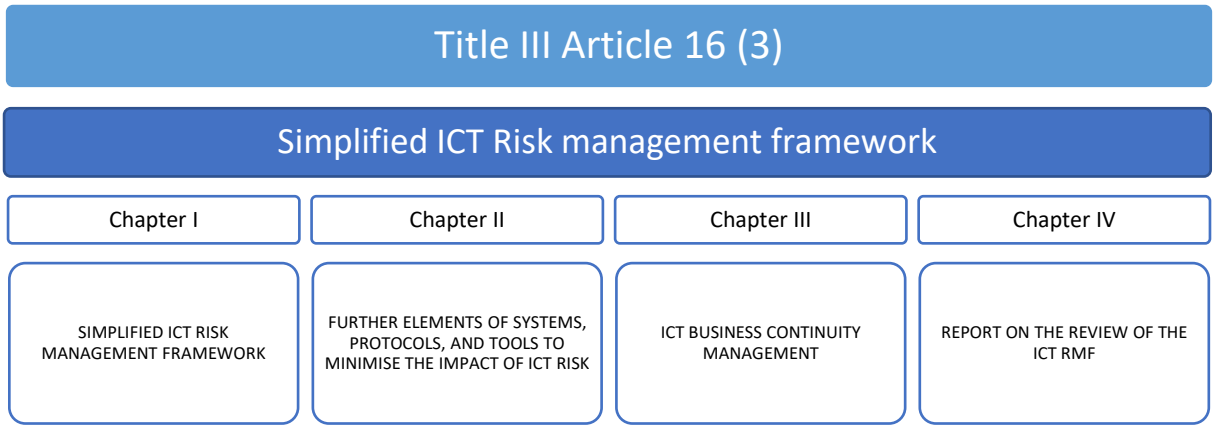
111. To specify the requirements that should apply to these financial entities, the ESAs have considered two sets of provisions in DORA:

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.

112. This mandate is covered under Title III of the proposed draft RTS and 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.

113. This title is divided into four 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.



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

115. In general, the approach followed by the ESAs in identifying the requirements for the financial entities that are subject to the simplified ICT risk management framework, was to focus on those essential areas and elements that are at a minimum necessary to ensure the confidentiality, integrity, availability and authenticity of their data and services, while considering their scale, risk, size and complexity. In this context, these financial entities should have in place an internal governance and control framework with clear responsibilities to enable an effective and sound risk management framework.

116. Also, to reduce the administrative and operational burden, the draft RTS mandates the development and documentation by these financial entities of only one policy, an information security policy, that defines the high-level principles and rules to protect the confidentiality, integrity, availability and authenticity of data and of the services financial entities provide.

117. Finally, considering the information security objectives identified in this policy, this draft RTS has identified only those key areas and technical implementation aspects, for which it is considered imperative for the financial entities to develop, document and implement ICT security controls, measures and procedures to ensure their digital operational resilience.

Chapter I – Simplified ICT risk management framework

118. The purpose of this chapter is to cover the elements to be included in the simplified ICT risk management framework. 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. 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.

119. To achieve this, the ESAs believe the framework should encompass various key elements. It is important to note here an important difference in the scope of the mandates granted to the ESAs under Article 15 and Article 16 of DORA: while the ESAs' mandate for the general ICT risk management framework under Article 15 is limited to the identification of further elements within specific aspects of this general framework, the ESAs' mandate under Article 16 for the simplified ICT risk management framework is broader, asking to define numerous elements of the ICT risk management framework itself. This means for instance that, differently from the general framework, governance and organisation aspects were an integral part of the ESAs' mandate for the simplified framework, and essential to define.

120. Firstly, governance and organisation 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.

121. Note that the reference in the proposed provisions to 'management body' also works in the context of smaller financial entities 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*".

122. 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.

123. 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.

124. 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.

125. ICT-related incident management is an essential part of the measures aimed at a quick, efficient and comprehensive management of ICT risks and in light of this the requirement to define

alert thresholds and criteria to trigger and initiate ICT-related incident response processes was inserted.

126. 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.

127. 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.

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

128. To mitigate the impact of ICT risk, financial entities benefitting from the simplified regime 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.

129. Access control is vital for financial entities to prevent unauthorized access to their ICT systems and sensitive information. Financial entities subject to the simplified regime 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.

130. ICT operations security ensures the secure functioning of ICT systems throughout their lifecycle. Financial entities submitted to the simplified regime should monitor and manage ICT assets supporting critical functions, assess capacity requirements, perform vulnerability scanning, manage outdated assets, log events, monitor and analyse information on anomalous activities and behaviour, 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. The ESAs concluded that these requirements should apply to all ICT assets, and not only to those supporting critical or important functions. However, as explained in Recital (7) of the draft RTS, financial entities should focus specifically on those ICT assets or systems necessary for the business operation and which bring value to the financial entity, considering their criticality and potential impact in case of the loss of their confidentiality, integrity, and availability.

131. Ensuring the security of data, systems, and networks is crucial for safeguarding the integrity, confidentiality, and availability of financial information. Financial entities subject to the simplified regime 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. Compliance with data protection regulations and the implementation of strong security measures are essential in maintaining a secure environment.

132. In addition to those requirements, the ESAs considered 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. However, for sake of proportionality and minimising the burden on financial entities in the scope of the simplified regime, the ESAs refrained from adding additional requirements.

133. Financial entities benefitting from the simplified regime 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.

134. Financial entities subject to the simplified regime 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.

135. 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.

136. 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 their services, activities and operations compared to the analogous elements included in Title II. In particular, 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 II 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, have not been included here.

137. Regarding cloud computing resources, in line with the abovementioned drafting principle of technological neutrality, no cloud-specific provision has been included in this draft RTS, to ensure to the extent possible that the legal text remains future-proof.

Chapter III – ICT business continuity management

138. Financial entities referred to in Article 16 of DORA should also ensure the continuity of their critical functions, especially in case of severe disruptions, in this context consider the scenarios to which their ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario. 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.

139. The identified components should include an analysis of their exposures to and potential impact of severe business disruptions. This requirement has been streamlined in order to reduce the burden for entities falling under the simplified approach.

140. 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.

141. Financial entities should also test their business continuity plans regularly to ensure their effectiveness. Testing covers backup and restoration procedures and occurs at least once a year or following 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.

142. Compared to the business continuity requirements in the general regime, the requirements here are less granular (e.g., no specific requirement as to scenarios, or in respect of response and recovery plans).

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

143. As under the general regime, financial entities covered by the simplified regime should submit a report on the review of their ICR risk management framework to their 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.

3. 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[6], and in particular Article 15, fourth subparagraph and 16(3), fourth subparagraph thereof,

Whereas:

(1) Considering the wide variety of financial entities under the scope of Regulation (EU) 2022/2554 in their size, structure, internal organisation and in the nature and complexity of their activities, financial entities should apply the requirements defined in this Regulation in a proportionate manner taking into account the increased or reduced elements of complexity or the overall risks profile.

(2) In order to take into account the diverse operational structures and existing risk management frameworks of financial entities subject to this Regulation, it is appropriate that financial entities may benefit of a certain degree of flexibility as regards the way they should put in place the policies and procedures required by this Regulation. To this end,

[6] OJ L 333, 27.12.2022, p. 1

financial entities should have the possibility to use and align their existing documentation to those required by this Regulation. Thus, this Regulation requires the inclusion of elements in specific policies only for certain essential elements, having also regard to leading industry practices and standards. Furthermore, in particularly technical areas such as capacity and performance management, vulnerability and patch management, data and system security and logging, it is appropriate that financial entities develop, document and implement procedures in order to cover specific technical implementation aspects.

(3) The elements of information and communication technology (ICT) security policies, procedures, protocols and tools specified in this Regulation will form a fundamental part of the ICT risk management framework, it is hence essential, to ensure a high level of digital operational resilience, that financial entities subject to Title II of this Regulation align them with the digital operational resilience strategy referred to in Article 6(8) of Regulation (EU) 2022/2554.

(4) In order to ensure the correct application over time of ICT security policies referred to in Title II, Chapter I of this Regulation, financial entities should ensure that roles and responsibilities relating to ICT security are correctly allocated and maintained. In order to limit the risk of conflicts of interest, financial entities should focus on the segregation of duties when allocating the ICT roles and responsibilities.

(5) Financial entities should, as part of the correct implementation of ICT security policies and procedures and to ensure awareness and transparency within their organisation, clearly set out the consequences of non-compliance with ICT security policies or procedures referred to in Title II, Chapter I of this Regulation. In order to ensure flexibility and simplify the financial entities' control framework, where the consequences of non-compliance are set out in another policy or procedure of the financial entity that is applicable to the area of ICT security, financial entities should not be required to develop further specific provisions on the matter.

(6) In a dynamic environment where ICT risks constantly evolve, it is important that financial entities develop the set of ICT security policies on the basis of leading practices in the different elements covered, and where applicable, of standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[7]. This should enable financial entities referred to in Title II of this Regulation to remain informed and prepared in a changing landscape.

(7) As part of the ICT security policies, procedures, protocols and tools and to ensure the digital operational resilience of financial entities referred to in Title II of this Regulation, the latter should develop and implement an ICT asset management policy, capacity and performance management procedures and as well as policies and procedures for ICT

[7] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316 14.11.2012, p. 12).

operations. These policies and procedures are necessary to ensure the monitoring of the status of the ICT assets throughout their lifecycles, so that they are used and maintained effectively (ICT asset management), to ensure the optimisation of ICT systems' operation and that the ICT systems and capacity performance meets the established business and information security objectives (capacity and performance management) These policies and procedures are also essential to ensure that the effective and smooth day-to-day management and operation of ICT systems (ICT operations) thereby minimising the risk of loss of confidentiality, integrity, availability of data. In this context, collectively these policies and procedures are thus necessary for ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data. In particular, the recording and monitoring of end-dates of support services provided by ICT third party service providers is also important for appropriate management of the legacy systems risk. While these requirements should apply to all ICT assets, in implementing these aspects, financial entities should focus specifically on those ICT assets or systems necessary for the business operation, considering their criticality and potential impact in case of the loss of their confidentiality, integrity and availability.

(8) As the use of cryptographic techniques can preserve availability, authenticity, integrity and confidentiality of data, it is important that financial entities referred to in Title II of this Regulation identify and implement appropriate cryptographic controls following a risk-based approach. To this end, they should perform the encryption of data at rest, in transit or, where necessary, in use based on the results of a two-pronged process, namely data classification and a comprehensive ICT risk assessment. Given the implementation complexity of encryption of data in use, financial entities referred to in Title II of this Regulation should be required to perform it only when appropriate in light of the results of the ICT risk assessment. They should be able, when encryption of data in use is not feasible or too complex, to protect the confidentiality, integrity and availability of the data through other ICT security measures. Given the rapid technological developments in the field of cryptographic techniques, financial entities referred to in Title II of this Regulation should remain abreast of relevant developments in cryptanalysis and consider leading practices and standards and should hence follow a flexible approach based on mitigation and monitoring to deal with the dynamic landscape of cryptographic threats, including those from quantum advancements.

(9) ICT operations' security and operational policies, procedures, protocols and tools are essential in ensuring the protection of confidentiality, integrity and availability of data. One pivotal aspect is the requirement for the strict separation of ICT production environments from their development, testing and other non-production environments. This separation serves as an important ICT security measure against unintended and unauthorised access, modifications and deletions of the production environment of data, which could result in major disruptions in the business operations of financial entities referred to in Title II of this Regulation. At the same time, considering current ICT system development practices, in exceptional circumstances these financial entities should be allowed to perform the testing in production environments and hence they should provide

a transparent justification, accompanied by approval of the testing in production environment, in order to manage the risk and to ensure accountability, confidentiality, availability, authenticity and integrity of production data.

(10) The fast-evolving nature of ICT landscapes, vulnerabilities and cyber threats necessitates a proactive and comprehensive approach to identifying, evaluating and addressing vulnerabilities. Lacking such approach, financial entities, their customers, users or counterparties would be severely exposed to relevant risks, which will put at risk their digital operational resilience and the security of networks as well as the availability, authenticity, integrity and confidentiality of data that ICT security policies and procedures should protect. Financial entities referred to in Title II should therefore identify and remedy vulnerabilities and ensure that both the financial entities and their ICT third-party service providers adhere to a coherent, transparent, responsible vulnerability management framework. Financial entities should monitor vulnerabilities using reliable resources and automated tools, verifying that ICT third-party service providers ensure prompt action on vulnerabilities in provided ICT services. Additionally, patch management is a crucial part of the ICT security policies and procedures for resolving identified vulnerabilities and preventing disruptions from installation of patches, through testing and deployment in a controlled environment. Furthermore, financial entities should establish procedures for responsible disclosure of vulnerabilities to clients, counterparts and the public, considering factors such as the severity of the vulnerability, the potential impact on stakeholders and the readiness of a fix or mitigation measures.

(11) Financial entities referred to in Title II of this Regulation should establish strong measures to ascertain the unique identification of individuals and systems accessing the financial entity's information to enable assignment of user access rights. The failure to do so would expose financial entities to potential unauthorized access, data breaches and fraudulent activities, thus compromising the confidentiality, integrity and availability of sensitive financial data. While the use of generic or shared accounts should be permitted under limited circumstances defined by the financial entity, it is crucial that the financial entities ensure that the accountability for actions taken through these accounts is maintained. Without this safeguard, potential malicious users would be able to hinder investigative and corrective measures, leaving the financial entity vulnerable to undetected malicious activities or non-compliance penalties.

(12) In order to manage the rapid advancement in ICT environments, financial entities referred to in Title II of this Regulation should implement robust ICT project management policies and procedures that are essential elements to maintain data availability, authenticity, integrity and confidentiality. These ICT project management policies and procedures should identify the elements necessary to successfully manage ICT projects, including changes, acquisitions, maintenance and developments of the financial entity's ICT systems, regardless of the ICT project management methodology the financial entity has chosen to use. In the context of these policies and procedures, financial entities should adopt testing practices and methods that suit their needs, while adhering to a risk-based approach and ensuring that a secure, reliable and resilient ICT environment is maintained.

In guaranteeing the secure implementation of an ICT project, it is vital for financial entities to ensure that staff from the specific business sectors or roles influenced or impacted by the ICT project can provide the necessary information and expertise. To ensure effective oversight, reports on ICT projects, especially those affecting critical or important functions, and their associated risks should be submitted to the management body. The frequency and details of the systematic and ongoing reviews and reports should be tailored to the importance and the size of the ICT projects.

(13) Financial entities referred to in Title II of this Regulation should evaluate thoroughly the software packages they are acquiring or developing to ensure their secure and effective integration into the existing ICT environment, in accordance with the established business and information security objectives. For that purpose, they should carry out ICT security testing aiming to identify vulnerabilities and potential security gaps within both software packages and the broader ICT systems. Additionally, the same financial entities should perform source code reviews, incorporating both static and dynamic testing methods, to assess the integrity of the software and ensure that the use of this software does not pose ICT security risks for the financial entities. Financial entities should perform source code reviews on software acquired, including on proprietary software provided by ICT third-party service providers, where feasible.

(14) Changes, regardless of their scale, carry inherent risks and may pose significant risks of loss of confidentiality, integrity and availability of data, and thus could lead to severe business disruptions. A rigorous verification process is thus necessary to confirm that all changes meet the requisite ICT security requirements, safeguarding the financial entities from potential vulnerabilities and weaknesses that could expose them to significant risks, as mentioned above. Financial entities referred to in Title II of this Regulation should hence have in place sound ICT change management policies and procedures as an essential element of their ICT security policies and procedures. To uphold the objectivity and effectiveness of the change management process, a clear segregation of duties is paramount, in particular it is necessary to separate the functions responsible for approving changes from those who request and implement them to prevent conflicts of interest and ensure that changes are evaluated objectively. Moreover, financial entities should assign clearly defined roles and responsibilities ensuring that changes are planned, adequately tested, and quality assured in order to achieve effective transitions, controlled change implementation and minimal disruptions to the operation of the ICT systems. Financial entities should also develop and implement fall-back procedures, as they play a pivotal role in the ICT security, providing a crucial safety net for financial entities. These procedures need to be clearly identified, with assigned responsibilities to ensure a swift and effective response in the event of unsuccessful changes, ensuring that ICT systems continue to operate effectively.

(15) Financial entities referred to in Title II of this Regulation should establish an ICT incident policy encompassing the components of ICT incident management process, in order to be able to detect, manage and report ICT incidents. In this context, financial entities should also have a well identified list of relevant contacts inside and outside the organisation,

which facilitates the correct coordination and implementation of the different phases within this process. Similarly, financial entities should place emphasis on the detailed analysis of those incidents considered most significant, also considering the reoccurrence of some of them, to optimise the detection of and response to these incidents and to properly identify the trends associated with them, which is a valuable source of information in order to enable the effective identification and addressing of root causes and problems.

(16) To guarantee an early and effective detection of anomalous activities, financial entities referred to in Title II of this Regulation should properly collect, monitor and analyse the different sources of information available, together with establishing an appropriate allocation of related roles and responsibilities. As regards internal sources of information, logs are an extremely relevant source, but reliance on them alone should be avoided; instead, financial entities should consider broader information to include what is reported by other internal functions, as they are often a valuable source of relevant information. For the same purpose, financial entities should analyse and monitor information gathered from external sources, including information provided by third party ICT providers on incidents affecting their systems and networks, as well as other sources of information that they consider as relevant.

(17) To ease ICT-incidents detection, financial entities should retain evidence of ICT-related incidents. In order to, on the one hand, ensure that such evidence is kept for a sufficient time and, on the other hand, avoid an excessive regulatory burden, financial entities should establish the retention period considering, among other things, the criticality of the data and retention requirements stemming from Union law.

(18) To ensure that incidents are appropriately detected, financial entities referred to in Title II of this Regulation should not consider the criteria for triggering ICT-related incident detection and response processes included in this Regulation as exhaustive and should take into account additional criteria where appropriate. Moreover, while each of the criteria included in this Regulation should be considered, the circumstances described in the criteria should not need to occur simultaneously and the importance of the affected ICT services should be appropriately considered to trigger ICT-related incident detection and response processes.

(19) In the development of the ICT business continuity policy financial entities referred to in Title II should consider the interrelated nature of such policy with several essential components of ICT risk management. This connection is particularly pertinent for aspects such as incident management, specifically concerning communication strategies, the change management process and the risks associated with ICT third-party providers. Hence, financial entities should take into account all these elements when preparing the ICT business continuity policy.

(20) This Regulation sets out the set of scenarios that financial entities referred to in Title II should duly take into account both for the implementation of ICT response and recovery plans and for the testing of ICT business continuity plans. The listing of these scenarios

should serve as a starting point for financial entities to analyse the relevance and plausibility of each scenario and the need to develop alternative ones. Financial entities should focus on scenarios, where investment in resilience measures could be more efficient and effective. The testing of switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities should assess if they operate appropriately and for a sufficient period of time identified and ensure that normal functioning is restored afterwards in accordance with the recovery objectives.

(21) Having regard to Recital 103 of Regulation (EU) 2022/2554, considering the specific risk profiles of central counterparties, central securities depositories and trading venues and the impact of their activities on the financial system and on service users this Regulation provides for certain requirements related to the operational risk of these financial entities. These entity=specific requirements relate to ICT project and change management (testing of ICT systems before use and after significant changes) and ICT business continuity management (components of the ICT business continuity policy and testing of the ICT business continuity policy). and they are considered necessary also as they ensure continuity with requirements, that proved particularly useful in ensuring digital operational resilience, applicable to central counterparties, trading venues and central securities depositories under, respectively, the frameworks of Regulation (EU) No 648/2012 of the European Parliament and of the Council[8], of Regulation (EU) 600/2014 of the European Parliament and of the Council[9] and of Regulation (EU) No 909/2014 of the European Parliament and of the Council[10]. As regards central counterparties and central securities depositories , the entity specific requirements are considered as fundamental also since they allow continuous compliance with the applicable international standards of the Principles for Financial Market Infrastructures issued in April 2012 by the Committee on Payments and Settlement Systems (CPSS) of the Bank of International Settlements (BIS) and the International Organisation of Securities Commissions (IOSCO).

(22) The report referred to in Article 6(5) of Regulation (EU) 2022/2554 should assist, internally, in the proper documentation and implementation of modifications or revisions of the ICT risk management framework and should serve as a basis for its periodic and ongoing review. 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. Regarding the format of the report, financial entities should select a searchable electronic format that guarantees an adequate transmission and access to the information.

(23) The provisions of this Regulation 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 and by designing the simplified ICT risk management framework for the financial entities set out in Article 16(1) of the

[8] OJ L 201 27.7.2012, p. 1.

[9] OJ L 173 12.6.2014, p. 84.

[10] OJ L 257 28.8.2014, p. 1.

same Regulation. To ensure coherence between the ordinary and the simplified ICT risk management framework, and considering that these provisions should become applicable at the same time, it is appropriate to include all the regulatory technical standards required by Article 15, first subparagraph, and Article 16(3), first subparagraph, into a single Regulation. For this purpose, this Regulation includes the technical standards adopted pursuant Article 15 of Regulation (EU) 2022/2554 in Title II and the technical standards adopted pursuant to Article 16 of the same Regulation in Title III. In light of this, Title II of this Regulation applies to financial entities as defined in Article 2(2) of Regulation (EU) 2022/2554 with the exception of those financial entities referred to in Article 16(1) of the same Regulation, and Title III applies to financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554.

(24) In identifying the requirements for the financial entities that are subject to the simplified ICT risk management framework in accordance with Article 16 of Regulation (EU) 2022/2554, only on those essential areas and elements were considered that are at a minimum necessary to ensure the confidentiality, integrity, availability and authenticity of the data and services were considered, taking into account the overall risk profile, the size and the nature, scale and complexity of the services, activities and operations of financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554. The simplified ICT risk management framework aims at ensuring a proportionate approach while providing for crucial requirements on ICT risk management.

(25) Financial entities referred to in Title III of this Regulation should have in place an internal governance and control framework with clear responsibilities to enable an effective and sound ICT risk management framework. Also, to reduce the administrative and operational burden, financial entities referred to in Title III of this Regulation should develop and document only one policy, the information security policy, that defines the high-level principles and rules to protect the confidentiality, integrity, availability and authenticity of data, security of networks, adequate safeguards against intrusions and data misuse. Finally, considering the information security objectives identified in the information security policy, financial entities referred to in Title III of this Regulation should develop, document and implement ICT security controls, measures and procedure only for the fundamental areas and technical implementation aspects identified in this Regulation.

(26) Any processing of personal data performed by financial entities in application of this Regulation should be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[11].

(27) 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

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(European Supervisory Authorities), in consultation with the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council[12].

(28) The Joint Committee of the European Supervisory Authorities referred to in Article 54 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[13], in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council[14] and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[15] 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, the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010,

HAS ADOPTED THIS REGULATION:

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

[13] 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).

