EUROPEAN
COMMISSION

Brussels, 13.3.2024
C(2024) 1532 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 13.3.2024

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to set out uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector. 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 aim of preventing and mitigating cyber threats.

In that regard, under DORA Article 15, fourth subparagraph "*the ESAs shall, through the Joint Committee, and in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards*" in order to further ensure the "*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. ENISA has accordingly been part of the ESA Joint Committee Sub-Committee on Digital Operational Resilience (JC SC DOR).

This delegated regulation corresponds to that mandate and was transmitted to the Commission on 17 January 2024.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

As part of developing the standards set out in this draft regulation, the ESAs published the draft RTS on 19 June 2023 for a three-month consultation period, which closed on 11 September 2023. The ESAs received 120 responses from a variety of market participants across the financial sector. The ESAs' final report provides a full overview of stakeholder responses.[1]

The respondents to the public consultation commented on the following aspects of the proposed draft RTS:

- Calls for an extension of the implementation deadline;
- Calls for stronger proportionality (e.g. proportionality going both ways, i.e. accounting for both increased and reduced complexity and risks; a more sectoral approach with further proportionality for e.g. insurance undertakings, …);
- Calls to exclude governance aspects from the draft RTS as appear outside mandate; and
- Calls not to consider additional measures for cloud computing resources.

In the light of the comments received, the ESAs introduced changes to the draft RTS. These changes related to e.g. the introduction of further proportionality, the removal of the article on governance from the general regime requirements, and clarification of provisions, especially those included in the articles related to network security, encryption, access control and business continuity aspects. ESAs concluded against the inclusion of cloud computing specific elements in order to comply with the principle of ensuring technology neutrality.

[1] The European Supervisory Authorities (2024), "Final report on Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554.

Instead, ESAs decided to broaden the considered requirements to cover ICT assets or services provided by ICT third party service providers in general. However, as regards the implementation deadlines, the ESAs did not consider any changes as these are set in DORA level 1.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Title I Chapter I establishes the main principle and elements to consider when developing and implementing the ICT security policies, procedures, protocols and tools (Article 1).

Title II Chapter II lays down the conditions for the further harmonisation of ICT risk management tools, methods, process and policies, establishing: general elements of ICT security policies, procedures, protocols and tools (section 1); specific elements of ICT security policies, procedures, protocols and tools (section 2): risk tolerance level, methodologies to conduct the ICT risk assessment, ICT risk treatment measures; a policy on management of ICT assets (section 3); a policy on encryption and cryptographic controls (section 4); an ICT operations security policy (section 5); a network security management policy (section 6); an ICT project management policy (section 7); a physical and environmental security policy to preserve the availability, authenticity, integrity and confidentiality of data (section 8). Chapter II establishes all the ICT security elements the financial entities shall include in the development of their human resources and access control policies. Chapter III establishes all the elements of an ICT-related incident detection and response policy financial entities shall develop and implement. Chapter IV establishes the content and the format of the report on the review of the ICT risk management framework the financial entities are required to prepare and submit.

Title III sets out a simplified ICT risk management framework, focusing on establishing a governance and control framework (chapter I); access and control mechanism and requirements (chapter II); establishing an ICT business continuity plan (chapter III); setting out the content and the format of the report on the review of the ICT risk management framework the financial entities are required to prepare and submit (chapter IV).

Title IV contains the final provisions on entry into force of the act (article 42).

COMMISSION DELEGATED REGULATION (EU) …/...

of 13.3.2024

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and 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[2], and in particular Article 15, fourth subparagraph, and Article 16(3), fourth subparagraph, thereof,

Whereas:

(1) Regulation (EU) 2022/2554 covers a wide variety of financial entities that differ in size, structure, internal organisation, and in the nature and complexity of their activities, and thus have increased or reduced elements of complexity or risks. To ensure that that variety is duly taken into account, any requirements as regards ICT security policies, procedures, protocols and tools, and as regards a simplified ICT risk management framework, should be proportionate to that size, structure, internal organisation, nature and complexity of those financial entities, and to the corresponding risks.

(2) For the same reason, financial entities subject to Regulation (EU) 2022/2554 should have a certain flexibility in the way they comply with any requirements as regards ICT security policies, procedures, protocols and tools, and as regards any simplified ICT risk management framework. For that reason, financial entities should be allowed to use any documentation they have already to comply with any documentation requirements that flow from those requirements. It follows that the development, documentation, and implementation of specific ICT security policies should be required only for certain essential elements, taking into account, *inter alia*, leading industry practices and standards. Furthermore, to cover specific technical implementation aspects, it is necessary to develop, document and implement ICT security procedures to cover specific technical implementation aspects, including

[2] 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, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

capacity and performance management, vulnerability and patch management, data and system security, and logging.

(3) To ensure the correct implementation over time of ICT security policies, procedures, protocols, and tools referred to in Title II, Chapter I of this Regulation, it is important that financial entities correctly assign and maintain any roles and responsibilities relating to ICT security, and that they lay down the consequences of non-compliance with ICT security policies or procedures.

(4) To limit the risk of conflicts of interests, financial entities should ensure the segregation of duties when assigning ICT roles and responsibilities.

(5) To ensure flexibility and to simplify the financial entities' control framework, financial entities should not be required to develop specific provisions on the consequences of non-compliance with ICT security policies, procedures and protocols referred to in Title II, Chapter I of this Regulation where such provisions are already set out in another policy or procedure.

(6) In a dynamic environment where ICT risks constantly evolve, it is important that financial entities develop their set of ICT security policies on the basis of leading practices, 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[3].This should enable financial entities referred to in Title II of this Regulation to remain informed and prepared in a changing landscape.

(7) To ensure their digital operational resilience, financial entities referred to in Title II of this Regulation should, as part of their ICT security policies, procedures, protocols, and tools, develop and implement an ICT asset management policy, capacity and performance management procedures, and policies and procedures for ICT operations. Those policies and procedures are necessary to ensure the monitoring of the status of ICT assets throughout their lifecycles, so that those assets are used and maintained effectively (ICT asset management). Those policies and procedures should also ensure the optimisation of ICT systems' operation and that the ICT systems' and capacity's performance meets the established business and information security objectives (capacity and performance management). Lastly, those policies and procedures should ensure the effective and smooth day-to-day management and operation of ICT systems (ICT operations), thereby minimising the risk of loss of confidentiality, integrity, and availability of data. Those policies and procedures are thus necessary to ensure the security of networks, to provide for adequate safeguards against intrusions and data misuse, and to preserve the availability, authenticity, integrity, and confidentiality of data.

(8) To ensure a proper management of the legacy ICT systems risk, financial entities should record and monitor end-dates of ICT third party support services. Because of the potential impact that a loss of confidentiality, integrity and availability of data may have, financial entities should focus on those ICT assets or systems that are critical for business operation when recording and monitoring those end-dates.

---

[3] 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, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(9) Cryptographic controls can ensure the availability, authenticity, integrity, and confidentiality of data. Financial entities referred to in Title II of this Regulation should therefore identify and implement such controls on the basis of a risk-based approach. To that end, financial entities should encrypt the data concerned at rest, in transit or, where necessary, in use, on the basis of the results of a two-pronged process, namely data classification and a comprehensive ICT risk assessment. Given the complexity of encrypting data in use, financial entities referred to in Title II of this