[14] 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).

[15] 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 - GENERAL PRINCIPLE

Article 1

Overall risk profile and complexity

For the purposes of defining and implementing ICT risk management tools, methods, processes, policies and procedures referred to in Title II and the simplified ICT risk management framework referred to in Title III, elements of increased or reduced complexity or the overall risk profile 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 - FURTHER HARMONISATION OF ICT RISK MANAGEMENT TOOLS, METHODS, PROCESSES AND POLICIES IN ACCORDANCE WITH ARTICLE 15 OF REGULATION (EU) 2022/2554

CHAPTER I

ICT SECURITY POLICIES, PROCEDURES, PROTOCOLS, AND TOOLS

SECTION I

Article 2

General elements of ICT security policies

1. Financial entities shall ensure that their ICT security policies concerning 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 referred to in this Chapter with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse, preserving the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guaranteeing 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) indicate the date of formal approval by the management body;

(c) include indicators and measures to monitor the implementation of the ICT security policies and to record exceptions from the implementation of these 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 ICT security policies from staff of the financial entity, where such provisions on the consequence of non-compliance with policies of the financial entity are not included in other policies 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, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012;

(i) identify the roles and responsibilities for the ICT security policies' development, implementation and maintenance;

(j) are reviewed in accordance with the requirements set out in in Article 6(5) of Regulation (EU) 2022/2554;

(k) take into account material changes concerning the financial entity, including material changes to the activities or processes of the financial entity, or to the cyber threat landscape or to the applicable legal obligations.

SECTION II

Article 3

ICT risk management

1. Financial entities shall develop, document and implement policies and procedures concerning ICT risk management that are necessary 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 delay. The policies and procedures concerning ICT risk management shall include all of the following:

(a) the indication of the approval of the risk tolerance level 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 those vulnerabilities being exploited by 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 referred to in point (a). 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 the financial entity takes actions to correct or improve the measures where necessary;

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

(i) provisions on the identification of residual ICT risks;

(ii) the assignment of roles and responsibilities regarding the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level referred to in point (a), and for the assessment process referred to in point (iv);

(iii) the development of an inventory of the accepted residual ICT risks, including an explanation of the reasons for which they were accepted;

(iv) provisions on the assessment of the accepted residual ICT risks at least once a year, including the identification of any changes to the residual ICT risks, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the review;

(e) provisions on the monitoring of any changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk of the financial entity to promptly detect changes that could affect its ICT risk profile;

(f) provisions on a process to ensure that changes to the business strategy and the digital operational resilience strategy of the financial entity, if any, are taken into account.

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 necessary to preserve the availability, authenticity, integrity and confidentiality of data.

2. The policy on management of ICT assets shall:

(a) require the monitoring and management of the life cycle of ICT assets identified and classified in accordance with Article 8(1) of Regulation (EU) 2022/2554;

(b) require the financial entity to keep 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 all ICT assets, as specified in Article 8(1) of Regulation (EU) 2022/2254;

(iv) the identity of ICT asset owners;

(v) business functions or services supported by the ICT asset;

(vi) the ICT business continuity requirements, including recovery time objectives and recovery point objective;

(vii) whether the ICT asset may be or is exposed to external networks, including the internet;

(viii) the links and interdependencies among ICT assets and the business functions using each ICT asset;

(ix) where applicable, for all ICT assets, the end dates of the ICT third-party service provider's regular, extended and custom support services after which it is no longer supported by its supplier or by an ICT third-party service provider;

(c) for financial entities referred to in Article 8(7) of Regulation (EU) 2022/2554, prescribe that they keep records of the information needed to perform a specific ICT risk assessment on all legacy ICT systems.

Article 5

ICT asset management procedure

1. Financial entities shall develop, document and implement an ICT asset management procedure, with a view to preserving 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 of the financial entity.

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 be designed on the basis of the results of approved data classification and ICT risk assessment and shall include all the following elements:

(a) rules for the encryption of data at rest and in transit;

(b) rules for the encryption of data in use, where necessary. Where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected

environment or take other equivalent measures that ensure the confidentiality, integrity, authenticity and availability of data;

(c) rules for the encryption of internal network connections and traffic with external parties;

(d) provisions for cryptographic key management 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 and standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets 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, where necessary, on the basis of developments in cryptanalysis, update or change the cryptographic technology to ensure they remain resilient against cyber threats and considering the information resources referred to in Article 10(2), point (a). 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 a requirement in the policy on encryption and cryptographic controls to record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4 and to provide a reasoned explanation for doing so.

Article 7

Cryptographic key management

1. Financial entities shall lay out in the provisions on cryptographic key management referred to in Article 6(2) point (d), the requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, 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 replace 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 for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date.

5. Financial entities shall ensure the prompt renewal of certificates in advance of their expiration.

SECTION V

ICT OPERATIONS SECURITY

Article 8

Policies and procedures for ICT operations

1. As part of the ICT security policies and procedures, financial entities shall develop, document and implement policies and procedures to manage the ICT operations of ICT assets, 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. These policies and procedures shall define how financial entities operate, monitor, control and restore their ICT assets, including the documentation of ICT operations.

2. The policies and procedures for ICT operations referred to in paragraph 1 shall include all of the following elements:

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

(i) secure installation, maintenance, configuration and deinstallation of ICT systems;

(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 restoration 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 separation of ICT production environments from the development, testing and other non-production environments. The separation shall consider all of the components of the environment, such as accounts, data or connections;

(vi) requirements to conduct the development and testing in environments which are separated from the production environment;

(vii) requirements to conduct the development and testing in production environments. The policies and procedures shall provide that the instances in which testing is performed in production environment are clearly identified, justified, for limited periods of time approved by the relevant function, and considering Article 16(6). The availability, confidentiality, integrity and authenticity of ICT systems and production data shall be ensured during development and test activities in production environment;

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

(i) procedures and protocols 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 the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages.

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. The vulnerability management procedures referred to in paragraph 1 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, with the frequency and scope of these activities commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset. For the ICT assets supporting critical or important functions it shall be performed at least on a weekly basis;

(c) verify that ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity and that they report to the financial entity in a timely manner at least the critical vulnerabilities and statistics and trends. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes and implement appropriate mitigating actions;

(d) track the usage of third-party libraries, including open source, used by ICT services supporting critical or important function, of ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider. The financial entity, in collaboration with the ICT third-party service provider as appropriate, shall monitor the version and possible updates of the third-party libraries. In case of ready to use (off-the-shelf) ICT assets or components of ICT assets acquired and used in the operation of ICT services not supporting critical or important functions, the financial entity shall track to the extent possible the usage of third-party libraries, including open-source ones;

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

(f) identify criteria to prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified. For the purposes of the prioritisation, financial entities shall consider the criticality of the vulnerability, the classification established

according to Article 8(1) of Regulation (EU) 2022/2554 and the risk profile of the ICT assets affected by the identified vulnerabilities;

(g) monitor and verify the remediation of vulnerabilities;

(h) require 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 and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data.

4. The patch management procedures referred to in paragraph 3 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 patches and updates in accordance with Article 8(2), point (b), points (v), (vi) and (vii);

(d) set deadlines for the installation of software and hardware patches and updates and escalation procedures in 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 ICT system security procedure.

2. The data and ICT system security procedure referred to in paragraph 1 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 Article 21, supporting the protection requirements for each level of classification;

(b) identification of secure configuration baseline for ICT assets that will minimise their exposure to cyber threats and measures to verify regularly that these baselines are those that are effectively deployed. The secure configuration baseline shall take into account leading

practices and appropriate techniques referred to in standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012;

(c) identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices;

(d) identification of security measures against malicious codes;

(e) identification of security measures to ensure that only authorised data storage media, ICT systems and endpoint devices are used 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 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 in an unauthorised manner;

(iii) the authorisation to use removable data storage devices only where the residual ICT risk remains within the financial entity's risk tolerance level referred to in Article 3, paragraph 1, point (a);

(g) the process to securely delete data, present 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 present on premises or stored externally containing confidential information;

(i) the identification and implementation of security measures to prevent data loss and leakage for ICT 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 ICT assets or services operated by an ICT third-party service provider, the identification and implementation of requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment. In identifying these requirements, financial entities shall consider at least the following:

(i) implementation of vendor recommended settings on the elements operated by the financial entity;

(ii) clear allocation of information security roles and responsibilities between the financial entity and the ICT third-party service provider, in accordance with the principle of full responsibility of the financial entity referred to in Article 28(1), point

(a), of Regulation (EU) 2022/2554, and, for financial entities referred to in Article 28(2) of the same Regulation, with [Article 3] of Commission Delegated Regulation (EU) XXXX/XXX [Commission Delegated Regulation supplementing Article 28(2) of Regulation (EU) 2022/2554;

(iii) ensuring and maintaining adequate competences within the financial entity in the management and security of the service used;

(iv) technical and organisational measures to minimise the risks related to the infrastructure used by the ICT third-party service provider for its ICT services, considering leading practices and standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012.

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 of 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. 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;

(b) alignment of the level of detail of the logs with their purpose and usage to enable the effective detection of anomalous activities as specified in Article 24;

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

(i) identity management in accordance with Article 20 and logical and physical access control, in accordance with Article 21 and;

(ii) capacity management;

(iii)change management;

(iv)ICT operations, including ICT system activities;

(v) network traffic activities, including ICT network performance;

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

(e) measures to detect failure of logging systems;

(f) without prejudice to any applicable regulatory requirements under national or Union law, the synchronisation of the clocks of each of the financial entity's ICT systems upon a documented 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 elements:

(a) the segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of ICT assets using them;

(b) the documentation of all of the financial entity's network connections and data flows;

(c) the use of a separate and dedicated network for the administration of ICT assets;

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

(e) the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks and wireless networks, for 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 Article 6(2);

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

(h) the identification of the roles and responsibilities and steps for the definition, implementation, approval, change and review of firewall rules and connections filters. Financial entities shall perform the review of firewall rules and connections filters on a regular basis according to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions, the financial entities shall verify the adequacy of the existing firewall rules and connection filters at least every six months;

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

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

(k) the implementation of a secure configuration baseline of all network components and hardening the network and network devices according to vendor instructions, to, where applicable, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 and leading practices;

(l) the 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 by an ICT intra-group service provider or by ICT third-party service providers;

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 for both the staff of the financial entity and of third parties are implemented, documented and regularly reviewed.

2. The policies, procedures, protocols and tools to protect information in transit referred to in paragraph 1 shall take into account the results of the approved data classification and the ICT risk assessment processes.

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 the 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) relevant milestones;

(f) change management requirements;

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

4. The ICT project management policy shall ensure the secure ICT project implementation through the provision of the necessary information and expertise from the business area or functions impacted by the ICT project.

5. The ICT project management policy shall provide that 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 the acquisition, development and maintenance of ICT systems;

(b) require the identification of technical specification and ICT technical specification, as respectively defined in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012, of requirements relating to acquisition, development and maintenance of ICT systems, with a particular focus on ICT security requirements and on 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, which shall include all of the following:

(a) the requirements to test and approve all ICT systems prior to their use and after maintenance, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). The level of testing shall be commensurate to the criticality of the concerned business functions 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.

(b) the requirements to perform source code reviews covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and

applications, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation.

(c) the requirements to perform security testing of software packages at no later than the integration phase, in accordance with Article 8(2), point (b), points (v), (vi) and (vii).

(d) the requirement that non-production environments only store anonymized, pseudonymized or randomized production data and that financial entities shall protect the integrity and confidentiality of data in non-production environments.

(e) the requirement to 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;

(f) the requirement that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment.

3. For the purposes of the testing according to paragraph 2, point (a):

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

(b) central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, 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.

4. By way of derogation from paragraph 2, point (d), production data that are not anonymized, not pseudonymized or not randomized may be stored only for specific testing occasions, for limited periods of time and following the approval by the relevant function and, for financial entities other than microenterprises, the reporting of such occasions to the ICT risk management function.

5. The 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.

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 the 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, central counterparties and central securities depositories shall submit their ICT systems to stringent testing by simulating stressed conditions:

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

(b) a central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, 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 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 cyber threat landscape, to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the 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) a reference to the section of the policy on control of access management rights referred to in Article 21(1) point (g);

(b) 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 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;

(c) 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;

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

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

CHAPTER II

HUMAN RESOURCES POLICY AND ACCESS CONTROL

Article 19

Human resources policy

1. As part of their human resource or other relevant policies financial entities shall include all of the following ICT security related elements:

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

(b) requirements for staff of the financial entity and of the ICT third-party service providers using or accessing ICT assets of the financial entity 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 behaviour, including, where applicable, those established according to Directive (EU) 2019/1937 of the European Parliament and of the Council[16];

(iii) upon termination of employment, requirements for the staff to return to the financial entity all ICT assets and tangible information assets in their possession that belong to the financial entity.

Article 20

Identity management

1. 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 21.

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

(a) without prejudice to Article 21(1), point (c), the assignment of a unique identity corresponding to a unique user account to each staff member of the financial entity or staff

[16] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).

of the third-party service providers accessing the information assets and ICT assets of the financial entity;

(b) the maintenance of records of all identity assignments referred to in point (a). These records shall be kept following a reorganisation of the financial entity or after the end of the contractual relationship without prejudice to the retention requirements set out in Union and national law;

(c) a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation and termination of all accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process.

Article 21

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) assignment of 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) provision on user accountability, by limiting to the extent possible the use of generic and shared user accounts and ensuring that users are identifiable for the actions performed in the ICT systems at all times;

(d) provision on restrictions of access to ICT assets, setting out controls and tools to prevent 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 provision on all the following:

(i) 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 (a);

(ii) assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Where 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 privileged access management;

(iii) revoking of access rights without undue delay upon termination of employment or when the access is no longer necessary;

(iv) update of access rights where changes are necessary and at least once a year for all ICT systems, other than ICT systems supporting critical or important functions and at least every six months for ICT systems supporting critical or important functions;

(f) authentication methods including all of the following:

(i) the use of authentication methods commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the 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 control measures including:

(i) identification and logging of natural persons who are authorised to access premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. This identification and logging 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;

(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 or both reside. The monitoring should be commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 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 22

ICT-related incident management policy

1. As part of the mechanisms to detect anomalous activities, including ICT network performance issues and ICT-related incidents, 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 relevant 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 management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours in accordance with Article 23;

(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, commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets, in accordance with [Article [15] of Commission Delegated Regulation (EU) […]/[…] [Commission Delegated Regulation on classification of ICT-related incidents] and with any applicable retention requirement according to Union law. This evidence shall be retained in a secure manner.

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

Article 23

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, 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, monitor and analyse all of the following:

(i) internal and external factors, including at least the logs collected according to Article 12, information from business and ICT functions and any problem reported by users of the financial entity;

(ii) potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity;

(iii) 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;

(b) identify anomalous activities and behaviour and implement tools generating alerts for 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 anomalies affecting the completeness and the integrity of the data sources or log collection;

(c) prioritise the alerts referred to in point (b) to allow the detected ICT-related incidents to be managed within the expected resolution time, as defined by financial entities, both during and outside working hours;

(d) record, analyse and evaluate any relevant information on all anomalous activities and behaviours automatically or manually.

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

4. The financial entity shall log all relevant information for each detected anomalous activity to enable identification of the date and 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 the availability, authenticity, integrity and confidentiality of data;

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

(d) ICT systems' and network unavailability.

6. When evaluating the criteria set out in paragraph 5, financial entities shall consider the criticality of the services affected.

CHAPTER IV

ICT BUSINESS CONTINUITY MANAGEMENT

Article 24

Components of the ICT business continuity policy

1. Financial entities shall include in their 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 and deactivate 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 26(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 ICT business continuity plans for severe business disruptions as part of these plans, and the prioritisationof 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 25 and 26;

(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) of Regulation (EU) 2022/2554 and to the communication and crisis communication actions referred to in Article 11(2), point (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 their 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 the 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 immediate access to a secondary business site 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 their 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 their 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 ICT service of the trading venue after a disruptive incident is close to zero.

Article 25

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).

2. Financial entities shall assess through the testing of their ICT business continuity plans whether they are able to ensure the continuity of the financial entity's critical or important functions. The testing of the ICT business continuity plan shall:

(a) be performed on the basis of test scenarios that simulate potential disruptions, including an adequate set of severe but plausible scenarios. The 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. In testing the business continuity plans as regards ICT third-parties services, financial entities shall duly consider scenarios linked to insolvency or failures of the ICT-third party service provider or of political risks in the provider's jurisdiction, where relevant;

(c) for financial entities referred to in the second subparagraph of Article 11(6) of Regulation (EU) 2022/2554, include scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities. The testing shall

verify whether at least critical or important functions can be operated appropriately, for a sufficient period of time and whether the normal functioning may be restored;

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

(e) include procedures to verify the ability of the staff of financial entities, ICT third-party service providers, ICT systems and ICT services to respond adequately to the scenarios duly taken into account in Article 26(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 their business continuity policies.

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 their business continuity policy.

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

Article 26

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, deactivation and any exceptions;

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

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

(d) be documented and made available to the staff involved in their execution and be 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 recovery;

(f) lay down the objectives and the conditions to declare a successful execution of the plans.

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. Financial entities shall duly take into account all of the following scenarios:

(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 consider 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 staff members in charge of guaranteeing the continuity of operations;

(f) impact of climate change and environment degradation related events, natural disasters, pandemic, and physical attacks, including intrusions and terrorist attacks;

(g) insider attacks;

(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 outages.

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 costs, risks, logistics or unforeseen circumstances.

4. As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers of ICT services supporting critical or important functions to the financial entity.

CHAPTER V

REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW

Article 27

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, the subject of the report and describes its group structure, where relevant;

(ii) 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 that a total loss or severe degradation of such systems would have in terms of critical or important functions and market efficiency;

(iii) summarises the major changes in the ICT risk management framework since the previous report;

(iv) provides an executive level summary of the current and near-term ICT risk profile, threat landscape, the assessed effectiveness of its controls and the 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 for 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 function responsible 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, where appropriate;

(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) conclusions resulting from 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 the mitigation 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 at least all of the following:

(i) for financial entities referred to in Article 6(6), of Regulation (EU) 2022/2554, results from internal audit;

(ii) results from compliance assessments;

(iii) results from digital operational resilience testing and, where applicable, advanced testing of ICT tools, systems and processes based on TLPT;

(iv) external sources.

TITLE III – SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK FOR FINANCIAL ENTITIES REFERRED TO IN ARTICLE 16(1) OF REGULATION (EU) 2022/2554

CHAPTER I

SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK

Article 28

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 framework that ensures 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 referred to in paragraph 1 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 in accordance with its 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) classification of information assets referred to in Article 30 paragraph 1, 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), point (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 policy and the measures included in Chapters I, II and III of this Title to identify, assess and manage the ICT risk the financial entity is exposed to;

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

(h) ensures that the staff of the financial entity is kept 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) establishes 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 ICT intra-group or ICT third-party service providers. 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 their ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. The 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 outcome of 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 29

Information security policy and measures

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document and implement 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 of 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 ICT third-party service providers.

3. The ICT security measures shall include all of the measures referred to in Articles 30 to 38.

Article 30

Classification of information assets and ICT assets

1. As part of the ICT risk management framework referred to in Article 16(1), point (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 31

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

(b) identification and assessment of the ICT risks to which the financial entity is exposed;

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

(d) monitoring the effectiveness of the mitigation strategies referred to in point (c);

(e) identification and assessment of any ICT and information security risks resulting from any major change in ICT system or ICT services, processes or procedures, as well as 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' ICT 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.

Article 32

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 designed according to the threat landscape and to the classification referred to in Article 30 paragraph 1 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 33

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 user and generic accounts, including generic administrator accounts. Privileged, emergency and administrator access shall be assigned on a need-to-use or an ad-hoc basis for all ICT systems and shall be logged in accordance with Article 34(1), point (f);

(d) the use of authentication methods commensurate to the classification referred to in Article 30 paragraph 1 and overall risk profile of ICT assets and considering leading practices.

(e) 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;

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

Article 34

ICT operations security

1. As part of their systems, protocols and tools, and for all ICT assets, 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 ICT third-party service providers, if applicable;

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

(d) perform automated vulnerability scanning and assessments of ICT assets commensurate to their classification referred to in Article 30 paragraph 1 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 information on anomalous activities and behaviour 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 35

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 ensure the security of networks against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data and shall establish all of the following taking into account the classification performed pursuant to Article 30(1):

(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 of or decommission 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 its critical activities in an adequate, timely and secure manner.

Article 36

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 Articles 33 to 35 and 37 to 38, and ensure that this plan considers threats and vulnerabilities identified as part of the ICT risk management framework referred to in Article 31(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 ICT systems supporting critical or important functions.

Article 37

ICT systems acquisition, development and maintenance

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall design and implement, where appropriate, a procedure governing the acquisition, development and maintenance of ICT systems 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 function;

(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 38

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 their initiation to 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 39

Components of the ICT business continuity plan

1. Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop their ICT business continuity plans considering the results of the analysis of their exposures to and potential impact of severe business disruptions and scenarios to which their ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario.

2. 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 the recovery and resumption of functions and key internal and external dependencies including ICT third-party service providers;

   (e) identify the conditions that may prompt the 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;

(f) identify the 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 the financial entities. These measures shall include the mitigation of failures of critical third-party providers as well;

(g) identify backup procedures and measures 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;

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

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

(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 40

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 39, including the scenarios defined in Article 39(1) at least once every year for the back-up and restore procedures or upon 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 RISK MANAGEMENT FRAMEWORK

Article 41

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. The report shall include all of the following information:

(a) an introductory section providing:

(i) a description of 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 implications that a total loss or severe degradation of such systems would have on critical or important functions and market efficiency;

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

(iii) information about the reported area;

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

(v) a summary and a description of the impact of major changes to the ICT risk management framework since the previous report;

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

(c) a description of the reasons 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 thereof;

(g) remedying measures identified to address weaknesses, deficiencies and gaps in the ICT risk management framework and expected date for implementing these measures including the follow-up on 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.

TITLE IV – FINAL PROVISIONS

CHAPTER I

FINAL PROVISIONS

Article 42

Entry into force

This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, XX XXXX XXXX

For the Commission

The President

XXXXX

4. Accompanying documents

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 Final Report (FR) 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. The feedback on the consultation paper on the same draft RTS has been considered for this impact assessment.

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 draft 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 draft RTS.

POLICY ISSUE 1: TECHNOLOGY NEUTRALITY

Options considered

11. Option A: the draft 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. Specific provision can be included regarding ICT assets or services managed by third-party service providers. These involves implementing vendor-recommended settings, clearly defining security roles and responsibilities as per Regulation (EU) 2022/2554, and ensuring robust management and security competences while aligning with leading standards and practices under Regulation (EU) No 1025/2012.

12. Option B: The draft 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 draft 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 draft 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 draft 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 draft 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 draft 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 A has been retained.

POLICY ISSUE 2: PRESCRIPTIVENESS OF THE DRAFT RTS

Options considered

17. Option A: the draft 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 draft RTS should take a principle-based and objective-focused approach.

19. Option C: the draft 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 draft 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 draft 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 draft RTS should define the logging retention periods for all logs it refers to.

24. Option B: the draft 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 draft 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 draft 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 draft 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.

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. DORA includes a general article on proportionality in the draft RTS would ensure that this principle is followed by both financial entities and supervisors reducing the overall costs for the implementation of the draft 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 draft RTS specific ways to adapt the implementation of the draft 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.

Preferred option

Both options have been considered by the ESAs to prepare their proposal. The preferred option consists of a general provision (Article 1) requiring financial entities to consider elements of increased or reduced complexity and the overall risk profile when defining and implementing the ICT risk management tools.

Moreover, in order to cater for specific risks related to certain financial entities, few entity-specific provisions have been added (relating to CCPs-CSDs-trading venues).

The ESAs consider also that the draft RTS provides for requirements that, while ensuring digital operational resilience, should not constitute an excessive burden for financial entities, which should further be calibrated in light of Article 1.

Views of the ESAs Stakeholders Groups

The ESAs stakeholder groups (SGs) provided responses selectively, addressing only certain of the questions posed in the consultation paper on the draft RTS which are included below.

4.1.1 General comments

The SGs welcome the overall approach the JC has taken of setting overall principles, with further specification for specific sectors or types of entity only where necessary in the light of their activities and the associated risk profile. The SG consider this is likely to be both simpler to implement and more effective than trying to anticipate and prescribe in advance every detail.

The SGs are also pleased to see that the three ESAs are working together as a single, integrated team which is necessary to deliver the regime efficiently and in a timely way, to make the best use of the available resources, and to ensure appropriate coherence in the resultant regime. Many of their specific comments are designed to ensure that in implementing the risk management framework, financial entities pay due consideration to the impact of an incident on its customers and users. This will help financial entities themselves by providing clarity about priorities and helping to reduce the reputational harm and other fallout from incidents that arise. It should also reduce the harm to customers, which is not only financial, but that can also arise from such incidents.

Finally, the SGs think it would be useful in due course to consider how physical impacts of climate change could interact with the ICT aspects of business continuity planning and incident recovery and to make a more explicit connection within the RTS to considering climate scenarios and climate stress tests in digital operational resilience. Some climate-related issues (e.g., a change in the propensity to flood of an area where datacentres are located) have a direct impact on digital operational resilience, while recognising that there are broader aspects of climate change that may be less directly relevant.

ESAs' response

The ESAs welcome and take note of the SGs' feedback. The impact of climate change is considered in the proposed draft RTS as, to design their response and recovery plans, financial entities shall also duly take into account the "impact of climate change and environment degradation related events" (cf. Article 26(2)(f) of the draft RTS).

4.1.2 Answers to specific questions

Q1. Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA ('general' ICT risk management framework) and in particular its article on Complexity and risks considerations (Article 29 in the CP draft RTS, now Article 1 of the draft RTS)? If not, please provide detailed justifications and alternative wording as needed.

The SGs agree that it is appropriate to include proportionality in this way as not all distinctions of risk and scale can be identified in advance and included explicitly in the rules. Incorporating this principle is therefore useful. However, the SGs think it is important that the proportionality criteria include consideration of the impact on customers and users, not just on the financial entity, and therefore suggest adding words as follows: "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 and on its customers and users." The SGs also think there would be benefit in carrying out supervisory convergence work after implementation to ensure appropriate coherence and consistency in the assessment of risk and complexity undertaken by different authorities.

ESAs' response

The wording chosen in the new Article 1 of the proposed draft RTS refers to "*elements of increased or reduced complexity or overall risk profile*" which the ESAs consider is wide enough to also cover the impact on the financial entity's customers and users.

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

The SGs welcome the explicit consideration of proportionality considerations.

ESAs' response

The ESAs welcome the SGs' comment. Please note that in addition, the general considerations on overall risk profile and complexity included in the abovementioned new Article 1 of the draft RTS also apply to the simplified risk management framework.

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

The SGs consider it important that assigning responsibilities to the 'control function' does not relieve the business itself, as first line of defence, of responsibilities to 'design-in' and facilitate the delivery of robust information security and service delivery. Doing so could mean that in practice security considerations are considered too late in the day or remotely from other decisions to be effectively incorporated. The SGs therefore suggest that the JC consider changes to the wording of Article 2(1), point (b) and point (f) as follows:

(b) ~~managing and~~ monitoring **and ensuring the management of** 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;

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

The SGs also think that consideration should be given to including a provision on the role of assurance in both preventing and remediating problems and in verifying the first line's assessment of ICT robustness and resilience, and that at least for systems supporting critical and important functions and for complex change projects that is likely to require some external assurance.

In Article 1 (2)(c) it is unclear whether having a specific policy for exception management, governing the lifecycle of exceptions, should be enough. Also, the requirement to record all potential exceptions could be unfeasible and should incorporate some criteria to discriminate exceptions according to risk, breadth of scope and/or pervasiveness in specific domains.

The SGs do not think adequately that a policy for security policies should define the consequences of noncompliance with those policies for staff members as indicated in Article 1 (2)(e). Banks articulate policies for employees that are not compliant with internal policies generically but not at specific policy level. This requirement has not been seen in other policies, nor required by any other EBA guidance.

ESAs' response

Regarding the proposed amendments to the former Article 2, please refer to the feedback included in the full table of responses to the public consultation. The ESAs consider that governance is a fundamental aspect of any ICT risk management framework, and that this is an element where introducing certain provisions could provide greater clarity in the process of implementing the requirements, and for these reasons the inclusion of governance requirements in former Article 2 was considered in the consulted RTS.

On the other hand, in view of the feedback received and in line with the scope of the mandate set out in DORA, the former Article 2 has been deleted in its entirety. The ESAs will assess the relevance of providing additional guidance on this issue in the future. All other proposals for specific modifications to this article have not been considered as they have no further purpose after the deletion of this article.

Regarding the proposed amendments to former Article 1, these have been considered and various amendments have been included in the revised text. In particular, the exemptions in former Article 1.2(c) have been clarified, considering on the other hand that the registration of such exemptions should be exceptional and, in any case, extremely relevant, and therefore no changes have been made in this respect. With regard to former 1.2(d), the text has been modified, limiting the obligation to include provisions linked to non-compliance by staff and eliminating references to third parties. Please also refer to the feedback table for a more complete overview of the changes in this article.

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

In Article 3(1)(b) to Article 3(1)(e) it is unclear whether the aim is to describe the content of the risk assessment methodology and procedure or the result: i.e., is this describing the procedure and methodology to identify vulnerabilities and threats, or what those threats and vulnerabilities actually are. The SGs think that both the content and result are needed and suggest that the easiest way to achieve this could be to include an explicit provision on the documenting of key assessments and decisions made in accordance with the policy and process as follows: (f) requirements for the documentation of key assessments and decisions made in the implementation of the policy. The SGs also think that consideration should be given to including a provision on the role of assurance in both preventing and remediating problems and in verifying the first line's assessment of ICT robustness and resilience, and that at least for systems supporting critical and important functions and for complex change projects that is likely to require some external assurance. Finally, the SGs suggest referring to 'risk mitigation measures' rather than 'risk treatment measures' in, for example, Article 3(1)(c) to better align with standard terminology.

ESAs' response

The ESAs believe that the requirements regarding Article 3(1)(b) to Article 3(1)(e) are sufficiently clear and refer to the documentation of those elements in the risk management policy and procedures. The request to add additional the requirements proposed is disregarded since their costs would outweigh the benefits.

Finally, the term "risk treatment measures" is maintained in the RTS as it is a comprehensive terminology that encompasses a broader range of actions including, but not limited to, risk mitigation. This phrase is aligned with established international standards which advocate for the usage of "risk treatment" to refer to the process of selecting and implementing measures to modify risk. This term not only involves mitigating risks but also accepts, avoids, or transfers them, thereby offering a more versatile approach to risk management. The usage of this term ensures consistency with international standards terminology and best practices and accommodates a multi-faceted approach to risk management, which is essential in addressing the varied and complex risk land-scape financial entities operate in. Risk treatment measures will not be changed into risk mitigation measures in Article 3(1)(c).

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

The SGs consider that the objectives specified in DORA Article 15(a) which underpin these provisions are broader than those incorporated in the current text. The missing element should be incorporated because the penetration of systems may result in harm to the institution and its customers even where the data remains available, for example where it enables a denial-of-service attack. The SGs therefore propose the following addition:

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 ensuring the security of networks against intrusion and preserving the availability, authenticity, integrity and confidentiality of data. In relation to the protection of data, the SGs consider that it would be helpful to make specific reference to the documentation of 'end-of-life' procedures for the ICT assets to ensure that data cannot be compromised after the ICT asset is taken out of use. The SGs therefore propose to add a new point x) as follows:

x) the measures to be taken at the end of the ICT asset's use to protect the integrity of data.

In Article 5(2) it is important that the assessment of the impact of data loss takes explicit account of the impact on customers, users or counterparties not only the financial institution's business processes and activities. Without this requirement there is a potential for financial entities to make prioritisation decisions that do not take account of the wider market impact of data being compromised or unavailable. The SGs therefore propose an addition as follows:

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 the financial entity's business processes and activities and its customers, users or counterparties.

Article 4.2. v prescribes that the financial entity will keep records of all the information needed to perform specific ICT risk assessment on all legacy ICT systems. The SGs think that it is an excessive burden for institutions to include all this information, the SGs think only information needed to assess the criticality of the application should be stored for all systems, and only when an application is critical all other information should be stored.

ESAs' response

The ESAs consider that the proposed point (x) on the integrity of data is already covered since financial entities should develop, document and implement a policy on management of ICT assets, with a view to preserving also the integrity of data. In particular, as specified under the proposed Article 4(2)(a), such policy should prescribe the monitoring and management of the life cycle of ICT assets identified and classified in accordance with Article 8(6) of Regulation (EU) 2022/2554.

Also, the proposal to add the impact on customers, users or counterparties is redundant because these groups are already encompassed within the scope of the 'business processes and activities' of the financial entity. The ESAs consider that the current proposal sufficiently covers the impact on all relevant stakeholders, including customers, users, and counterparties, by addressing the broader spectrum of business processes and activities.

Article 8(7) of Regulation (EU) 2022/2554 introduces a specific ICT risk assessment on all legacy ICT systems. Such requirement cannot be modified by the RTS. The policy on management of ICT assets should prescribe that the information needed to perform the specific ICT risk assessment foreseen by Article 8(7) should be recorded. The ESAs do not consider this as an excessive burden since a financial entity should base its specific risk assessment on the said information.

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?

Yes. This should help financial entities themselves to identify and manage sources of potential risk and is a key safeguard for customers, users and counterparties who may be affected if such risks are not managed. The risk profile of an asset increases significantly once it is out of support, so clarity on when this will happen is an important first step towards risk management.

ESAs' response

The ESAs agree with the feedback received and included new point (ix) under Article 4(2)(b).

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

In general, the SGs agree with the approach taken.

In particular, the SGs support the reference to 'leading practices' given the rapid evolution likely to occur in this area. The SGs also support the requirement to document the reasons where a financial entity concludes it cannot adopt such 'leading practices', and the mitigation and monitoring undertaken as a result. However, it would be useful to identify – not necessarily in the legal text but perhaps in supporting material – the kinds of situations in which it might be necessary and acceptable not to use leading practice. Given the quick evolution on encryption technology and practices and the time required to adopt them, policies should reflect adoption times, having in mind that "leading practices" could change due technology evolution (even when the former leading practices stay secure) or due to not being secure or due to vulnerabilities published in protocols (e.g., TLS 1.0)

In relation to Article 6(2)(a), the SGs note that it is increasingly feasible to encrypt data 'in use' and that such encryption is likely to be the best way to protect 'in use' data. If there are situations where this is not possible with the available technology, the SGs agree that there should be a requirement for a segregated environment, although some stakeholders envisage this would be costly to implement and would welcome clarification of the benefits in terms of risk reduction. Developing a new segregated environment for data that cannot be encrypted at use can be excessively prescriptive on the mitigation solution, it could be better stated that banks should define compensatory measures to minimize the associated risks.

On the other hand, the SGs think that this provision should make it clear that data must be encrypted in the case of sensitive data, and depending on the classification of the information established by the entities. The current wording is not too clear, and it seems that it is necessary to encrypt all data, regardless of its classification. The SGs think it is important to include the specific measures on cryptographic key management in Article 7 given the impact of any loss or failure to protect such keys on entities and their customers.

ESAs' response

The ESAs may consider developing further guidelines specifying the situations in which it might be necessary and acceptable not to use leading practice.

The ESAs amended Article 6 to permit alternative mitigation measure to the processing of data in use in a separated and protected environment. It is important to notice that the encryption of data is made in accordance with the results of approved data classification and ICT risk assessment. Therefore, if the data classification and the ICT risk assessment foreseen an encryption of data in use and the latter is not possible, financial entities can process data in use in a separated and protected environment or use other mitigation measure that offer the same level of protection as the one envisaged in a separated and protected environment.

The ESAs amended Article 6 to make it clear that encryption and cryptographic controls shall be designed on the basis of the results of approved data classification and the ICT risk assessment.

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

Yes, subject to the points below.

Article 10(2)(b) requires a weekly automated scan for vulnerabilities in relation to critical systems. There may be situations where:

- in times of heightened threat, a weekly scan is clearly insufficient.
- regardless of the scanning an entity is specifically alerted to a particular vulnerability.

The SGs consider that provision should be made for these two situations, such as the following:

(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 **or more frequently where a heightened threat level or vulnerability is identified by or notified to the financial entity**.

Article 10 does not appear to require patches to be deployed promptly once identified, even though it is not until the patch is deployed that the risk is reduced and it is entirely possible that an extended

delay between identifying the patch and implementing it could be the root cause of vulnerabilities being successfully exploited. The SGs do not think this gap is addressed by the wording on prioritisation in point (g) because 'prioritise' is used there more in the sense of determining relative priorities. The SGs therefore suggest adding to point (f) as follows:

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

The criteria for prioritisation of patches in Article 10(g) should also cover the impact of a successful exploitation of a vulnerability on customers, users or counterparties, not just the criticality to the entity itself".

(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 **and the impact of a successful exploitation of a vulnerability on customers, users or counterparties**;"

Article 10(2)(c) requires the ICT TPSP to handle "any" vulnerability. It would be useful to consider whether there is scope for incorporating a risk-based approach more explicitly in this requirement.

In Article 12(2)(c)(i) and in relation to logging for physical access control it would be preferable to limit the scope to the financial entity's premises that hold critical and important ICT [processing] facilities.

Article 12(2)(g) requires the synchronization of all the financial entity's clocks to a single, reliable reference source. Given that for trading venues and their members both the acceptable sources and tolerances for the required accuracy are already specified in Level 2 measures, the SGs consider it would be helpful to include a cross-reference here, as follows: (g) the synchronisation of the clocks of all the financial entity's ICT systems upon a single reliable reference time source, taking account where applicable of the time source and accuracy requirements in Commission Delegated Regulation 2017/574.

ESAs' response

The ESAs believe that mandating an automated weekly scanning for ICT assets supporting critical or important functions is a proportionate measure to be applied across the whole financial sector. The provision does not preclude to have more frequent scanning since the scope and frequency of such scanning should be in any case commensurate to the classification established according to 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset.

The ESAs believe that the use of "promptly" for the deployment of patches does not add more clarity compared to what is already in the text of RTS. New Article 10(2)(f) already foresees a risk-based approach through a prioritisation process based on the criticality of the vulnerability, the classification and risk profile of the ICT assets affected by the identified vulnerabilities. Also, the criticality of the

vulnerability already encapsulates the potential negative impact on customers, users, or counterparties.

Regarding Article 12(2)(c), the ESAs limited the scope of the reporting for at least the critical vulnerabilities. However, for the financial entity to have a comprehensive view, the financial entity should also verity through the vulnerability management procedure that the ICT third-party service provider provide at least statistics and trends on all vulnerabilities.

Regarding Article 12(2)(c)(i), the ESAs specified that the logging of logical and physical access should be performed in accordance with Article 21 of the RTS on access control. Article 21(1)(g) refers to logging of natural persons who are authorised to access premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. This identification and logging 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. Also, the monitoring of such access should be commensurate to the classification of the assets established according to Article 8(1) of Regulation (EU) 2022/2554 and the criticality of the area accessed. The ESAs believe that the reference to Article 21 solve the concerned raised by the group.

Regarding Article 12(2)(g), the ESAs amended the provision including the wording “without prejudice to more stringent applicable clock synchronisation requirements set in sectorial regulations” to address the concern raised by the group.

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.

The SGs believe that requiring vulnerability scans to be performed on a weekly basis for assets supporting critical and important functions is too demanding. A monthly periodicity would be more in line with the risk criteria referred to in this same article.

ESAs’ response

The ESAs believe that mandating an automated weekly scanning for ICT assets supporting critical or important functions is a proportionate measure to be applied across the whole financial sector.

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

In relation to Article 13 (b) mapping and visual representation of all the financial entity’ networks and data flows, maintaining up-to-date diagrams of this type is extraordinarily costly and technically challenging. A clarification of the expected level of detail and scope would be helpful, as it is obviously

impossible to maintain this for "all networks & data flows". Perhaps it should be considered to maintain only the most critical.

ESAs' response

The ESAs considered the feedback and changed the requirement by referring to documentation of all of the financial entity's network connections and data flows rather than their mapping and visual representation. The ESAs consider the control should be applied to all networks connections and data flows to maintain a high standard of digital operational resilience of the financial entities. This comprehensive approach ensures that no potential vulnerabilities are overlooked preventing the spread of issues from less monitored areas to critical ones. Therefore, the proposal to have this documentation for the most critical network connections and data flows is disregarded.

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

The SGs welcome the inclusion of provisions on ICT project and change management to address situations in which exposure to risks and vulnerabilities can change and may be particularly acute.

The SGs welcome the fact that the requirements are applied to both the 'acquisition' and 'development' of systems as both require effective security management. The SGs think it is important to clarify that the requirements apply not only in relation to the initial acquisition or development, but also to any subsequent development, upgrade or material reconfiguration, for example as follows:

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, the initial and any subsequent further development or material reconfiguration of the financial entity's ICT systems.

In relation to Article 15 g) testing of all requirements, including security requirements, and respective approval process when deploying an ICT system in the production environment, the SGs would ask for clarification about what is meant by "all requirements" since it could be unapproachable as part of all the changes. Perhaps it is necessary to clarify that they are only the requirements associated with the change itself.

The SGs propose that two extra matters should be addressed in Article 15(3):

- Criteria for 'Go/no go' decisions should include consideration of the risk of harm to customers/users/counterparties from either decision, at least for critical systems; and
- It would be helpful to specifically reference the identification and management of interdependencies in planning and in 'go/no go' decisions.

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, including identification and management of dependencies; (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; (h) criteria for 'go/no go' decisions on deployment which take account of the risk of harm to the financial entity's customers or users from either decision.

The SGs agree that it is important to ensure appropriate reporting on ICT projects to the management body. A typical problem with such reporting is that information is conveyed in a way which might be meaningful for IT professionals but does not convey the impact on the business, its customers, clients or counterparties. The SGs think it is important that this problem is recognised and addressed. This would help both the customers, clients and counterparties and also enable the financial entity to better manage reputational and other risks. The SGs therefore propose an addition to paragraph 5 as follows:

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). **Such reporting should be in a form that conveys to non-ICT specialists the business impacts and impacts on customers, users and counterparties of the status of the ICT projects and of any alternative options under consideration**.

It is important that Article 16(2) applies in relation to any upgrade or reconfiguring of functionality, not just to the initial deployment. This should be clarified. It is also important that assessment of criticality takes account of the impact on customers and users, not just the financial entity itself.

The SGs propose to address the first two points as follows:

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 policy shall cover the initial acquisition or development and any subsequent development or significant reconfiguration**. The level of testing shall be commensurate to the criticality of the concerned business procedures and ICT assets **and the risk of harm to customers or users from any resulting incident or outage**. 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;

And the third point by adding a new point (c) based on the drafting for CSDs.

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

Article 16.5 establishes that financial entities shall perform security testing of software packages not later than the integration phase. A clarification is needed on what is meant by "packages", whether it is an application unit or if it refers to each of the libraries, including OSS and third-party proprietary software.

As per Article 16.9."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." This requirement is difficult to guarantee for the owner; it could be prohibited in the license to perform these tests or be complex due to not having the source code. Clarification is needed on what is expected for third-party software for which financial institutions do not have source code or for which there is no compile in-house.

ESAs' response

The ESAs consider that the current provisions included in the three articles under the ICT project and change management section significantly cover not only procurement but also changes in the form of development or maintenance. The need to consider such modifications is not only included in the ICT project management policy but has been detailed in the two articles that complement the section. In particular, Article 17 elaborates the detailed requirements linked to the management of all changes.

Article 15 establishes the elements to be included in the ICT Project management policy, and at this level, it is necessary to elaborate how the different requirements included in the projects will be tested. Therefore, its scope of application is linked to project management itself, and elements not included in this context should not be considered.

The inclusion of two additional elements in Article 15(3) has been analysed and it has been found that the current provisions provide a sufficient level of granularity but also proportionality with respect to the elements to be identified in the ICT Project management policy. Moreover, the policy already considers elements linked to project governance in point (b) and risk assessment in point (d).

In relation to the extension of reporting to the management body to report specifically on the impact on customers, users and counterparties, the ESAs consider that the current provisions already provide sufficient coverage for the reporting of risks associated with these stakeholders. It is important to note that such reporting refers not only to establishment and progress but also to the associated risks, linking such risks to the project's risk assessment.

Similarly, the proposals to expand the scope of Article 16(2) have been analysed, together with the changes recommended above, and it has been considered that the granularity of the requirements included is sufficiently comprehensive and clear.

Please refer to responses to Q17 with regards to the provisions on CCPs and TVs.

The ESAs have included additional elements in the Recitals in order clarify some of the provisions related to this section.

This proposal regarding former Article 16(9) (under 16(8) in the final text) have been considered and the text amended to include, “where feasible”.

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

The SGs agree that it is appropriate to have provisions relating to CCPs and CSDs that involve appropriate users in testing, given the centrality of CCPs and CSDs to the functioning and stability of markets.

However, the SGs are surprised not to see analogous provisions for at least the most significant trading venues. Trading venues also play a key role in enabling the market to function and in some cases are not substitutable for alternative venues. Furthermore, as ESMA has indicated in its consultation and subsequent Opinion on Market Outages there have been many challenges with outages at exchanges, and significant potential wider market impacts where, for example, closing auctions cannot take place. Some other jurisdictions have already recognized this through enhanced requirements for market infrastructures including significant trading venues, and associated supervisory oversight programs. An example is the US SEC’s Regulation Systems Compliance and Integrity (‘Reg SCI’). The SGs think this gap in the JC’s proposed requirements should be addressed. The SGs also note that the SEC is currently consulting on expanding the scope of Reg SCI to a wider range of entities and would encourage the JC to consider whether such an approach would have merit here.

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

The SGs also think that consideration should be given to similar provisions for Approved Publication Arrangements (APAs) and Approved Reporting Mechanisms, at least in relation to users.

ESAs’ response

The specific requirements in the draft RTS for CCPs and CSDs to involve their users in the testing of their ICT systems are copied from requirements already existing under Regulation (EU) 153/2013 and Regulation (EU) 2017/392 and their application has not raised any issue so far. The ESAs considered that their inclusion in the draft RTS is permitted by Recitals 101 to 103 of DORA, in particular the latter one which refers to the narrowing down of articles on operational risks included in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU 2016/1011 “with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those Regulations”. To the contrary, no such requirement currently exists under Regulation (EU) 2017/584 for trading venues nor under Regulation (EU) 2017/571 for APAs and Approved Reporting Mechanisms, therefore the ESAs considered no new requirement could be added in respect of these financial entities.

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

The SGs think it should be made explicit that the financial entity needs to take into account the impact of any incident on its customers in determining priorities and proportionality for protection of physical and environmental security, as follows:

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, the criticality of the operations or ICT systems located there and the impact of penetration or outage on customers.

ESAs' response

The ESAs consider such proposal already covered by the current draft RTS. According to Article 18(1), the physical and environmental security policy shall be designed according to the threat landscape and to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of ICT assets and information assets that can be accessed. The identification of ICT risk profiles already takes into account incidents, especially when the financial entity asses the likelihood of risk occurrence.

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

Yes, but about the requirement that programs and training shall be conducted at least yearly, it could be a too high a frequency. The SGs would ask for reconsideration.

ESAs' response

The ESAs agree with feedback from other stakeholders about the absence of a mandate for this article and decided to delete it.

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.

Yes.

ESAs' response

The ESAs welcome the feedback received.

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.

The SGs support many aspects of the criteria set out in Article 24(5). In particular, the SGs welcome the inclusion of the non-availability of systems as a trigger given the potential for this to have customer/user impacts even if at that point the financial entity has not determined the cause. We propose one clarification and one addition to the criteria. The SGs agree it is appropriate for financial entities to consider all the factors listed. However, the SGs think it is important to clarify that not all the factors need to be present in a particular situation before it is appropriate to launch the incident response processes. Any one of the factors, or combination of them, may be sufficient to warrant triggering the incident response. The SGs therefore propose redrafting as follows: 5. Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes and shall trigger a response where warranted by any one or more of the criteria: the SGs also think it is important to add a criterion relating to the notification to the financial entity by a relevant public authority of an ongoing incident which could affect it, which may or may not be specific to the financial sector. An example could include a widespread distributed denial of service attack, or a concerted exploitation of a known vulnerability in widely-used software. The SGs have not attempted to draft this because the wording will need to mesh with other legislation and means for referring to such relevant public authorities, but the SGs consider it important that on receipt of such an alert a financial entity would at least consider triggering its incident response.

ESAs' response

Regarding the simultaneity of triggers, the ESAs have considered that the current formulation is sufficiently clear, but additional clarity on how to interpret these triggers has been introduced in the recitals. This clarification mainly underlines that not all elements need to be present simultaneously and that the list is not limited to them, but that these triggers should, at a minimum, be considered by the financial institution.

Regarding the possibility of adding an additional trigger for "notification by the authorities", it has not been considered necessary to include it in the final text.

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

The SGs generally support the provisions, subject to three important additional comments below. The SGs particularly welcome the explicit reference to locating the ICT business continuity management clearly within the overall business continuity management in Art 25(1)(a) so that the focus on ICT continuity management is given due prominence but not to the exclusion of other elements. The SGs

also welcome the emphasis on testing of recovery plans in Articles 25(h), 26 and 27 as this is essential to ensuring that they are realistic and achievable when the need arises. The SGs think that explicit provision should be made in Article 25 for the business continuity policy to require consideration of ways to limit the harm to customers, users, market integrity and financial stability. It is important that where options are available about the response these factors inform decision-making and not solely matters such as cost or convenience for the financial entity. The SGs suggest doing this through a new provision as follows:

(xx) criteria to guide decision-making during incident response and recovery, including reducing the impact on the financial entity's customers and users.

The SGs think that consideration should be given to further specifying how appropriate recovery time and recovery point objectives should be determined for systems needed to provide customer access to current accounts (credit institutions) and payment accounts (PSPs) to retail clients. Given the widespread decline in the use of cash and increased reliance on electronic payments, without access to such accounts, customers may be unable to meet basic needs where such facilities are unavailable, particularly where the system outage is not pre-planned and pre-announced. Ideally, the recovery timeline would be within the same day. However, if this is not considered feasible at this stage, the SGs consider that next-day recovery is essential and should be feasible. The SGs also suggest that this is an important area for future supervisory focus and benchmarking.

Finally, the SGs think it is important that ICT business continuity management takes account of how climate change may impact both the physical threats to digital operational resilience and potential recovery scenarios. The SGs therefore suggest that a reference is added to considering any relevant national climate risk assessment or strategy when identifying potential threats to digital operational resilience and planning responses.

ESAs' response

With regard to the inclusion of elements related to reducing the impact on customers and users of the financial entity and specific considerations for current accounts (credit institutions) and payment accounts (PSPs), the ESAs considered that the current content of the provisions is sufficiently comprehensive to cover the elements identified. While within the basic principles on which this Regulation has been formulated, elements linked to specific services or technologies have been omitted.

Finally, the ESAs consider that it is relevant to include Climate Change considerations and have introduced this proposal in the text.

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

The SGs agree that specific provisions are appropriate for these entities given the role they play in the wider market.

However, the SGs also think Articles 25 and 26 should specifically reference the need for trading venues to prioritize ensuring that opening and closing auctions or other mechanism for determining opening or closing prices can operate, and that explicit provision is made for back-up arrangements to enable this to happen and for regular testing of fail-over procedures needed to maintain trading, including with the venue's users.

ESAs' response

The ESAs take note of the SGs' comment in relation to the provisions on CCPs and CSDs. As explained in our response to the SGs' comments on questions 16 and 17 above, these provisions replicate existing requirements under Regulation (EU) 153/2013, for CCP, and Regulation (EU) 2017/392, for CSDs.

As such requirements such as those proposed by the SGs do not currently exist under the regulatory framework applicable to trading venues, the ESAs considered it was not possible to include them in the draft RTS.

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.

It is important that the report and review demonstrably take account of lessons learned from previous incidents. This learning should consider both root cause analysis and also lessons learned on how the impact of incidents on the entity, its customers and markets could be reduced. The SGs therefore propose adding a new point to Article 28(2)(l) as follows: "v. lessons learned from incidents since the last review, including root cause analysis and analysis of how the impact of the incident on customers and markets could be reduced."

ESAs' response

The ESAs have carefully considered the inclusion of this element, but it has been finally discarded, as this element is sufficiently covered in several current provisions included in the text, in particular in points (2)(c)(f)(g)(h)(k). In addition, comments received from other stakeholders, which advised a reduction in the number of elements to be included in this report, have also been taken into account.

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.

Yes, broadly speaking the SGs agree. However, the SGs think the JC should incorporate suitably tailored versions of our comments in relation to the 'non-simplified' regime here. In particular, the SGs think it is important that there should be a ceiling placed on the permitted time for recovery of systems critical to the provision of current accounts or payment accounts. This would ideally be the same as that provided under Article 25. However, if this is not considered to be feasible at present, a transitional period could apply during which a longer, specified recovery time would be acceptable. The SGs also

cannot envisage what circumstances the “where applicable” in Art 39(1) is intended to capture and propose that this should be deleted. It would also be helpful to clarify the extent to which the simplified ICT risk management framework is applicable to small entities that are part of a larger group.

ESAs’ response

With regard to the inclusion of specific provisions in the recovery time of systems linked to current and payment accounts, please refer to the reply to Q24. The arguments raised there are also relevant in the simplified version.

The wording where applicable has been substituted with where appropriate that refers to the possibility of financial entities not developing or maintain ICT systems.

The applicability of the simplified ICT risk management framework is already specified in Article 16(1) of Regulation (EU) 2022/2554.

Feedback on the public consultation

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
General comments		
Delaying the application of the requirements	A number of respondents from all categories of entities asked for an extension of the implementation deadline to take into account the effort from the financial entities to define and implement their ICT risk management framework in compliance with DORA.	While it is essential to weigh these factors, the DRAFT RTS shall legally comply with the date of application of DORA.
Flexibility on policy documents used to cover RTS requirements	Several respondents suggested that it must be clarified whether a separate DORA policy/document is required, or if existing policies and frameworks can accommodate the requirements advocating for more optionality on how financial institutions should organize their policies and procedures to avoid unnecessary administrative overhead. Also, one responded noted that not all requirements pertain to policies asking if these can be defined at levels below the policy where control objectives are established.	The concern is now addressed by Recital (2) acknowledging the different operational structures and risk management frameworks of financial entities and allows them flexibility in implementing the required policies and procedures. The same recital clarifies that financial entities can align their existing documentation with the requirements of this regulation. The ESAs reviewed all policies and can confirm that the regulation mandates the inclusion of specific elements in policies only for certain critical aspects, considering industry practices and standards. Additionally, in highly technical domains like capacity and performance management, vulnerability and patch management, data and system security, and logging, financial entities are expected to develop, document, and implement procedures addressing specific technical implementation aspects.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Proportionality **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.**		
Proportionality should go both ways	A number of respondents highlighted that Article 29, as it was drafted, only took into account "increased complexity and risks" therefore only allowing to go beyond the requirements provided in the draft RTS. They considered the draft RTS should also allow to take into account elements of reduced complexity or risks.	The ESAs agree proportionality should allow to either strengthen or soften the requirements established in the draft RTS, and have modified the article on proportionality as suggested, to cover both "elements of increased and reduced complexity and risks" (see Article 1 of the draft RTS).
More elements to consider when applying proportionality	Several proposals were made to modify Article 29 of the draft RTS: - Include explicit reference to the proportionality principle in Article 4 of DORA. - Include explicit references to the elements mentioned in the mandate in Article 15 of DORA, in particular to the size and to the risk profile of the financial entity.	The ESAs note that proportionality has already been embedded in DORA and in the draft RTS in several ways: - Article 4 of DORA 'Proportionality principle'; - Exemptions for microenterprises from various requirements of Chapter II on ICT risk management; - Article 16 of DORA 'Simplified ICT risk management framework' for a number of financial entities identified as smaller than the others. - The draft RTS contains provisions addressed to specific entities that present specific profiles of ICT risks (CCPs, CSDs, trading venues)

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		- Article 1 of the draft RTS provides for considerations on elements of complexity and increased or reduced overall risk profile in the application of the draft RTS. I These suggestions were therefore rejected.
More sectoral approach	Various respondents requested the ESAs to adopt a more sectoral approach in the draft RTS on proportionality for the following financial entities, based on size or risk/business profile: • appropriate calibration rules consistent with each entity's risk profile, possibly with thresholds per type of entity; e.g., for insurance, based on Solvency II. • IORPs, due to their social purpose and to their specific set up as they outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers, as recognised under Recital 32 of DORA. • Insurance undertakings: Solvency II which is the core regulation of insurance sector contains specific provisions for small and low-risk undertakings, this draft RTS should have a similar approach due to lack of systemic risk.	These categories of financial entities cover a very wide range of entities with different sizes, types and complexity of services and operations and by consequence with different risk profiles. Therefore, it appears irrelevant to refer to categories as such, and the ESAs are of the view that it makes more sense at this stage to address proportionality in three ways in the draft RTS: (a) Article 1 on considerations of overall risk and complexity, (b) limiting some requirements to only critical or important functions or only where relevant, available or appropriate, and (c) adopting a principle-based approach when defining the requirements. On the introduction of specific thresholds, given the variety of entities covered by the draft RTS, the ESAs consider it makes more sense to have a principle-based approach, as highlighted above. On the risk of unlevel-playing field, the ESAs and the competent authorities fully acknowledge this, and will be assessing at a later stage whether supervisory

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	• Investment funds, pension funds. • CRAs: approach should take into account different categories of CRAs. • APAs. Some respondents fear that letting all decisions to be made in this respect to competent authorities would introduce important discrepancies between Member States and introduce unlevel-playing field.	convergence measures are necessary to harmonise the implementation of these requirements.
More proportionality at requirement level	Some respondents argued that proportionality should be introduced at the level of each requirement, in addition or in alternative to the general provisions of Article 29 of the draft RTS.	The general approach taken to develop this draft RTS was to have principle-based requirements as much as possible. The provisions of the initial draft RTS have been reviewed and have been streamlined further, considering the overall risk profile, size, scale, and complexity of financial entities. These are flagged below in the different items.
RTS requirements are too detailed and therefore too prescriptive	A few members claimed that the draft RTS did not incorporate the proportionality principle sufficiently also due to its prescriptiveness: the draft RTS requirements are very detailed and prescriptive, leaving no room to financial entities to adapt them, to assess whether all elements of the framework should be implemented in their situation and according to their business model.	On this the ESAs would like to reiterate that the provisions of the draft RTS incorporated in the consultation paper have been reviewed and some have been streamlined further, as appropriate. These are flagged below in the different items. In addition, the ESAs would like to note that more detailed and more granular requirements, are also linked to the specific mandate, which requests "further elements" on topics such as encryption and network security. It is also important to provide sufficient clarity to the industry. At the same time, the ESAs took due care

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		to include provisions are mandated does not mean they cannot be adapted, based on an assessment agreed with their competent authorities.
Financial entities to provide their proportionality assessment	In relation to the application of the proportionality principle, introduce a requirement for financial entities to have their proportionality analysis approved by the management body and to provide it to their competent authorities (cf. paragraph 6 of the Circular CSSF 22/806).	The ESAs consider there is no need to impose such requirement at this stage, as there is a risk competent authorities would receive too many documents. Authorities will be able to request such proportionality assessment as necessary.
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.		
Explicit reference to application of proportionality	Many respondents argue that the concept of proportionality also applies to for entities subject to DORA Article 16(1). Therefore, in line with Article 29 of the draft RTS, there should be a new Article 44 detailing the applicability of the proportionality principle to these entities.	The proportionality principle is embedded in DORA and applies throughout DORA. The ESAs agree the general provisions in former Article 29 of the draft RTS should therefore also apply to the entities subject to the simplified ICT risk management framework regime. The ESAs thus replaced the former Article 29 with a new Article 1 applying to both the general and the simplified regimes, and added Recital (1) to further explain the concept of proportionality in DORA and its general application throughout DORA.
RTS requirements should be less prescriptive, and more principle based	A number of respondents perceive the drafting of draft RTS on Article DORA as (too) prescriptive while they favour a more risk-based approach, especially because existing legislation, such as Solvency II, is risk-based.	The concept of a risk-based approach to applying rules & regulations is in this aspect similar to the concept of proportionality as it considers the appropriateness of certain requirements based on a range of elements among which is the concept of risk. In the view of the ESAs the perceived prescriptive requirements in the draft RTS can therefore be applied in a proportionate, e.g., risk-based, manner. In addition, the nature of the mandate is requesting the identification of further elements in

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		aspects such as network security, encryption etc, which inevitably lead to the identification of more detailed aspects.
More entities should be in scope	Several respondents argued the scope of entities subject to DORA Article 16 and therefore the simplified ICT Risk Management Framework, should be enlarged to more entities arguing that these requirements are more appropriate for those added entities than the general DORA requirements.	The scope of entities subject to DORA and therefore to DORA Article 16 is determined in DORA. An RTS cannot alter this scope.
Overlap with existing regulations and standards	A few respondents urge the ESAs to make better use of existing rules & standards in order to reduce the complexity for entities to comply with DORA regulations.	The draft RT Shas been developed with the intention of leveraging and depending on existing rules and standards whenever feasible. However, it is important to note that DORA is designing a consistent framework across financial entities as regards digital operational resilience, deliberately replacing certain existing sectoral rules.'s regulations will naturally differ from individual regulations that intersect with DORA. Because DORA is considered 'Lex specialis' its requirements take precedence over those of a more general nature, thereby preventing conflicting requirements from being applied.
Provisions on governance **Q3. Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.**		
Governance aspects out of mandate	Several responses proposed to remove it entirely as considered out of the scope. Respondents considered it falls outside the scope of the ESAs' mandate. They pointed out that Article 15 of DORA does not grant the ESAs the authority to specify requirements related to Article 6(4) of DORA, which is the focus of Article 2 in the draft RTS. They suggested that	The ESAs consider that governance is a fundamental aspect of any ICT risk management framework, and that this is an element where introducing certain provisions could provide greater clarity in the process of implementing the

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Article 15 of DORA is more concerned with ICT security policies and tools, rather than specifying tasks and responsibilities for functions.	requirements, and for these reasons the inclusion of governance requirements in former Article 2 was considered. At the same time, in view of the feedback received and in line with the scope of the mandate set out in DORA, the former Article 2 has been deleted in its entirety. The ESAs will assess the relevance of providing additional guidance on this issue in the future. All other proposals for specific modifications to this article have not been considered as they have no further purpose after the deletion of this article.
Clarity and consistency in the terminology and definitions	Several respondents raised concerns about inconsistent usage of definitions in the document and suggested adhering to the wording used in DORA and other documents (e.g., EBA Guidelines) to prevent confusion. Several responses shared that there were confusion surrounding different types of policies, such as "ICT policies", "ICT security policies" and "ICT risk management policies" in Chapter 1 and how they fit in the overall Risk Management Framework. Similarly, a number of respondents proposed to modify some of the terms used in former Article 1 of the draft RTS, such as "prompt data transmission", "authenticity", etc.	The ESAs considered that most terms used are sufficiently clear and that they are in line with the objectives set out in DORA. Terms such as "guarantee", "prompt data transmission" or "authenticity" are directly extracted from the DORA Level 1 text and therefore their inclusion in this draft RTS seeks an alignment with them to facilitate their understanding and implementation. Also, the ESAs are of the opinion that point (j) of Article 2(2) of the draft RTS (former Article 1(2)(j)) effectively complements the requirements included in Article 6(5) of DORA and point (k) provide additional guidance on the areas in which material changes should be considered and analysed. The ESAs have duly considered the other wording used in DORA and aligned with it wherever possible, and it is also important to note that other standards and

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	- One example was the use of the word "guarantee" since some respondents considered that it might not be possible to "guarantee" these requirements in all situations. - One respondent suggested to replace "are aligned to" with "implement" in Article 1(2)(b), considering that the strategy shall be implemented in the policies. - One respondent raised the question of deleting "indication of" in Article 1(2)(b) as be considered unclear. - 4 respondents requested more clarity on the term "material" in Article 1.2(j) or suggested modifications.	regulatory frameworks have been taken into account in the development of this draft RTS. Where possible, in view of the feedback received, other changes have been made to the text to achieve greater clarity in the interpretation of it, keeping unchanged those points where there was not a representative number of respondents seeking for greater clarity. For example, the reference to "ICT policies" has been modified in Article 2 (former Article 1), aligning it with the rest of the articles where the reference is to "ICT security policies". The reference to "ICT risk management policies" is intentional and remains unchanged. Also, further clarity has been provided in the provision on the date of approval of the ICT security policies by the management body by modifying the previous text and now including a direct reference to the date of formal approval. Another modification was included in Article 1.2(i) replacing "their" with "the ICT Security policies" in order to provide more clarity and readability to the text. Additional elements have also been introduced in the recitals, providing more clarity on some of the key provisions of this chapter, with emphasis on elements such as the fit of ICT security policies in the ICT risk management framework, alignment with the digital operational resilience strategy, etc.
Scope of exceptions	A few respondents expressed concerns about the lack of clarity on the type of exceptions in Article 1.2(c) and the process around them, in particular if this article refers to the exceptions from the requirements to	The ESAs consider that more clarity should be provided on what exceptions are referred to in Article 2(2)(c) (former Article 1). The text has been amended to clarify

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	the policies in Article 1 or exceptions from the policy discovered as part of the control measures. One respondent also expressed that risk acceptance should be also covered. The was also a proposal for adding alternative controls in case of exceptions. One response also expressed concern about the feasibility of recording all the exceptions and the possibility of including some criteria to discriminate them.	that the reference should be made to the exceptions from the implementation of these ICT security policies. Regarding the feasibility of recording the exception, ESAs consider that exceptions in the implementation of ICT policies are of utmost importance, and their recording is crucial for any future action. It is also emphasized that exceptions should not be the norm, and therefore, their number should be minimized. Consequently, it has been decided to retain this point. Finally, it is considered that control measures must be sufficient to monitor the implementation, and these controls should be appropriate, with the financial entity being the one to decide on their expansion if deemed necessary.
Responsibilities of staff	Article 1.2(d): One response indicates that "set out the responsibilities of staff" may not be suitable at group level and would perhaps be more appropriate at local level.	It is considered that one of the main elements aimed at a correct implementation of the requirements introduced in this article and in the draft RTS in general is a correct identification of the responsibilities of staff at each of the levels established in the financial institution where the ICT security policies apply. The reference to the "set out" of responsibilities is fundamental and it is therefore proposed to keep the provision unchanged.
Non compliance	There was a proposal to delete Article 1.2(e) supported by 5 responses. The proposals have two fundamental elements: - Regarding staff responsibilities, this reference does not fit in an ICT security policy given that there is usually the possibility for an employer to apply sanctions in the event of serious and proven misconduct in other policies withing the Financial Entity.	The ESAs agree with the concerns about this requirement. Considering the feedback received, it is proposed to clarify that the consequences of non-compliance need to be included in ICT security policies in case that such provisions on the consequence of non-compliance with policies of the financial entity are not included in other policies of the financial entity.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	- Regarding ICT third-party service it was emphasised that this requirement would introduce a significant compliance burden on each financial entity's security policies and procedures, which could be disproportionate and operationally unfeasible to implement. Also, that this requirement may be better addressed in contracts or vendor management policies rather than in the security policy, and it may be justified to transfer this provision to another RTS.	Furthermore, references to the TPP are deleted, as it is considered that it should be covered by other mandates and at contractual level.
Reference to standards	Some respondents suggested to add "national" or "industry standards" to the requirement included under Article 1(2)(h).	The ESAs consider that the term "leading practices" allows for sufficient flexibility. At the same time, to avoid confusions in the interpretation of "standards", the ESAs have modified the text and included a reference of the term 'standard' as defined in Article 2(1) of Regulation (EU) No 1025/2012.
Proportionality	Some respondents suggested the possibility of adopting a more proportional approach for the requirements under this section.	Proportionality considerations at provision level have already been already included and reflected, as appropriate. The general article on the overall risk profile and complexity consideration (Article 1) also serves to this effect.
ICT risk management **Q4. Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.**		
ICT security policy VS ICT risk management policy VS	A respondent inquired if the ICT security policy is equivalent to the ICT risk management policy and if they can be referenced interchangeably. Additionally, they sought clarification on the specific elements to be included under the ICT risk management framework beyond the ICT risk	The ICT risk management policy is outlined in Article 3 3, which distinctly focuses on ICT risk management. Conversely, the ICT security policy encompasses the broader criteria referenced in the other sections of the draft RTS.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
ICT risk management framework	management policy. In the same context, a few pointed out inconsistencies in risk management activities between the draft RTS and DORA. They noted confusion due to varying documented actions in both DORA and the draft RTS, questioning the exact requirements for financial entities.	Regarding the specifics of what is to be included under the ICT risk management framework, those should be identified by a comprehensive reading of DORA and the related draft RTS.
Harmonization and consistency	Some respondents emphasize the need for the draft RTS to harmonize with existing industry standards, reference internationally recognized frameworks, and align with established practices. This approach aims to reduce compliance burdens, foster collaboration and harmonisation across jurisdictions, and provide practical guidance for effective ICT risk management, especially benefiting smaller entities. One respondent recommends a more precise lexicon to better serve the cybersecurity professionals who will be implementing these standards. The same respondent expected to see a minimum set of provisions to be incorporated in the draft RTS.	The ESAs have given diligent consideration to harmonizing the draft RTS with existing EU and international ICT risk management standards to the extent possible, adhering to DORA principles without mandating a specific international standard. The alignment of the terminology used in this draft RTS is based on the terminology stipulated in Level 1, as opposed to directly mirroring any standards. While the ESAs have endeavoured to incorporate standard terminology where applicable, the primary alignment remains with the principles laid out in Level 1, ensuring adherence to DORA's foundational guidelines. Regarding the minimum provisions to be incorporated in the draft RTS, the ESAs note that a considerable number of the suggested aspects are already included in the text. However, some elements fall outside the mandated scope, hence their exclusion.
Proportionality and granularity	Multiple respondents called for the principle of proportionality in ICT risk management policies, underscoring the need for tailored requirements based on a financial entity's size, sector, and systemic risk.	Proportionality considerations at provision level have already been reflected as appropriate. The general article on the overall risk profile and complexity consideration (Article 1) also serves to this effect. The ESAs consider the article on ICT risk management flexible enough and based on general principles.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Specific wording was proposed to relax and make more proportionate the requirements foreseen in Article 3 3. Multiple respondents highlighted concerns about the draft RTS's rigid nature and the heightened costs for smaller entities urging a focus on existing standards to reduce compliance expenses. One respondent expressed concerns about additional costs for entities that already aligned spent money to specific standards. Some respondents recommended prioritizing asset mapping and evaluations on assets crucial to important functions, advocating for a risk-based approach centred on asset criticality and classification. They suggested limiting requirements to significant changes and essential assets to prevent overly complex processes.	Regarding concerns about high costs for smaller entities, these should be addressed by following the proportionality principle. On the additional costs for firms using current standards, the risk management framework is designed to be abstract yet aligned with DORA. The draft RTS offers flexibility for entities to stick to their existing models ensuring compliance across different risk management frameworks based on different international standards. Focusing only on the risk management of ICT systems supporting critical or important functions could leave ICT systems not supporting critical or important functions exposed, potentially affecting the one supporting critical or important functions due to their interconnectedness. This broad risk management approach aligns with regulatory principles like DORA, emphasizing holistic digital operational resilience.
Financial entities outsourcing operations	Respondents emphasized the challenges of implementing ICT risk management policies for financial entities that outsource operations and lack in-house ICT resources. They advocate for managing risks with crucial third parties via contracts. A query was raised about whether specific policies and procedures are required for outsourced activities beyond the general ICT risk management framework and policy.	DORA already include provisions that address ICT services carried out by third-party providers, including the necessary policies related to them. Therefore, financial entities are already mandated to manage and oversee the risks associated with outsourcing their operations to third parties, maintaining an established ICT risk management framework and policy, which can encompass specific areas even when activities are outsourced. This assures that the concerns raised regarding outsourced operations and collaborations with critical third parties through contractual agreements are duly covered under the existing mandates.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Clarification on the content of the risk assessment method	A respondent questioned if Article 3(1)(b) to Article 3(1)(e) refers to the content of the risk assessment method or the outcome, specifically whether it's about the process to identify threats or the actual threats identified.	The ESAs believe that the requirements are sufficiently clear and refer to the documentation of those elements in the risk management policy and procedures.
Clarifications on risk tolerance level	Several respondents emphasized the necessity for greater details on how risk tolerance levels should be defined, including the granularity and parameters for determining such levels. Finally, one respondent asked a more detailed question on whether risk tolerance is the maximum level of disruption to be accepted or the deviation from risk appetite while some other respondents advocate for including both qualitative and quantitative aspects in determining the risk tolerance levels in Article 3.1(a). Some respondents requested clarification on whether the expected risk tolerance is determined specifically for each of ICT risk or for all of them together. Two respondents recommended to replace "indication of the approved risk tolerance level" with "the approved risk tolerance levels", making the provision more distinct. Another respondent indicated that Risk tolerance levels are to be defined and documented, but typically these are not set out within policy documents. One respondent suggested aligning terminology with EBA Guidelines, favouring "risk appetite" over "risk tolerance," while another sought clarity on the omission of a risk appetite statement. Finally, one	The ESAs decided not to include details on how risk tolerance levels should be defined to grant discretion to entities in determining the specifics of defining risk tolerance levels, including the granularity and parameters involved. This approach is designed to allow for a more tailored implementation that can suit the individual circumstances and complexities of different entities. The draft RTS has now been refined to indicate that the "approved risk tolerance level for ICT risk" is to be determined singularly, not on a per-risk basis. This adjustment in phrasing to the singular form is in line with DORA Level 1 requirements and underline the expectation that a consolidated risk tolerance level should be established, guiding the holistic approach to managing various ICT risks within the boundary of the defined tolerance threshold, thereby harmonizing the risk management process. The phrase "indication of the approved risk tolerance level" in the draft RTS is focused on signalling that a process of approval has taken place, rather than delineating the specifics of the actual risk tolerance level. This distinction is key to maintaining a strategic oversight and aligns with the provisions laid out in DORA, where it is highlighted that the tolerance level details are to be positioned within the broader ICT risk management strategy, not in the policy document. The

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	respondent suggested to replace "risk tolerance" with "target risk tolerance" to encourage continuous improvement.	provision is now amended to make the requirement clearer by referring to the approval of the risk tolerance level for ICT risk. The term "risk tolerance" is used in the present mandate according to Article 6(8), point (b) of DORA, thereby retaining this term ensures compliance and alignment with the existing regulatory framework. Also, the term used broadly in international standards and frameworks, therefore, using this term can potentially align more closely with globally recognized terminology, aiding in international comprehension and collaboration. Keeping "risk tolerance" in this context ensure a more detailed, focused, and regulated approach to risk management.
Clarification on the measuring of the likelihood and impact of vulnerabilities and threats	Article 3.1(b): According to some respondents the articulation around measuring the likelihood and impact of vulnerabilities and threats needs refinement. One respondent recommended specifying that both quantitative and qualitative indicators should only be used "if possible" to measure these vulnerabilities and threats. A respondent observed inconsistent use of the terms "process" and "procedure" in the CP and draft RTS documents, questioning if they mean the same thing. They recommend defining these terms for clarity. One respondent noted that vulnerabilities have likelihood of 100% and the text should be amended considering this.	The ESAs decided not to include details on how measuring the likelihood and impact of vulnerabilities and threats to grant discretion to entities regarding the quantitative or qualitative indicators to be used. This approach is designed to allow for a more tailored implementation that can suit the individual circumstances and complexities of different entities. Also, the ESAs disagree with the statement on the qualitative and quantitative indicators that are not always possible to be established. Measuring the impact and likelihood of vulnerabilities and threats without quantitative and qualitative indicators is generally not advised as it would lack objective metrics and could lead to imprecise risk assessments. Also, the industry standard and best practice precrime the use of quantitative and qualitative indicators to support a structured, consistent, and evidence-based approach to risk assessment. The ESAs also clarifies that the terms process and procedure have not the same definition. In this context there was an oversight in the consultation paper and the

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		term procedure is the correct one. The mistake regarding the terms process and procedures is now rectified in the final report. The ESAs take onboard the comment on vulnerabilities likelihood being 100% and amended the provision.
Risk treatment measures VS risk mitigation measure	Article 3.1(c): Some respondents express the need for clarity regarding the term "risk treatment measures". They recommend using the term "risk mitigation measures" or another terminology that aligns with standard industry language for improved readability and coherence.	The term "risk treatment measures" is maintained in the draft RTS as it is a comprehensive terminology that encompasses a broader range of actions including, but not limited to, risk mitigation. This phrase is aligned with established international standards which advocate for the usage of "risk treatment" to refer to the process of selecting and implementing measures to modify risk. This term not only involves mitigating risks but also accepts, avoids, or transfers them, thereby offering a more versatile approach to risk management. The usage of this term ensures consistency with international standards terminology and best practices and accommodates a multi-faceted approach to risk management, which is essential in addressing the varied and complex risk land-scape financial entities operate in. Risk treatment measures will not be changed into risk mitigation measures in Article 3(1)(c).
Clarification on residual ICT risk integrate into the overall risk management process.	Article 3(1)(d)(i): One respondent requested clarification on the request for residual ICT risk to be integrated into the overall risk management process and whether this means that the residual risk need to be accepted following the right governance procedure.	The requirement implies that once the primary risk treatment measures are implemented, there may still be some remaining or 'residual' risks. While the provision is amended by deleting the last sentence to better reflect the mandate of the draft RTS, it is still important to consider that these residual risks need to be assessed and managed as part of the entity's broader risk management process.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Responsibility for accepting residual risks.	Some respondents express a need for clarification on who is responsible for accepting residual risks in Article 3(1)(d)(ii). Some of them suggested also that the responsible for this should be the Administrative Management and Supervisory Bodies (AMSB) in the decision process.	In line with the considerations expressed on the deletion of Article 2 on governance of the consulted draft RTS, the ESAs cannot specify the responsible function for accepting residual risk.
Development of an inventory: limitation of scope	Article 3(1)(d)(iii): Two respondents proposed that in accordance with the principle of proportionality, the development of an inventory of the accepted residual ICT risk should be performed only on critical or essential processes when the risk tolerance levels for ICT risk are exceeded. One respondent asked for clarification on whether the "explanation of the reasons" is required for all ICT risks, or only the one over the risk appetite (medium-high, high risks). Another respondent asked for clarification regarding what is acceptable with regards to legacy systems as a potential major systemic risk. Two respondents suggested that the term "accepted ICT risks" (plural) should be used in-stead of "the accepted ICT risk". The latter suggests an aggregated quantification of the individual risks.	Implementing the strategy of documenting accepted residual ICT risk only for critical or essential processes when the risk tolerance levels are exceeded may overlook potential vulnerabilities and threats that can emerge from ICT systems not supporting critical or important functions. It is essential to maintain a holistic approach to risk management, which encompasses both ICT systems supporting critical or important functions and ICT systems not supporting critical or important functions to ensure comprehensive security and resilience. Moreover, ICT systems not supporting critical or important functions can still have substantial interdependencies with ICT systems supporting critical or important functions, and vulnerabilities in the ICT systems not supporting critical or important functions can potentially be exploited to affect ICT systems supporting critical or important functions. Therefore, maintaining an inventory of all accepted residual ICT risks, regardless of the criticality of the processes involved, would provide a more robust defence against potential ICT disruptions and foster a stronger ICT risk management framework. As clearly stated in the article, the explanation of the reasons for which the accepted residual ICT risks were accepted is for all accepted residual ICT risks. Moreover, the draft RTS does not make a distinction regarding what is acceptable with regards to

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		legacy systems. Therefore, accepted risks are those that remain within the tolerance level. The ESAs agree with suggestion to use the plural form of "accepted ICT risks" and amended the article accordingly.
Assessment of accepted residual ICT risk	Article 3(1)(d)(iv): Some respondents suggested that the draft RTS should focus on identifying "significant" or "relevant" changes to residual ICT risk rather than "any" changes. This emphasis aims to prevent undue burdens and prioritize changes that have a substantial impact on the risk profile. Additionally, there were questions about whether all accepted risks need review or just those deemed critical or with special attributes. A respondent recommended a triennial review instead of an annual one for SMEs with limited risk profiles to alleviate resource constraints. Two respondents suggested adding "monitoring that the aggregation of accepted risks is within the risk appetite of the financial entity".	The proposal to replace "any" with "significant" or "relevant" is declined, as it's imperative to identify all changes initially. The determination of a change's significance or relevance can only be made following its identification and subsequent assessment. Regarding the annual review being too burdensome for SMEs, the ESAs note that DORA foresees the annual review of the whole management process; therefore, this cannot be changed at RTS level. The proposal to add "monitoring that the aggregation of accepted risks is within the risk appetite of the financial entity" is declined since additional monitoring could introduce unnecessary administrative overhead without proportional value. The lack of this requirement does not preclude financial entities to monitor this aspect.
	Article 3(1)(e): Some respondents requested amending the draft RTS to emphasize the monitoring of "significant" or "relevant" changes in the ICT landscape instead of "any" changes, to avoid unnecessary burdens and to maintain a focus on changes that materially affect the risk profile. Some respondents suggested replacing the word "promptly" with "appropriate" for better interpretation.	The proposal to replace "any" with "significant" or "relevant" is declined, as continuous monitoring of all changes is essential to discern their potential effect on the ICT risk profile. Moreover, cumulative minor changes can collectively result in a substantial impact on the ICT risk profile. The word "overall" referring to ICT risk profile is now deleted to align to DORA terminology. The proposal to replace the word "promptly" with "appropriate" for better interpretation is declined. Given the rapid evolution of the ICT landscape and the

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	One respondent asked for clarification on how financial entities determine what amounts to "significant changes" to the ICT landscape and advocate for providing guidelines on initiating reviews in light of these changes. Respondents find the annual review framework challenging for SMEs and recommend a triennial review for limited risk profiles. They seek more flexibility and alignment with existing standards. Given that strategies typically span three years, they suggest that review cycles should match a firm's strategy duration, emphasizing alignment with risk tolerance levels. One respondent noted that changes in the ICT risk profile may likewise impact the digital operational resilience strategy: the relationship is two directional.	potential for immediate threats, it's crucial to promptly detect changes to ensure timely mitigation and maintain a secure environment. The ESAs will not define significant changes to the ICT landscape to grant discretion to entities regarding the quantitative or qualitative indicators to be used. This approach is designed to allow for a more tailored implementation that can suit the individual circumstances and complexities of different entities. Regarding the annual review being too burdensome for SMEs, The ESAs note that DORA foresees the annual review of the whole management process; therefore, this cannot be changed at the RTS level. The verification process under point (e) is now moved into the new point (f) that now provides for a general process. The word 'year' has been removed to avoid overlap with DORA. Regarding the fact that the changes in the ICT risk profile may likewise impact the digital operational resilience strategy, the ESAs agree with this statement, however, it is crucial to note that there is no mandate to further specify elements of the digital operational resilience strategy.
More flexible approach to update of ICT risk management policies and procedures	Some respondents propose to amend Article 3(3) providing a flexible approach to updating policies and suggested adding "as needed" to Article 3(3) to allow financial institutions the discretion to decide when a change necessitates a policy update.	This provision is now deleted since it was replicating point (e) and new point (f).
ICT asset management **Q5. Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.**		

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Definition of ICT asset	A group of respondents noted a too broad definition of ICT asset when it comes to the provisions of Article 8 on ICT operating policies and procedures and Article 9 on capacity and performance management. In their eyes, it is important for a financial entity to take a proportionate approach to the mapping of ICT assets. Taken literally, DORA and the draft RTS could imply the mapping of every ICT asset, including, for instance, computer headsets, computer mice and keyboards, etc., which are immaterial to the functioning of the financial entity or its ICT risk.	The definition of ICT Asset is in DORA Level 1 and can therefore not be changed by the draft RTS.
Definition of Business Function	Several respondents requested a definition of 'business function' as used in Article 26(2)(c).	As the term 'business function' is used in DORA Level 1, the ESAs do not see the need to define the term.
Clarification of other certain terms used in the RTS	Few respondents asked for more clarity of the relationship between BIA for BCM and criticality assessment, the definition of 'portable endpoint', 'authenticity' and the term 'exposed' in Article 4(2)(b)(viii).	The mentioned terminologies and concepts align with EU and international leading practices and standards. Some are further detailed or mentioned in DORA or within the pertinent sections of the draft RTS itself. Thus, no amendments have been made in the text.
Unique ICT asset identifier	One respondent stated that the requirement to have a unique identifier for each ICT asset would create a significant administrative burden.	The ESAs have considered the feedback received on this and while it is acknowledged that setting a unique identifier for each ICT asset can be burdensome for financial entities with a large number of ICT assets, it is however necessary to meet the objectives of ICT asset management in this draft RTS and in line with the scope defined in DORA for asset identification.
ITC risk assessment on legacy systems	One respondent indicates that ICT risk assessment on legacy system would be costly and add no value from a risk management perspective.	The ESAs would like to highlight that legacy systems may pose an important ICT security risk on the network and information systems environment of the FE, which

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		is also highlighted in DORA. It is thus important to include them in the ICT risk management.
Guidance on risk assessment methodology	One respondent asks for clarity on how organizations should implement the risk assessment referenced under Article 8(1) of DORA.	The ESAs have no empowerment to specify this element further.
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?		
Importance of end date for regular and extended support	A group respondents noted that the respective end dates, i.e., for both support types, are equally relevant and serve different purposes. Several respondents noted that keeping both dates allows for monitoring of information systems, for effective ICT asset lifecycle management, and for compliance to the CIA model. For some product types in general, but in particular in relation to cloud services, some respondents indicated that the end dates were not very useful.	The ESAs agree with the relevance of the information as indicated in the respondent comments. The aim is to have a technology neutral RTS, which is why cloud-specific provisions or exceptions are avoided.
Burden of record keeping and proportionality	A group of respondents underlined that the record keeping of the end date(s) implied a significant burden for financial entities. The application of this provision should be done using a risk-based approach. Proportionality should be applied to Article 4. Several respondents indicated that the end date(s) might not be known at the moment of reporting.	Point (ix) of Article 4(2) has been added. Financial entities should record, where applicable, the mentioned end dates for all ICT assets. However, as explained in the proposed Recital (7), financial entities should focus specifically on those ICT assets or systems necessary for the business operation, considering their criticality and potential impact in case of the loss of their confidentiality, integrity and availability.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Several respondents suggested to limit the provisions to ICT assets that function that serve critical or important functions. Some respondents indicated that the implied record keeping was burdensome for entities that outsourced their entire business, such as IORPS.	
Further clarification or additional requirements	One respondent suggested to add a definition of provider support in this context. Few respondents suggested to also add further requirements including the expected End- of-Life of ICT assets, especially for Legacy Systems and to record all updates and patches and to select all ICT assets that have not been updated for 12 months.	The ESAs believes that the new point (ix) in paragraph 2 of Article 4 is sufficiently clear. The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits.
Encryption and cryptography **Q7. Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.**		
General	Some respondents raised concerns on the operational burden needed to ensure compliance with the proposed requirements and overreliance on encryption overlooking other equivalent security measures. This was complemented with suggestions to allow for more flexibility (e.g., principle-based approach or risk-based approach), less prescriptiveness and proportionality (e.g., application of proposed requirements to 'critical' financial entities such as banks).	The scope of the RTS is mandated in Article 15 of DORA and where possible, amendments were made to this draft RTS allow more flexibility while remaining within the ICT risk management requirements as prescribed in DORA. Moreover, Article 15 (a) of DORA makes explicit reference to cryptographic techniques as a safeguard to preserve the availability, authenticity, integrity and confidentiality of data.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Some respondents also argued the rules for encryption are to protect authenticity, integrity and confidentiality but not availability, hence they suggested to exclude reference to availability.	In relation to availability, encryption covers all CIA principles and indirectly availability. Cryptography supports availability by making available encrypted information to only authorised users.
Encryption of data	Some respondents proposed to explicitly limit encryption only to sensitive data or based on risk assessment and data classification. Many respondents raised concerns on Article 6(2)(a) - encryption of data in use – and the challenges to process data in a separated and protected environment. It was suggested to allow further limit encryption of data in use and to allow the use of other measures, based on a risk-based approach, where the use of separated and protected environment is not possible.	It is clarified that the text already states that rules for encryption shall take 'into account the approved data classification and ICT risk assessment processes to protect the availability, authenticity, integrity and confidentiality of data'. Therefore, the request for a risk-based approach was already included in the text. Further clarity is now provided by dividing the rules for encryption of data at rest and in transit with the one on data in use. The latter is now in new Article 6(2)(a). Encryption of data in use shall be performed based on the results of the ICT risk assessment of the financial entity. Moreover, the text has been amended to allow the use of other mitigation measures which however need to have the same level of protection as the one envisaged in a separated and protected environment.
Use of leading practices and international standards	Mixed views on the reference to 'leading practices' in Article 6(3) where some respondents suggested further specifying such practices/standards whereas others suggested to remove such wording as it may be difficult to keep monitoring such practices and also not feasible to follow them.	ESAs consider that the term "Leading Practices" allows for sufficient flexibility. At the same time, to avoid confusions in the interpretation of "standards", ESAs have modified the text and included a reference of the term standard as defined in Article (2)(1), of Regulation (EU) No 1025/2012.
Monitor developments in cryptanalysis	Article 6(4): Some respondents suggested to reconsider the explicit reference to cryptanalysis given the absence of in-house expertise and others to avoid prescribing such a specific requirement.	The requirement does not envisage the financial entities to perform cryptanalysis but to update or change the cryptographic technology on the basis of developments in that field if any (technology watch).

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Cryptographic keys	A respondent suggested to also add 'renewal' in Article 7(1). Several respondents noted it is not technically possible to recover such keys hence suggestion to restore or to replace lost keys or to recover the data in Article 7(2). Moreover, respondents suggested alternative approach on certificate lifecycle management and a risk-based approach in relation to the register for certificates and certificate storing devices (Article 7(4)).	The text has been amended by adding the renewal step to the said lifecycle. The word 'recover' in Article 7(3) has been changed with the word 'replace'. A risk-based approach has been introduced in the creation and maintenance of certificates foreseeing it for at least ICT assets supporting critical or important functions. Also, following the inclusion of the risk-based approach a further clarification has been added regarding the assurance of the prompt renewal of certificates in advance of their expiration.
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.		
General comment	The majority of respondents considered the measures and controls presented in the consultation paper sufficient and did not support any further additions. However, some respondents proposed specific additional measures and controls to be included in this regulation. Few respondents proposed to add in this regulation explanation on how encrypted information may interfere with the security controls and how existing applicable laws and requirements may restrict the use of cryptography. It was also suggested for this regulation to be updated to reflect risk assessment of risks expose to current vulnerabilities.	Given the preference expressed by the majority of the respondents, the ESAs limited the additional aspects to the ones that provide an important benefit to the area of encryption and cryptography. The purpose of this regulation is to supplement the provisions prescribed in the Regulation (EU) 2022/2554 rather to provide guidance or explanations on the implementation of legal provisions. It is also noted that should this regulation need to be revised the prescribed legislative process will be followed. Such a review could take place for example when some aspects in this draft RTS are considered obsolete.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Proposals for additional measures or controls	A respondent suggested to specify roles and responsibilities for staff involved in cryptographic key management. Another respondent suggested to expand Article 7(1) to include additional key management aspects such as key expiration, rotation, multi-factor authentication (MFA), auditing, secure software development, and security awareness training. A respondent proposed to extend Article 7(4) and a provision on the prompt renewal of certificates: "Financial entities shall develop and implement controls to ensure the prompt renewal of certificates in advance of their expiration. Another respondent noted the usage of encryption for an ICT system should be documented to ensure crypto agility in terms of being able to identify places where encryption algorithms no longer live up to Article 6 paragraph 3-4.	The ESAs do not consider the specification of roles and responsibilities within the mandate. All these aspects proposed for Article 7(1) should be considered in the whole life cycle of the cryptographic key management. The proposal for Article 7(4) is considered appropriate and relevant hence it has been integrated in the final text. The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits.
ICT operations security **Q9. Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.**		
Proportionality principle not met	Some respondents noted that the provisions on ICT operations security do not meet the proportionality principle or should be applied following a risk-based approach.	Proportionality considerations at provision level have already been reflected as appropriate. The general article on the overall risk profile and complexity consideration, Article 1, also serves to this effect.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	One respondent noted that the requirements should be simplified when a financial entity chooses to use critical third-party ICT providers and/or "market certified ICT providers.	Management of ICT third-party risk is generally addressed by DORA and the simplification required cannot be achieved through the RTS due to lack of mandate.
Interaction with or modification of DORA Level 1	Some respondents proposed modification of DORA provisions specifically on, restricting the restoring of backup data, simplified regime for financial entity choosing to use critical third-party ICT providers and/or "market certified ICT providers, removal of specific ICT third-party services providers from the list of ICT service.	DORA provisions cannot be amended or restricted by the draft RTS.
Interaction with other regulations.	One respondent noted that there should be better consistency with other legislations.	The draft RTS cannot address consistency with other Regulations that apply in any case depending on their specific scopes.
Additional clarifications on certain terms	Few respondents requested clarifications on the meaning of specific terminology or concepts used in Article 8, like risk profile, ICT systems, secure, control of legacy ICT systems, criticality of information, scheduling requirements, external support contacts, vulnerability, vulnerability scanning and its assessment, patch management, access restrictions, endpoint devices, private non-portable endpoint devices.	The mentioned terminologies and concepts align with EU and international leading practices and standards. Some are further detailed in DORA or within the pertinent sections of the draft RTS itself. No amendments in the text. The term ICT systems under Article 8(2)(a) is now changed with ICT assets while ICT assets under Article 8(2)(a)(i) is now changed to ICT system. The amendment reflects the broader scope of the term ICT assets compared to ICT system.
Segregation of environments – ICT operations	Several respondents noted that implementing and monitoring certain cloud-based systems, as mentioned in Article 8(2)(b)(v), is challenging. This article also doesn't align with modern development methods like Agile and DevOps, potentially slowing down product releases. Some cloud developments can occur directly in production; financial entities should decide the best approach.	The ESAs agree with the comments and amended the draft RTS to accommodate innovation while ensuring comprehensive digital operational resilience.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	A similar comment was raised regarding Article (10)(4)(c) on the testing and deployment of software and hardware patches and updates.	
Performance of internal audit and other testing	Some respondents requested clarifications regarding Article 8(2)(b)(iv) on controls and monitoring of ICT systems, including (iv) requirements to ensure that the performance of internal audit and other testing minimises disruptions to business operations).	The objective of the requirement is that activities by the internal audit and other testing should be performed in a way that do not have consequences for business operations.
Error handling limitation	One respondent proposed not to limit the provision to error handling (Article 8(2)(c)(iii)) and noted that the financial entity should not develop separate recovery procedures for specific causes of disruption such as errors as this would introduce unnecessary complexity and likely result in inferior capabilities.	The overall requirement prescribes that the ICT operating policies and procedures need to include an element on "Error handling concerning ICT systems" and then lists some minimum requirements that should be followed. If a financial entity identifies more measures than the listed ones, they can still implement them.
Capacity and performance management	With respect to Article 9, some respondents noted that managing capacity for low-risk applications isn't standard due to its inefficiency in risk reduction. Any capacity issues with low-risk applications should be resolved by the financial entity without material impact. The provision should be limited to ICT systems supporting critical or important functions. One respondent proposed to include measures to detect and prevent denial of service attacks.	Proactive capacity management, even for low-risk applications, can prevent larger systemic disruptions and is more cost-effective than addressing issues reactively. This is particularly valid due to the interconnectivity of modern systems. Also, addressing capacity proactively, even for low-risk applications, can be more cost-effective than reactive measures after a failure. The objective of the provision is to remain principle based without limiting the measures to threat actors. Therefore, the proposal to add further measures is disregarded.
Vulnerability Notifications ICT TPSP	On Article 10(2)(c), several participants noted that notifying financial entities of every vulnerability detected by ICT third-party service providers can lead to information overload and misallocation of	The ESAs limited the scope of the reporting for at least the critical vulnerabilities. However, for the financial entity to have a comprehensive view, the financial entity should also verity through the vulnerability management procedure that the ICT

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	resources, potentially overlooking critical vulnerabilities. Instead, third-party providers should manage and remediate vulnerabilities themselves, assuring financial entities of their actions. Focusing on the holistic effectiveness of a third-party's vulnerability management is more crucial than individual vulnerabilities, especially when disclosure might lack actionable mitigation steps or when the financial entity can't act due to the nature of the service.	third-party service provider provide at least statistics and trends on all vulnerabilities.
Tracking of third-party libraries	Some respondents noted that the obligation to monitor the usage, versions, and updates of third-party libraries, including open source, is quite burdensome for financial entities. It's suggested to modify the wording to more flexible terms, such as 'as feasible or necessary to understand the material risks associated with software components'. A distinction should be made between self-developed and third-party software. Finally, the responsibility for this should lie primarily be with the manufacturers and ICT service providers. It should not be shifted to the financial entities.	Considering the feedback received, Article 10(2)(d) has been amended to make the requirement more flexible.
Vulnerability Notifications Financial Entities	Article 10(2)(e): Several respondents noted that publicly disclosing vulnerabilities by financial entities can lead to a loss of trust in the financial sector and may spotlight weaknesses for potential hackers. Vulnerability disclosure should be at the financial entity's discretion, focusing on those requiring public action or caution. Often, contractual agreements may also prohibit such disclosures.	The provision caters already for responsible disclosure that is also used by Article 14(1) of DORA.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Risk based - patch management	Article 10(2)(f)(g): Some respondents requested to deploy patches or other mitigation measures following a risk-based approach or also based on the impact of a successful exploitation of a vulnerability on customers, users or counterparties. Other respondents advocate for a prompt deployment once the vulnerability is identified.	The article already foresees a risk-based approach in Article 10(2)(g) through a prioritisation process based on the criticality of the vulnerability, the classification and risk profile of the ICT assets affected by the identified vulnerabilities. The criticality of the vulnerability also encapsulates the potential negative impact on customers, users, or counterparties. Point (g) is now merged with point (f) for clarity.
Access restriction feasibility	One respondent claimed that it may not be feasible to set out access restrictions for all data classifications like non-sensitive data classification stored in unstructured data locations as is provided under Article 11(2).	Access restriction is defined by the financial entity on the base of its our data classification. No amendments to the text.
Logging and proportionality	Several respondents noted that the logging requirements set out under Article 12 need flexibility to accommodate varying ICT capabilities and avoid unnecessary administration through false positives. A risk-based approach and professional judgment are vital as well as a distinction between self-developed software and third-party software. Some respondents noted that small financial entities may find these mandates beyond their means, leading to potential outsourcing challenges due to limited cybersecurity service availability. According to some respondents, the logging should be limited to the buildings of the financial entity that hold critical or important processing facilities.	Article 12(2)(a) offer already flexibility since the identification of the events to be logged, the retention period, and the measures to secure and handle the log should consider the purpose for which the logs are created. The provision provides also further criteria for defining the retention period. Also, point (b) of the same article provides further criteria to limit the detail of the logs. While flexibility is essential and already provided by Article 12, consistent logging standards ensure uniform security levels across the financial industry. Allowing too much flexibility can create gaps in security monitoring. Also, whether software is self-developed or third-party the risk implied remain the same. While smaller financial entities may face initial challenges, market dynamics typically adjust to regulatory shifts. As demand for cybersecurity services grows due to regulations, more market entrants can be expected, leading to increased competition, enhanced quality, and broader accessibility, ensuring the financial

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		sector's adaptability and resilience. Also, as mentioned in the paragraph above, the article caters for flexibility regarding the logging requirements. The concern regarding the logging of physical access to be limited to critical or important facilities is already addressed by the article on Access control. A cross reference to the article has been added.
Clock synchronisation	Article 12(2)(g): Synchronisation of the clocks of all ICT systems with a single reliable reference time source is not possible with regard to the cooperation of different service providers and can only be implemented under their own responsibility.	The article has been amended to achieve the main objective to have a register of reliable reference to allow synchronisation of different log files.
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.		
Additional requirements	Few respondents required additional requirements in this section.	The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits or such requirements are covered in other sections or articles of the draft RTS.
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.		
Automation of vulnerability scanning and handling and automation	Article 10(2)(b): Some respondents noted that while regular vulnerability scans are essential, a weekly scanning frequency could indeed impose a significant workload. A general weekly frequency for vulnerability scanning or assessments is disproportionate. Frequency should follow a	The requirement already follows a risk-based approach as weekly scanning is only necessary for critical/important functions. Also, the provision does not restrict the possibility of having more frequent vulnerability scanning. No amendments required.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	risk-based approach. Other respondents noted that weekly scanning is insufficient. Some respondents noted that the RTS should consider when automated vulnerability scanning and assessment is not possible.	The scanning and assessment of the vulnerability is performed normally in an automated way. No amendments required.
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.		
Specific requirements for cloud computing resources	A large majority of the responses to this question supported the current text. In addition, in those cases where no additional measures were requested, more clarity was sought on the requirements included. A small number of responses requested to include specific aspects for cloud computing resources, in addition to those already present. A relevant number of respondents also expressed doubts on two points in particular: - the need to include technology-specific aspects, rather than remaining technology-neutral. - the overlaps in the current requirements with provisions already included in DORA and the draft RTS.	The ESAs consider that the draft 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. At the same time, the ESAs acknowledge the relevance and the specificity of cloud-based resources in the current landscape of technological solutions and the increasing dependence of the financial entities on them. In this context, and based on the received feedback, the ESAs amended the requirements previously associated with cloud resources, to ICT assets or services provided by ICT third party service providers. This works towards maintaining the technological neutrality of the draft RTS while ensuring the adaptability of provisions to future changes in the ICT assets and services landscape.
Network security **Q13. Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.**		

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Proportionality	Some respondents expressed Article 13 on network security management does not take into account the principle of proportionality for these requirements	Proportionality considerations at provision level have already been reflected as appropriate. The general article on the overall risk profile and complexity consideration, Article 1, also serves to this effect.
Further details	Some respondents have expressed a desire for clearer guidance regarding the expected level of detail referred to in Article 13.	To allow to financial entities enough flexibility on the application of the requirements and the use of lead practice. Financial entities should be able to decide on the applicability and design their own security architecture based on their unique needs and circumstances aligning it with their risk-based approach.
Segregation of environments – Network security	Article 13(1)(a): Some respondents noted that separating production from administration is complex, costly, and can lead to operational issues. Also, having a test environment identical to production, especially on network backbones, isn't realistic. Requirements should be risk-based and focused on critical systems or those with critical data. A few respondents proposed to include the Zero trust model and least privilege principle.	This is addressed by Article 13(1)(a) that takes into account the criticality or importance of the function the ICT systems and networks support, the classification and overall risk profile of ICT assets using them. The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits. Also, the intention of the regulation is not to prescribe any specific model or techniques to leave flexibility to financial entities.
Mapping and visual representation	Article 13(1)(b): A few respondents noted that depending on the architecture of the financial entities, visual representation of all network and data flows can't be always performed. Maintaining both representations could be redundant and indeed could require high cost and medium/low security values.	Article 13 (b) is now amended by referring to documentation of all of the financial entity's network connections and dataflow.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Separated and dedicated network for administration of ICT assets.	Article 13(1)(c): Some respondents requested clarification on the meaning of 'direct internet access'. Also, this requirement does not consider the different set-ups needed to securely administrate network devices, server farms, applications on a server or cloud applications.	The article is now modified mandating only for the use of a separate and dedicated network for the administration of ICT assets.
Firewall rules and connections filters review	Article 13(1)(h): the majority of the respondents noted that the frequency of 1 year would be more appropriate, and would be aligned with the frequency of Article 13(1)(i).	The ESAs believe that the review of the firewall rules and connections filters is an important control that should be performed at least every six months.
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.		
No additional measure	A majority of the respondents believes the proposed measures are sufficient and that any additional measure might create even higher costs and burden. Flexibility and proportionality would be crucial.	The ESAs agree with the feedback received.
Consideration of the information classification system	Regarding Article 14(1), for any controls related to protecting data, some respondents claimed that it is important to consider the financial entity's information classification system.	The ESAs agree with the feedback received and included the new paragraph 2 considering the classification aspect.
Data leakage prevention	Few respondents proposed to replace the word leakage in Article 14(1)(b) with the word "loss" to avoid confusion.	While we agree that data leakage may result in data loss as well, from the perspective of loss of availability of data, the scope of this provision is on prevention from unauthorized exposure of sensitive data, typically due to malicious actions and weaknesses in security controls and their implementation. In this context, we maintain the reference to data leakage prevention.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
ICT project and change management **Q15. Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.**		
ICT project management	Some respondents suggested to remove the Article 15 due to lack of correspondence with DORA requirement. Several respondents asked to specify elements in the ICT project management policy, include communication standards, and establish minimum criteria and approvals for change requests. Various respondents asked to focus tests on new ICT assets with an emphasis on non-regression testing and critical elements before deployment, considering current complex ICT frameworks. Other asked to implement a criticality assessment to selectively test requirements. Several members asked for inclusion of Agile development methodologies (or other non-linear methodologies). Some respondents asked to separate project and change management. Several respondents asked for clarification of terms: "project risk assessment", "change management requirements". Several respondents asked to have dedicated personnel in the project teams (ICT security personnel, qualified professional third parties, business staff) or clauses for training/expertise.	The ESAs stress the importance of project management in enhancing digital operational resilience, aligning with DORA's objectives and strengthening risk management practices for Financial Entities. The ESAs confirm that the draft RTS provides Financial Entities with the necessary flexibility to tailor staffing and team composition to their unique needs, with no major amendments needed to existing articles. This balance ensures a standardized, yet adaptable framework, catering to the diverse requirements of different financial entities. The ESAs agree with the suggestions to provide more clarity in some of the terms and have introduced additional elements also in the recitals. The term "key" has been changed to "relevant" with respect to milestones in Article 15(2)(e), to provide more clarity. In this respect, and considering the feedback received, it is important to note that the project management policy does not advocate for any specific project management methodology. In addition, Article 15(4) has been amended to link the requirement to the ICT project management policy and not to the financial entity itself and to clarify that an adequate flow of information and expertise from the business functions or areas impacted by ICT projects is essential for the secure implementation of such projects.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Some members asked to include "project ownership", "project performance metrics" as a new element in the ICT project management policy. Include "non-project" activities in the ICT project management. Clarification of terms: "impacting", "periodically", "depending on the size of the ICT projects"	
ICT systems acquisition, development, and maintenance	Respondents seek clarity on whether all ICT systems or only critical ones are covered by the provisions. Many recommend granting financial entities more flexibility in structuring their policies and demonstrating DORA compliance, suggesting a removal of Article 16 and less prescriptive rules. Certain respondents ask for clear definitions of "ICT project" and "all ICT systems." A respondent suggests considering "ICT systems acquisition, development, and maintenance" separately, following the EIOPA Guidelines. Various responses suggest including IT Operations in project and change management for smoother implementation. Several respondents ask to introduce ongoing monitoring for asset misconfigurations, adhering to security and operational guidelines. Various respondents ask for additional details on risk mitigation for both unintentional and intentional alterations during ICT system handling.	Considering the feedback received, it is relevant to clarify that the requirements included in Article 16 apply to all ICT systems. This approach is necessary to ensure complete and consistent protection since ICT systems not supporting critical functions play a relevant role in terms of operational resilience. It is also important to highlight that certain requirements included in Article 16 consider the criticality of the business procedures and ICT assets as proportionality factor, for example, concerning testing linked to such systems, as established in Article 16(2). The draft RTS offers flexibility for implementation, allowing financial entities to tailor practices to their specific operational needs and overall risk profiles, adopting a risk-based approach. While some respondents have suggested additional measures, such as continuous monitoring and mandatory penetration testing, following a risk-based approach, the ESAs believe these could introduce unnecessary complexity and costs while they may be outside of the scope of the current draft RTS. The ESAs find the existing guidance on testing and production environment segregation, source code integrity, and third-party provider certifications to be clear and risk-based, negating the need for further amendments. Some changes have been introduced in certain paragraphs to achieve better alignment of requirements across different articles of the draft RTS. In this regard, it is important to highlight

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	A respondent recommends risk-based penetration testing. Various respondents emphasize the implementation of a risk-based approach for data handling in non-production settings, with considerations for data type and system specifics. Suggestions include using anonymized or pseudonymized data in testing environments and revising data protection requirements in non-production areas. Various respondents seek clarification on the required degree of segregation between testing and production environments. Several responses ask to review data storage rules in "Staging" and "Disaster Recovery (DR)" environments, potentially allowing production data storage under strict security protocols. Various responses ask to implement a risk-based approach for source code reviews, considering activity criticality and incorporating SAST and DAST methodologies. Several answers ask for clarification regarding the extent, frequency, and circumstances for source code reviews, potentially limiting them to in-house or FE-specific developments. Various responses suggest limiting security testing of software packages to the application unit, excluding libraries and third-party software, and define "source code review where feasible."	the references included to Article 8 of the draft RTS, in particular for testing-related provisions. Additionally, modifications have been made to the wording and the order in some paragraphs to enhance clarity. The previous reference to "functional" and "non-functional requirements" has been deleted and replaced by "technical specification and ICT technical specification" as described in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012.Finally, "where feasible" has been introduced with respect to the analysis and testing of source code, limiting this process to those cases where such code is indeed available. Considering the feedback received, the ESAs agree with the suggestion of clarifying the Article further and have introduced additional explanations in the recitals.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Respondents emphasize the importance of testing recovery mechanisms to ensure system availability after disruptive events. Various responses encourage reliance on certifications or reports from TPPs, acknowledging limitations due to licensing and proprietary interests. Several responses ask to address the ambiguity around TPP software qualifying as an ICT system, noting varying effectiveness of control measures across financial entities. A respondent suggests excluding certain network, firewall, and connectivity services from segregation requirements, citing cost and practicality. Several respondents asked to define the terms "software packages" and "security testing", provide a clear definition of non-production environments and how secure measures would be compliant with the RTS	
ICT change management	Article 17: Some respondents recommend re-evaluating the segregation of duties in change implementation, especially for emergency changes or system updates. Several respondents asked for clarification between emergency changes and patches, along with the suggestion to remove	The ESAs favour keeping the current version of the draft RTS, emphasizing its clarity and suitability for financial entities of various sizes and contexts. There is no or very limited added value for amendments regarding the roles in change implementation, guidelines for TPPs, and the terminology used in ICT change management. Moreover, the ESAs express concern over potential complexity and costs associated with consulting error databases or introducing a risk-based focus to fallback

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	the term "systems" from the ICT change management scope for simplicity. A suggestion has been made to include guidelines for third-party service providers involved in changing ICT systems of financial entities. Various respondents have asked for a requirement to refer to known error databases or CTPP knowledge during the change process. There is a collective proposal emphasizing that fallback procedures should prioritize major changes, adopting a risk-based approach for enhanced efficiency.	procedures, advocating instead for a comprehensive testing of changes to ensure digital operational resilience.
Proportionality and granularity	Several respondents asked to review of the reporting requirements in terms of proportionality defined.	The ESAs have reviewed these provisions again, and consider the requirements are now sufficiently flexible, focusing on the policy, not the implementation. Proportionality considerations at provision level have already been reflected as appropriate. The general article on the overall risk profile and complexity consideration, Article 1, also serves to this effect.
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.		
	Respondents ask to sharpen the provisions on testing, integrating advanced tools such as SAST, SCA, and continuous evaluation of vendor software and hardware. Some respondents ask to integrate comprehensive guidelines to evaluate risks related to the supply chain, emphasizing continuous monitoring,	The ESAs consider that the suggested integrations focus on strengthening risk management, transparency, and supply-chain security. However, the ESAs consider that these additions could potentially escalate complexity and operational costs within the framework.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	attention to software supply chain in DevSecOps, open-source libraries, developer's defects, and third-party services. Several respondents ask for transparency in supply chains with Register of Information, adopt a risk-based focus on critical areas, and set baseline standards for supply chain risk management. Respondents ask to distinguish between outsourcing and purchasing, advocating transparency in delivered solutions from vendors. Respondents encourage comprehensive vendor evaluations, contractual security standards, ongoing monitoring, redundancy, automation tools, and regular reviews. Respondents ask to highlight the necessity of customized software and hardware for smaller financial entities, addressing the risk of reliance on a single market provider and ensuring operational continuity for micro third-party service providers. Various respondents ask to limit specific and challenging requirements for communication and roll-back procedures to major changes only. Certain comments suggest reliance on tests on identical hardware held by manufacturers, particularly for storage systems. There are comments asking for a deeper consideration of Article 16 of DORA in relation to both outsourcing and purchasing.	There is a need of maintaining a balanced approach, ensuring that any potential addons are proportional to their impact on the efficacy of the draft RTS. Therefore, the ESAs are supportive for the current version of the text, to ensure operational continuity and simplified requirements.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Q17. Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.		
Delete sectoral requirements	Some respondents suggested to remove CCP- and CSD-specific provisions from the draft RTS due to DORA being a legislation with a horizontal approach across the financial sector.	This is not an argument that should lead to the amendment of the CP text; in Level 1 there are these types of entity specific provisions and the consultations with the commission have not flagged any restrictions in this direction. With respect to the argument of transforming them to provisions that apply to all entities; The drafting of the draft RTS has been performed with this objective in mind, how-ever, given the heterogeneity of entities in scope of DORA, when it has not been possible to design requirements that were applicable to all entities, sector specific requirements have been used to cover those gaps.
Involvement of external respondents	Concerns about the involvement of external respondents: they should be involved only in case there is a significant visible impact for them.	As a reminder this requirement already applies under CSDR and EMIR, and its wording ("involve, as appropriate,") allows to address this concern.
Extension of requirements to all financial entities	Suggestion to extend the requirement to the rest of the financial entities.	It should be recalled that for CCPs and CSDs, this requirement originates from the PFMIs and have been carried over in EMIR and CSDR. The ESAs consider that in order to ensure continuity of compliance with the PFMIs these requirements should be carried over in the draft RTS. It does not appear that this requirement would make sense in other segments of the financial markets given the differences in interconnectedness and business types.
Coordination with sectoral regulations	A few respondents raised concerns as to how the coordination between DORA Level 2 and EMIR and CSDR Level 2 will be carried out, and the risk of redundancies and inconsistencies.	It is the intention that the draft RTSwill govern all ICT-related matters. The necessity to amend EMIR and CSDR Delegated Regulations in this respect will be carefully considered by the ESAs.
Physical and environmental security		

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Q18. Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.		
Further guidance based on ISO standards	Few respondents proposed to further clarify 'environmental threats' in Article 18(2)(b) and 'information processing facilities' in Article 18(2)(e).	Regarding the terms a few respondents have brought forward for further clarifications, the ESAs believe that these terminologies and concepts are already defined and aligned with EU and international leading practices and standards. Thus, the ESAs didn't make any amendments in the text.
Cloud-specific requirements in the draft RTS	One respondent demanded specific requirements to be related to Software as a Service (SaaS) and other cloud provisions need to be made more explicit.	Aiming at a technology neutral draft RTS, the article does not include any cloud-specific provisions regarding the security of ICT assets located outside the premises of a financial entity. All technologies need to adhere to requirements of Article 18. Several other provisions have been amended to be aligned with respect to Article 18, such as for instance Article 11. Having said that, particularly the provisions under Article 11(2)(k) have considered the specificities and nature of ICT third party services, such as cloud computing.
Proportionality	Several respondents would like additional proportionality elements to be applied.	Proportionality aspects are already sufficiently considered in the draft RTS.
Inclusion of more detailed requirements	One respondent suggested to the inclusion of physical penetration or intrusion tests in the provisions of Article 18(2)(e). One respondent suggested to define minimum requirements in in Article 18(2)(d).	The inclusion of physical penetration or intrusion tests in the provisions of Article 18(2)(e) would add another layer of complexity and cost for concerned entities. These implied costs are do not seem proportionate compared to the implied benefits to include the suggested provisions. In order to leave discretion and flexibility to financial entities we restrain from defining explicit minimum requirements.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
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.		
Additional controls/measures to be added	A large majority of respondents supported the current version of the text. A limited number of replies are sought to put into action improved measures for the transport and disposal of physical data carriers/devices, while striving to keep the controls for transportation and disposal of these items largely unchanged. Also, a small number of respondents suggested additional measures around, Implementation of failover tests, adoption of certain standards for selecting security control measures, consideration of customer impact while determining priorities and proportionality for protection of physical and environmental security, and implementation of security controls through the evaluation of ICT third party providers.	The ESAs do not consider the proposals to be feasible due to the additional complexity and costs they would introduce, including the significant resources and time required for regular failover tests, which could negatively impact the overall operational efficiency. The proposals are also seen as lacking flexibility, potentially enforcing a one-size-fits-all solution that may not suit the varied needs of different financial entities. While proportionality is mentioned in the proposals, the ESAs believe the amendments would add complexity and costs, in significant resources, time, and potential impact on operational efficiency. Additionality, there are concerns regarding the impracticality of over-reliance on third party providers certification, though this is addressed in another draft RTS, prepared under another mandate (see the draft RTS on ICT policy, prepared under Article 28 of DORA).
ICT and information security awareness and training **Q20. Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.**		

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
ICT and information security awareness and training	A group of respondents noted that Article 19 might not be in scope of the mandate of the RTS.	The ESAs agree with feedback from other respondents about the absence of a mandate for this article and decided to delete it. For this reason, the other feedback received was not considered. At the same time, the ESAs will consider developing further guidance on this area, as it is considered vital to ensure an effective digital operational resilience.
Human resources policy and access control **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.**		
Principle based VS Rule based	Few respondents requested more principle-based provisions rather than having such rule-based ones	As per comments on the general approach ESAs have taken with this draft RTS, principle-based being one of the key approaches followed. At the same time, the ESAs had to balance this with the requirement to fulfil the mandate and providing sufficient clarity to the financial entities on what is required. To this effect, in some area where the mandate is very specific and asks for further elements in a specific area, it is inevitable that the provisions would need to be more rule-based or detailed. This is the case with this section. the mandate under Article 15(b) of DORA foresees a specific task to develop further components of the controls related to access management rights referred to in Article 9(4)(c) of DORA. Therefore, being more principle-based than we currently are with these provisions would raise the risk of the draft RTS not meeting the specific mandate or not being sufficiently clear on the requirements.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Additional requirements	Few respondents required additional requirements in this section.	The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits, or such requirements are covered in other sections or articles of the draft RTS.
Third-parties service providers as human resources	Some respondents expressed concerns regarding categorizing ICT TPPs as "human resources" is problematic. The current expectations for TPPs might be overly burdensome and challenging for larger providers, especially in multi-tenant cloud environments where applying individual FE security policies isn't feasible.	The ESAs acknowledge the concern and restricted the provision to ICT third-party service providers using or accessing ICT assets of the financial entity.
Financial entities outsourcing operations	Few respondents emphasized the challenges of implementing ICT risk management policies for financial entities that outsource operations and lack in-house ICT resources. They advocate for managing risks with crucial third parties via contracts. A query was raised about whether specific policies and procedures are required for outsourced activities beyond the general ICT risk management framework and policy.	DORA already includes provisions that address ICT services carried out by third-party providers, including the necessary policies related to them. Therefore, financial entities are already mandated to manage and oversee the risks associated with outsourcing their operations to third parties, maintaining an established ICT risk management framework and policy, which can encompass specific areas even when activities are outsourced. This assures that the concerns raised regarding outsourced operations and collaborations with critical third parties through contractual agreements are duly covered under the existing mandates.
Additional clarifications	Few respondents requested clarifications on the meaning of specific terminology or concepts like need-to-know, need-to-use, least privilege, generic account, critical ICT systems, where applicable.	The mentioned terminologies and concepts align with EU and international leading practices and standards. No amendments in the text. Further guidance on generic account is provided in the proposed Recital (10). The wording 'critical ICT systems' has been replaced with 'ICT systems supporting critical or important functions' throughout the whole draft RTS.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Human resources policy	Few respondents noted that the Article 20 on Human resource policy is out of mandate. Few respondents noted that the article is not taking into consideration anomalous behaviour as requested by the mandate. Few respondents noted that Directive (EU) 2019/1937[17] is not applicable to all financial entities.	Article 19 of the draft RTS (former Article 20) has been drafted under the mandate given in Article 15(b) of DORA. Considering also the feedback received, the wording 'anomalous activities' has been replaced by 'anomalous behaviour' in Article 19(1), point (b)(ii). In addition, to solve the issue of applicability of the Directive (EU) 2019/1937, the wording 'where applicable' has been added. To further clarify Article 19(1), point (b)(iii), the ESAs modified it by referring to tangible information assets and to the fact that all assets referred to under this point should be in possession of the staff upon their termination of employment.
IM policy and associated risk	One respondent noted that the identity management policy should be based on the associated risk and that maintaining records of all identity assignments should only be mandatory for ICT assets supporting critical and important functions.	Identity management policy should be universally applied, regardless of associated risks. Every ICT asset, irrespective of its function, can be an entry point for security threats. By selectively maintaining records only for assets supporting critical functions, an organization may leave vulnerabilities exposed in lesser-guarded assets, potentially compromising the entire system. No amendment to the text.
Unique user accounts requirements	Article 21(3)(a): Several respondents raised concerns about the requirements for unique user accounts. While the aim is clear mapping between an individual and their system actions, there are instances, especially with electronic vaulting solutions, where multiple users access	The objective of the provision is to ensure accountability for any action taken in an ICT system. The concern has been considered and a sentence has been added to ensure accountability in accordance with Article (21)(1(c) [former Article 22].

[17] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, PE/78/2019/REV/1, OJ L 305, 26.11.2019, p. 17–56

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	a single privileged account. For TPPs, mandating unique identities/accounts seems unrealistic. According to one respondent the provision is also precluding the possibility for a single user to have more than one account.	The article does not preclude the possibility for a single user to have more than one account.
Frequency on the review of access rights and clarifications	Article 22(1)(e)(iv): Several respondents advocate for more flexibility on the review of access rights rather than strictly adhering to a prescriptive timeline. Some respondents request clarification on the meaning of "at user level".	The ESAs have reviewed again the frequency considering the feedback received and have decided that the six-months' requirement for ICT systems supporting critical or important functions is important to maintain. Considering the importance of this control towards ensuring confidentiality, integrity, authenticity and availability of data. At the same time, it is important to highlight that the ESAs considered a risk-based approach in this element, as it applies only to the ICT systems supporting critical or important functions. The ESAs also deleted the wording "at user level" that was reported to be creating confusion. The review and update of access rights shall be performed whenever a change is necessary.
Recertification and reconciliation	Article 22(1)(e)(iv): a few respondents advocated for the inclusion of user reconciliation and recertification of access rights.	The ESAs considered the feedback received regarding the inclusion of user recertification of access rights and modified Article 22(1)(f)(iv). As a result, they have revised Article 22(1)(f)(iv) to incorporate provisions for the update of access rights. The ESAs have considered introducing the additional requirements proposed regarding user reconciliation and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Authentication methods	Article 22(1(f): Some respondents noted that authentication methods should consider existing controls and align with leading practices and regulations. Risk assessments should guide the need for strong authentication, which might not be necessary for non-critical public functions. One respondent noted that the draft RTS's perceived blanket MFA requirement for all internet-exposed applications needs clarity and a more risk-based approach mentioning that is also unclear whether strong authentication is mandated also for customer-side access to publicly accessible ICT assets supporting critical or important functions.	The "overall risk profile of ICT assets" would naturally incorporate the existing control mechanisms because risk profiling involves understanding both vulnerabilities and the controls in place to mitigate potential threats. Also, further regulatory requirements already apply without the need to mention them here. Strong authentication methods are foreseen 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. No amendment to the text. After reviewing the provision, the ESAs deem it sufficiently clear. Due to the substantial threat posed by successful cyber-attacks, particularly those targeting remote access to a financial entity's network, privileged access, or access to ICT assets that support critical or important functions, or those that are publicly accessible, there is an increased vulnerability in the ICT systems. Consequently, in these contexts, robust authentication measures are mandated to enhance security.
Physical access clarifications and scope	Article 22(1)(g): a few respondents required clarification regarding the monitoring of physical access and what recording means. Few respondents requested to limit the recording and identification of natural persons to critical premises or sites only. One respondent requested to include expand the provision to areas where ICT or information assets reside.	Monitoring of physical access will not be specified further to leave flexibility to financial entities. Recording is now changed to logging to avoid any misinterpretation. For the same reason, the provision has been amended, referring to "*access*", rather than use the verb "*enter*" used in the previous version, to provide additional clarity. The requirement on identification and logging is now limited and the text is aligned with the rest of the draft RTS and DORA. Finally, the text has been amended taking into consideration the feedback received on expanding the provision to areas where ICT or information assets reside.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
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.		
Additional requirements	A few respondents required additional requirements in this section.	The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that their costs would outweigh the benefits, or such requirements are covered in other sections or articles of the draft RTS.
ICT-related incident detection and 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.**		
Anomalous activities and anomalous behaviour	Some respondents requested more clarity on the definition of anomalous activities and anomalous behaviour.	Both terms are already included in DORA text and the ESAs consider that their use in the draft RTS is sufficiently clear.
Relevant contacts	One respondent suggested to limit the list of contacts included as the current proposal is too granular, other respondents suggested to included "relevant" to the requirement.	The ESAs have modified the text to include "relevant" contacts only, to create some flexibility on the configuration of this list and limiting to those related to ICT operations security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management.
Retain evidence and personal data provisions	According to some respondents, the retention requirement may, in some cases, be conflicting with the GDPR. Another also that the requirement may conflict with national law. One respondent indicated that the wording is open for wide interpretation. Some concerns were also raised on the retention period, for some respondents, in an ICT security sense,	The reference to relevant provisions on personal data is deleted given that is not necessary since compliance with GDPR is required for financial entities (as clarified in the recitals of the draft RTS and is directly applicable, personal data protection applies to all personal data collected/records kept on this basis The text is reflecting

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	is a business decision based on legal requirements, which should reflect sectoral and national specificities.	enough flexibility for different needs and considerations within the Financial Entity. No additional changes are introduced.
Remove review of the ICT response and recovery plans	Several responses indicated that the reference to ICT response and recovery plans is misleading, the yearly review of ICT-related incident management policy, its procedures, protocols, and tools is unnecessary as it is captured by review of the risk management framework.	Considering the feedback received, the text has been amended and this provision has been deleted.
Collect and analyse data	Some respondents expressed confusion about the provisions where financial entities are required to collect and analyse all the following information on "internal and external factors, including business and ICT administrative functions in former Article 24(2)(a). Some other respondents recommend removing or clarifying the part "including usual scenarios of detection used by threat actors and scenarios.	The ESAs have considered the feedback received and clarified the text by introducing the following changes: - inclusion of "monitor" and removal of "information" in the introduction of paragraph (a). This simplifies the requirement by removing monitoring and log analysis as a specific measure (previously included in paragraph (d) and now reflected and clarified in the first bullet point of paragraph (a)); - clarification of the elements that should be considered, at least, in the first point, with regards to the internal and external factors to collect, monitor and analyse; - modification of point (ii) clarifying the text; - finally, two of the elements previously listed as trigger events have now been included in this section, as they do not constitute, in view of the feedback received, events for triggering ICT-related incident detection and response processes, but rather elements relevant to the detection of anomalous activities (i.e. problems reported by users and ICT-related incident notification from an ICT third-party service provider of the financial

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		entity detected in the ICT systems and networks of the ICT third-party service provider and which may affect the financial entity).
Data source alerts	For Article 24 (2)(b) some respondents shared that the requirements regarding tools for automated alert generation should be amended and/or clarified.	Considering the feedback received, the text has been amended to reflect whether alerts should be generated if a data source of a critical or important system is compromised or the log source.
RTO time and incidents	For Article 24 (2)(c) several respondents requested modification of the text. Respondents advocated for a clear distinction between recovery time objectives and incident resolution time, suggested removing the reference to managing an incident within RTO and adding the word "prompt" in front of detection to convey the expectation that alerts are considered and acted upon at an appropriate time. One respondent raised the issue that the requirement could imply a requirement to have human resource on duty (24/7),	The ESAs considered that most of the issues raised are relevant and have modified the text by introducing a reference to manage the ICT related incidents within the expected "resolution" time, as defined by financial entities.
Scenarios and logs	For Article 24 (2)(d) Respondents pointed out that the requirement is not clear, the text should be revised and completed by clearly describing the mapping between scenarios and logs. Several respondents pointed out that the sentence is incomplete, therefore the requirement is not clear.	The ESAs have considered the feedback and deleted the text in order to avoid overlaps with paragraph 2, which is now reformulated to include the requirement for monitoring that was previously included in this paragraph.
Record, analyse and evaluate information	For Article 24 (2) e) several respondents commented that a risk-proportionate approach would be required regarding the information to be analysed, suggesting deleting "all" from the sentence.	The ESAs have modified the text following the feedback received. Also reference to "staff" has been deleted. The ESAs consider that the amended approach is sufficiently risk-based.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Criteria to trigger the ICT-related incident detection and response processes	Several respondents recommended changes in the criteria which should trigger the ICT-related incident detection and response process. Some of the changes proposed and the concerns raised were: - Inclusion of additional criteria. - Deletion of some elements. - Lack of clarity or justification in some of the elements. - Remove of "all" in the introductory text. - Some respondents raised the issue that certain criteria are triggers for alerts in terms of security of functioning incidents, others include certain types of aspects which are more on the side of incident analysis in terms of identifying its impact. - Some respondents shared that the criteria are too broad and likely to result in too many false alarms being captured. - Some criteria to be subjective.	The ESAs are of the opinion that some of the proposed elements from respondents are relevant, and the text has been modified accordingly. - Firstly, the triggers related to the analysis of the information itself have been removed and relocated to paragraph 2 of the article. - It has been decided to retain the reference to 'all' in the introductory phrase. The text remains unchanged in this respect. It is also important to clarify that not all elements need to occur simultaneously and that the list is not limited to these; rather, these triggers shall be considered, at a minimum, by the financial entity. - Finally, it has been clarified that, in applying the criteria introduced in this provision, the criticality of the affected services shall be taken into consideration.
ICT business continuity management **Q24. Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.**		
Missing elements	Some respondents shared feedback on elements they considered are missing in the text:	Most of the responses supported the current proposal for this chapter of the draft RTS. Amongst the feedback received, reference was made to the additional elements

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	- 2 respondents shared that an overview of the minimum contents of ICT business continuity plans is missing. - 1 respondent shared that there are no requirements for Testing for ICT response and recovery plans. - Art 25(1) – In addition to "activation" (25(1)(d)) the paragraph should also include "deactivation". - Suggestions on Article 26(2) - One of the items in the list should be "Minimise the risk of affecting the business operations". - Explicit provision should be made in Article 25 for the business continuity policy to require consideration of ways to limit the harm to customers, users, market integrity and financial stability.	not included in the current proposal, in this respect it is important to note that the current content is based on the mandate set out in Article 15(d)(e)(f) of DORA and therefore it is not within the scope of the mandate to cover additional aspects as those mentioned in the first two points. On the other hand, some of the proposed elements have been included, such as the inclusion of "deactivation" in Article 24(1)(d) and Article 26(1)(b) [Former articles 25 and 27]. Regarding the last two points, it is considered that the current content of the provisions is sufficiently comprehensive to cover the elements identified.
Relation of ICT-BCM & BCM	Several respondents have expressed concerns that the approach and wording used in DORA and the draft RTS may lead to confusion between the ICT Risk Management Framework, ICT Response and Recovery Plans, and Business Continuity Plans. They emphasize that, in practice, the ICT business continuity plan under Article 25 will be integrated into the financial entity's broader business continuity plan, specifically addressing ICT-related considerations.	The terminology used in Chapter IV is in line with the Articles of DORA related to this area and from the mandate under Paragraphs (d)(e) and (f) of Article 15 of the same Regulation. Considering the feedback received on the relationship between the BCP plan and ICT BCP policy, the ESAs already included specific provisions to clarify the interrelation of ICT and overall business continuity in Article 24(1)(a). It is thus important to consider that Article 11(1)(a) of DORA provides that the ICT business continuity

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	These respondents recommend that ESAs clarify that the requirements outlined in the draft RTS for the ICT business continuity plan and the ICT business continuity policy can be met through more comprehensive business continuity plans and policies. They particularly welcome the explicit reference in Article 25(1)(a) to locating ICT business within the overall business continuity of the financial entity.	policy may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.
Definitions, clarification of terms used	Some respondents shared feedback on elements they considered are not clear in the text: - A number of respondents have noted that in Articles 25, 26, and 27, various terms such as 'critical functions,' 'critical operations,' and 'critical ICT systems and services' are utilized. There's also mention of 'critical business functions' in Article 26(2)(c) and a similar reference to 'critical ICT systems and services of the financial entities' in Article 27(1)(b). - In Article 27.4, one respondent notes the creation of a new category of ICT third-party providers referred to as 'key importance.' - In relation to Article 27(1)(e), one respondent emphasizes that, in the short term, only partial recovery is achievable, and a full recovery may not be attainable. - Few respondents shared that there is a need for clarification in both Article 26 and Article 27, specifically regarding the	The ESAs have considered the feedback provided and included changes and clarifications in the articles included in this chapter. In this way, the different terms used, for example, criticality of functions, operations, etc., have been homogenised and aligned. The same has been done for the previously named "key importance" providers. As regards 'partial systems and recovery', the text has been amended. The term 'and' has been deleted as its inclusion was inaccurate, simply retaining the possibility of partial recovery of systems. About the definitions, the ESAs believe that the terms used do not need further clarification and that they are either sufficiently clear or are already contained in the Level 1 text. Regarding the elements that apply to only critical or important functions, the ESAs consider that the text is clear enough. Finally, the recitals have been completed to bring more clarity to the interrelationships of the provisions included in this chapter and the other provisions of the draft RTS.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	definitions of terms like 'business cycle,' 'short-term recovery plan,' 'long-term recovery plan,' 'partial systems,' and 'the establishment of an adequate set of severe but plausible scenarios'. - One respondent seeks confirmation that in Article 25, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements are exclusively applicable to critical or important functions. - One respondent suggests that the requirements outlined in Article 26(2) should solely apply to critical and important functions. The same principle should be extended to Article 27, subsections 2 and 4. - Lastly, one respondent proposes the integration of the proposed text of Article 25(1) with certain other elements of the draft RTS to enhance clarity and coherence.	
Proportionality, Risk-based approach, Frequency	Several respondents shared concerns about the proportionality / principle of proportionality, the need to adopt a risk-based approach and the impact on SMEs and micro-enterprises. Similar concerns were raising on the testing and their frequency, the need to have different approaches for different types of financial entities based on their characteristics.	The ESAs consider that the current text incorporates numerous elements of proportionality, allowing for a risk-based approach in its implementation. Proportionality considerations at provision level have already been already included and reflected, as appropriate. The general article on the overall risk profile and complexity consideration, Article 1, also serves to this effect. In the articles included in this chapter, these elements have been duly considered. Consequently, the application of certain requirements has been restricted to critical

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	Few respondents raised that the requirements should be specified in a different way for IORPS and Trading Venues due to their specificities. There is a proposal to delete the term "at least" in Article 27(1)(b).	functions, and flexibility has been introduced in the definition and implementation of certain provisions. Regarding the proposal to delete "at least" from Article 26(1)(b) [former Article 27], ESAs have decided to maintain this, as its use is deliberate and serves in providing some proportionality to the text. Article 25(6) and Article 26(1)(g) [former Articles 26 and 27] have been deleted as the requirements previously included have been considered covered in DORA.
Entity level vs. asset/process level	Feedback from a respondent highlighted that the use of Business Impact Analysis in this chapter is inconsistent, particularly in terms of the level at which BIA is to be performed.	The ESAs consistently refer to the definition of BIA as outlined in Level 1 text, and we do not propose any additional modifications in this regard.
Involvement of TPP in ICT BCM Testing	Several respondents raised concerns about the involvement of TPP in ICT BCM testing and in ICT response and recovery plans, as included in Article 26(2)(b)(e) and Article. 27(4)): - ICT Business Continuity Testing Impact and Feasibility with Third Parties: A number of respondents expressed concerns about the feasibility of ICT business continuity testing with third-party providers. They're particularly worried about the challenges faced by TPPs in allocating resources for individualized testing and the potential for significant costs and disruptions if numerous financial entities conduct individual testing. Respondents recommended relying on standards and independent certification, such as ISO 22301:2019. A group of	The requirements introduced in Articles 25 and 26 [former Articles 26 and 27] regarding third-party service providers should be interpreted in conjunction with the provisions included in Level 1 text. This requires considering the mandate established in Article 15(e), which explicitly references "any relevant ICT third-party service provider" regarding testing. It is also relevant to collectively consider the requirements included in Chapter IV of this draft RTS with the elements present in Chapter V of DORA regarding the management of ICT third-party risk. It is equally important to collectively consider the requirements included in Chapter IV of this draft RTS with the elements present in DORA, specifically in Chapter V regarding the management of ICT third-party risk.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	respondents also interpret Article 26(2)(b) as primarily focusing on testing ICT services rather than third-party business continuity plans and recommend limiting the testing scope to deployed services. - Specificities for Trading Venues: some respondents emphasized the need for introducing a mitigating clause to prevent adverse repercussions on trading venues. These concerns stem from the fact that modern technology enables low-latency trading, and respondents fear that the proposed changes could significantly slow down global trading, introducing substantial latency.	The provisions included in the aforementioned articles also encompass considerations regarding proportionality in their implementation. Furthermore, Article 25(2)(b) [former Article 26] explicitly refers to the testing of ICT services provided by ICT third-party service providers, where applicable. In the same article, more clarity has been added, including a clarification of the scenarios that shall be dully considered. The use of related certifications cannot serve as a substitute for the requirements established in DORA and further detailed in this draft RTS. Addressing the concerns raised concerning trading venues, the ESAs have analysed the specificities and have not identified sufficient elements to include mitigating requirements. Other responses related to the specific requirements for CCPs, CSDs and trading venues can be found in Q25.
ICT BCM - Cloud aspects	Few respondents shared that with regards to testing ICT continuity plans, more attention should be paid to the advancement of cloud and technologies used for continuity.	As previously mentioned in this Final Report, ESAs have followed a technology-agnostic approach in preparing the draft RTS. Regarding ICT business continuity management, the ESAs consider that the proposed requirements allow for sufficient flexibility in their implementation, while not limiting the provisions to a specific technology.
Redundant Capacities & switchover	Different respondents suggest changes and more clarity in Article 25(2)(c) Article 26(2)(c) and Article 27(2)(c) of the proposed draft RTS: - Some respondents expressed concerns about Article 26.2(c) regarding switchover. They consider that the article presumes a primary/secondary systems ICT business continuity framework,	The ESAs consider that the current proposal incorporates flexibility in the options that the Financial Entity may consider or implement. The reference to switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities is extracted from DORA. The text has also been amended to provide greater clarity, in line with the feedback received in this and previous points.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	sometimes referred to as "hot/cold." However, some firms may operate a "hot/hot" framework. To address this, flexibility should be introduced. - Concerns were raised about Article 27(2)(a), which similarly presumes a "hot/cold" operating model. It is suggested that the requirements be adaptable to firms operating a "hot/hot" model. Clarity is needed on terms such as "second location" and when it is required to run production applications from a secondary location. - There were concerns raised for the "Disaster recovery environment" (Article 26, 2c), which may be cost-prohibitive in the case of cloud solutions. Considerations for cloud-based solutions need to be factored into the requirements. - Some respondents requested more clarity on some of the terms used, for example "sufficient period of time". - Respondents raised concerns about Article 26(2)(c) and the possibility of interpreting it as testing simultaneously the fall-over of people, processes, and technology.	On the other hand, it is not deemed necessary to introduce additional definitions for the terms included in these articles. The requirements regarding testing in Article 25(2)(c) [former Article 26] should be understood in the context introduced in paragraphs 1 and 2 of the same article, with their primary objectives being to ensure the continuity of the financial entity's critical or important functions.
Reporting to management body	Some respondents requested more proportionality in Article 26(5) of the proposed draft RTS, particularly by considering the removal of the term "any" and specifying material deficiencies that need to be reported to the	This article has not been amended as the ESAs consider that the current text focuses only on the reporting of the deficiencies found and this is a key element to be transmitted to the management body. This is without prejudice to possible

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	management body, along with determining which function should be responsible for reporting such deficiencies.	delegations in the analysis and assessment of these deficiencies by the management body.
Scenarios	Several respondents shared proposals regarding the scenarios included in Article 27(2) of the proposed draft RTS. - Inclusion of new scenarios (e.g., climate change, concentration risk) and deletion of others (e.g. political and social instability). - Proposals for removal of the imperative to include "all" proposed scenarios for proportionality and introducing flexibility in testing scenarios based on a risk-based approach, focusing on scenarios relevant to the financial entity's nature of operations, risk profile, and potential threats and suggesting that mandated scenarios could result in firms navigating towards the same prescribed scenarios rather than taking a risk-based approach. - Emphasis on the importance of plausible scenarios for testing resilience and avoiding implausible ones requiring the coordinated failure of numerous controls. Suggestion to focus on the root cause of scenarios, not just their effects.	Regarding the scenarios considered and the inclusion of additional scenarios or the removal of some of those included, the ESAs consider that it is indeed relevant to include climate change considerations and have introduced it the text. On the other hand, it is considered that concentration risk should not be introduced as it is out of the scope of this RTS and already covered in DORA Level 1. At the same time, this does not imply that concentration risk is not important and that it doesn't need to be considered; on the contrary the ESAs believe that this is a significant risk that needs to be considered and assessed in accordance with provisions of DORA. Finally, the scenario related to political and social instability (also considered in DORA) is maintained as it is considered relevant. In addition, more flexibility has been introduced in the identification of scenarios, both at the testing level and in the development of ICT response and recovery plans. It has been clarified that financial entities shall "duly take into account" all of them in their identification process. This, together with the mentions of the "relevance" of scenarios in Article 26 [former Article 27] and the "plausibility" of scenarios with respect to testing in Article 25 [former Article 26] and considerations included in Article 24 [former Article 25], reflects fully the risk-based approach followed in the text. Finally, it was considered appropriate to include some granularity in the number of scenarios in order to be able to account for the different risks and effects of each

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		scenario. Moreover, the description of some of these scenarios has been slightly modified to provide more clarity.
Q25. Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.		
Remove or reduce sectoral requirements	There are various requests to remove or reduce sector specific requirements that have been transposed from the current legislation to the DORA legislation with their current wording.	These requirements were discussed and agreed through a separate legislative process before DORA by taking into account the specificities of these entities, the views of the NCAs, Industry and other relevant respondents as well as international guidance. Based on this, and while the ESAs have considered the feedback submitted during this PC, they believe that there hasn't been any change in those specificities and in the technological development to justify a change in the approach. Specifically, there have not been any developments that justify a reduction of standards by removing or reducing requirements linked to recovery time objectives, recovery point objectives and redundancy of data centre and facilities.
Remove or amend the 2-hour RTO for CCPs, CSDs and trading venues	Different respondents suggest removing or amend the 2-hour RTO for CCPs, CSDs and TVs, arguing that this requirement may not be appropriate in all cases, for example, a cyber-attack where the specifics of the attack mean that additional risk management controls are required to prevent further contagion.	The RTO of 2h is a requirement for entities to design their IT infrastructure and business continuity measures with the objective of achieving downtime of less than 2h by design. This requirement does not imply that in the event of an incident affecting the entity in an unforeseen manner, that the entity shall resume its activity in 2h without considering the consequences. It is a requirement that implies the need to design its infrastructure and operational resilience measures with the objective of achieving a high availability of its systems, with the specific quantitative threshold of 2h as reliability objective.
Trading venues	Different respondents suggest removing or amend the existing requirement 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	These requirements are consistent with the existing requirement in Regulation (EU) 2017/584, and while the ESAs have considered the feedback submitted during this PC, they have also considered the critical nature of services provided by trading

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	zero" such that "close to zero" is changed for "minimised" of for "when the market operator is comfortable that it can ensure again a fair and orderly market". The proposed amendments are based on thresholds that are not clear and measurable, in addition to that, the objections have not argued what are the technical barriers to adopt technologies that enable "close to zero" data loss or why the requirements should be lowered from the existing applicable standards.	venues and believe that there has not been any change in those specificities and in the technological development to justify a change in the approach.
CCPs	request to specify whether "secondary processing site" in art 25.2 refers to secondary data centres. removal of Article 25 (2) (c) (iv) on "secondary processing site". Regarding Article 26(3), it is suggested to include the phrase "where applicable", as it may not always be appropriate to include members in the testing of ICT Business Continuity Plans.	These requirements are consistent withthe existing requirement in Regulation (EU) 153/2013, and while the ESAs have considered the feedback submitted during this PC, they believe that there has been no change in those specificities and in the technological developments to justify a change in the approach.
CSDs	With respect to the request to replace "any" by "relevant" in Article 25.3(a).	These requirements are copied from the existing requirement in Regulation (EU) 2017/392, and while the ESAs have considered the feedback submitted during this PC, they believe that there has not been any change in those specificities and in the technological development to justify a change in the approach.
DRSPs	Some respondents requested to incorporate the existing requirement for data reporting service providers "*the target maximum recovery time for critical functions should be no longer than six hours in the case of approved publication arrangements (APAs) and consolidated tape providers*	The ESAs have opted not to set a specific RTO for DRSPs, allowing financial entities the flexibility to determine their own recovery objectives in offering and maintaining services at all times, in compliance with Article 12 of DORA. Also, to foster a sector-neutral approach in developing the draft RTS, only a limited number of existing requirements regarding the RTO were incorporated. This policy

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	(CTPs) and until the close of business of the next working day in the case of approved reporting mechanisms."	decision considered the relevance of market infrastructures like CCPs and CSDs and existing international Article 22 like the PFMIs, and the critical nature of services provided by trading venues.
Report on the ICT risk management framework review **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.**		
Additional clarity on some terms and requirements	Most respondents support the current proposal in relation to the report on the review of the ICT risk management framework, among them there are a number of respondents who requested more clarity on some of the terms used and some of the provisions, in particular regarding the following elements: - Replace "the staff" with "the responsible function" in Article 28(2)(h)(iii). - Define the purpose of the required report. - Guidelines for electronic format. - Examples or best practices. - Purpose of "start" and "end" dates. - Clarity on the terms "changes" in the framework and "weaknesses".	The ESAs consider that the text is sufficiently clear regarding most of the elements on which respondents have identified that further clarity is needed. In particular, the ESAs have kept the text on the following provisions largely unchanged: - Electronic format: the reference to searchable electronic format should cover all the possibilities without mandating or referring to specific document types. - Examples or best practices: this is out of the scope of the RTS. - Purpose of "start" and "end" dates: we believe that the text is sufficiently clear. At the same time, some changes have been introduced to provide more clarity and some elements have been deleted. Specifically, we list some key changes below: in Article 27(2)(h)(iii) [former Article 28], as the term "staff" was too general, it has been changed into "the function responsible".

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
		Given the purpose of the report is already clear, the requirement introduced in Article 27(2)(a)(ii) [former Article 28] has also been deleted as it did not provide additional information. Finally, the ESAs are of the opinion that the purpose and scope of the report are sufficiently clear and there is no need to introduce additional elements on what constitutes "changes" or "weaknesses" in the ICT risk management framework.
Clarification on roles	Some respondents seek clarification on roles within the report. Questions include the delegation of penal risk by the management body and which function should own the report. Entities seek clarification on which function should own the report and inquire about roles and responsibilities, specifically whether it falls under the purview of first line of defence or second line of defence.	It is important to note that the governance aspects and the specific allocation of responsibilities are out of the scope of the mandate granted under Article 15(g) of DORA, and thus they cannot be considered in the draft RTS Please also refer to the topic on governance aspects (former Article 2).
Clarity on the need to produce the report on the review of the ICT risk management framework	Some respondents requested clarity on whether existing annual reporting obligations fulfil the requirements or whether having some related certification for information security is sufficient for meeting reporting obligations under Article 28. Also, whether the report should be prepared at the individual financial entity level or also at the consolidated group level.	It is important to note that the report on the review of the ICT risk management framework is included in Article 6(5) of DORA. In line with the mandate granted under Article 15(g) of DORA, the proposed draft article only covers format and content considerations. Therefore, the comments received are outside the scope of the considerations for this draft RTS.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
More proportionality on the report	Some responses looked for greater proportionality in the content and periodicity of the report. Few suggestions were made to align the report to established frameworks.	It is important to highlight that the report is a requirement established at Level 1 of DORA. Considerations about the size of the financial entity are also embedded in the draft RTS itself. In general terms, the report will cover changes made in the review process, whether periodic or ad hoc. The included elements are the minimum necessary to ensure that the report is comprehensive and understandable for the reader. Considerations about other frameworks, standards, etc. are outside the scope of this draft RTS.
Major ICT operational incident	A number of respondents raised questions about the necessity of a review/report if a "major ICT operational incident" doesn't lead to changes in the framework. Also, clarity is sought on the definition and reporting requirements for "major and immediate deficiency.	ESAs have considered the feedback received and modified the requirement, deleting the reference to "in case of major and immediate deficiency" and including "where appropriate".
Simplified ICT risk management framework **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.**		
Segregation and independence clause	A few respondents suggested eliminating Article 30(4) from the draft RTS. This article mandates financial entities to segregate and ensure independence between control and internal audit functions. Such an obligation isn't found in Article 16 of DORA. Furthermore, according to Article 24 of Delegated Regulation 2017/565 and Article 16(5) of MiFID II,	The draft RTS mandate gives the possibility to introduce requirements related to governance. DORA introduces requirements for internal audit independence to investment firms via Article 6(6), regardless of MiFID II. The ESAs considered that the requirement can be met regardless of the size of a firm.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	investment firms aren't required to have a segregated and independent internal audit function.	
Risk tolerance level for ICT risk	A few respondents noted that Article 16 of DORA does not include an obligation, comparable to Article 6(8)(b) of DORA, to establish a risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity and analysing the impact tolerance for ICT disruptions. Therefore, mitigation strategies should be defined according to Article 33(1)(c) of the draft RTS only for major ICT risks and only when necessary.	Mitigation strategies should be defined for the ICT risks that are not within the risk tolerance levels. The respondent hasn't provided any justification as to why the simplified framework shouldn't establish risk tolerance levels for ICT risk, apart from the mandate concerns. This requirement is consistent with the mandate of the draft RTS.
Additional clarification	A few respondents advocated for more detailed descriptions of physical and environmental control in accordance with specific international standards.	The mentioned terminologies and concepts align with EU and international leading practices and standards. No amendments in the text.
Additional requirements	A few respondents suggested to integrate Article 30(2) with new points: (j) monitoring the accuracy of security scans referred to in Article 26. (k) defining and maintaining the ICT and information security objectives aligned with the company business.	The ESAs have considered introducing the additional requirements proposed and have decided not to include them. This is due to the consideration that such requirements are covered in other sections or articles of the draft RTS. Proposed (j) on security scans is just a specific aspect to be reviewed and points (g), (h), (i) of Article 28(2) already cover this aspect from a principle perspective. Proposed point (k) is already covered by Article 28(2)(a).

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
Further elements of systems, protocols, and tools to minimise the impact of ICT risk **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.**		
General	Most respondents agreed with the suggested approached regarding the simplified ICT risk management framework. Few respondents requested further clarity while others requested further flexibility and consideration of proportionality given the expected implementation challenges for small financial entities.	The proportionality principle of Article 4 of DORA also applies to the simplified ICT risk management framework and this is considered already sufficient for financial entities to implement the legal provision in accordance with the principle of proportionality. Moreover, recital (21) of DORA clarifies that the digital operational resilience baseline for financial entities should be increased while also allowing for a proportionate application of requirements for certain financial entities, particularly financial entities subject to a simplified ICT risk management framework.
Detailed proposals	A number of detailed proposals were provided by respondents, such as to reiterate the relevance of ICT and information security awareness and training, to stress further the aspect of resolution by focusing on follow-up actions, to cover identity management, to explicitly mention technical debt management and tech life cycle management. A respondent proposed the introduction of common requirements for all assets as a security baseline and to allow financial entities to add complementary controls for highly critical systems as having distinct security controls for non-critical and critical systems will add complexity to the compliance projects initiated by the financial entities. Another suggestion was to explicit consider imperatives in Article 37(1) and (2) to harmonise the implementation of security measures with the low latency imperative	A number of proposals were going beyond the legal mandate of this regulation, as provided in Article 16 (3) of DORA, for example the proposal to included awareness and training also for small financial entities, which is covered in Article 16(1)(h) of DORA. Furthermore, some proposals were quite prescriptive and/or more detailed than the provisions of the 'full' ICT risk management framework or not relevant to the financial entities falling under the scope of the simplified ICT risk management framework (e.g., low latency impact on EU trading markets).

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	and future trading developments as well as overall ICT risk impact while pursuing efficient financial activities.	
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.		
General	Respondents noted that the expansion of ICT operation security for all ICT assets would represent extra building and running costs, which can be disproportionate for small financial entities. It was further noted that, at the very least, such expansion would require a longer implementation planning period of no less than 2 years. In this regard, respondents suggested to allow financial entities to expand the perimeter of ICT services to be included in the DORA framework on the basis of an internal costs/benefits analysis or, a more pragmatic and cost-effective solution, would be to apply ICT operation security only to ICT assets supporting critical and important business functions.	Having considered the comments from respondents, the ESAs believe that it is important to expand the ICT operation security requirements to all ICT assets. The reasoning is two-fold: information security risks cannot be analysed solely through the assets supporting the important and critical functions, since other vulnerable assets can be points of entry into the network and information systems; and considering implementation of financial entities on this, it would not introduce significant additional operational burden, as the frameworks in place normally cover all the ICT assets anyway. At the same time, as explained in the proposed Recital (7), when implementing the ICT operation security requirements, the financial entities should focus specifically on those ICT assets or systems necessary for the business operation and which bring value (not only financial value) to the financial entity, considering their criticality and potential impact in case of the loss of their confidentiality, integrity and availability.
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.		
General	Few respondents noted the current requirements are sufficient and in line with existing sectorial guidance. Other respondents suggested additional measures or control specific for cloud resources such as ICT	The ESAs consider that the draft RTS should remain technology-neutral and should not identify specific products or technologies. Such approach should ensure that

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	business continuity management measures, further information on the security of other elements in the cloud environment, specifying remediation times, the 'attack surface reduction' control, identification and assignment of responsibilities in compliance with the Shared Responsibility Model, technical/organizational segregation of access to the management plane and, in general, to administrative interfaces, including both web consoles and APIs, proactive and detective management of issues/non-compliances arising from misconfigurations of cloud resources and detective management of issues arising from cloud native workloads.	the legal text remains future-proof to the extent possible, thus avoiding the need of frequent revisions.
ICT business continuity management **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.**		
Proportionality aspects	Two respondents disagree with the proposed approach to ICT risk management policy, as applying it is impractical for most IORPs that lack own staff or ICT infrastructure, typically relying on third-party providers who have their own ICT policies. Financial entities outsourcing all operations should focus on managing ICT risks with critical third parties rather than setting up a comprehensive framework. The requirements, especially those in Article 4(2), should be proportionate and limited to critical ICT systems for practicality and relevance. One respondent agrees	Please refer to our response in Q2 on proportionality. The proportionality principle is embedded in DORA and applies throughout DORA. The ESAs agree that the general provisions on consideration on overall risk profile and complexity (former Article 29 of the draft RTS, now Article 1) should therefore also apply to the entities subject to DORA Article 16(1). On the introduction of specific provisions for IORPS: as mentioned in responses above, the ESAs favour a sector-agnostic approach. In addition, the principle-based requirements coupled with the proportionality provisions of DORA and the general provisions on consideration on overall risk profile and complexity (Article 1 of the

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
	with the proposed approach, provided that a new article on the principle of proportionality is added.	draft RTS) should provide reasonable flexibility for financial entities that are of lower scale, size, complexity and overall risk profile than others. In this context, the ESAs didn't introduce specific provisions for IORPs.
More clarity and granularity	Two respondents request more granularity on scenarios and their assessment to establish and implement response and recovery plans. Another respondent asked to clarify that Business Continuity Planning includes disaster recovery. Also, regarding Article 41: smaller financial entities alongside communication plans should consider decision-making procedures as part of their ICT business continuity policy. Finally, the reference to testing ICT business continuity plans against "severe but plausible" scenarios should be re-inserted for the simplified ICT risk management framework.	The complexity and granularity of the provisions in the Title III had been significantly reduced compared to the articles on Business Continuity in Title II in the initial draft RTS presented for public consultation. This reduction included, among others, the requirements linked to the scenarios to be considered or the requirements related to the testing of the plans. This approach is consistent across the different elements of Title III and therefore no additional granularity is included. Furthermore, the final draft RTS has also simplified and clarified the requirements concerning the components of ICT Business Continuity Plans. Specifically, previous paragraphs (1), (2), and (3) have been consolidated into a single requirement now found in the new Article 39(1), which now also encompasses references to the scenarios. Requirements related to insurance identification have been deleted too, as it is usually performed by the financial entities in a more general way and therefore it is not considered relevant in the context of the draft RTS.
Guidelines on business continuity management	One respondent believes that business continuity management is another area where smaller entities could beneficiate from further non mandatory guidance, developed by the ESAs at a later stage, in order for them to fully understand the importance of this topic and the steps that should be taken.	The ESAs welcome the feedback and may consider whether further guidelines are needed in this area.

Topic	Summary of the comments received *References here below and in the consultation questions are made to the articles of the draft RTS submitted to public consultation.*	ESAs' analysis *References below are made to the articles of the final draft RTS.*
ICT BCP VS BCP	According to one respondent, Article 42 seems only related to business continuity, without any particular reference to the ICT.	Article 16(3)(d) of DORA mandate the ESAs to specify further the rules of testing of Business continuity plans. Therefore, Article 40 remains unchanged.
Report on the ICT risk management framework review **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.**		
Major changes	Three respondents suggested to include "major" in the Article 43(2)(a)(iv), adding more proportionality and aligning the requirements with those included under Article 28.	ESAs have included a modification in the requirement in line with the comment received. This will mirror the same requirement in the regular ICT risk management framework, and it is relevant given that the simplified framework should not be more demanding than the regular framework. Other editorial changes have been introduced to provide more clarity to the text.
Governance	A few responses requested clarity on the function responsible for developing the report and the possibility to rely on external parties.	Governance aspects are out of the scope of the mandate for this article. The possibility to rely on external parties is not limited in the text.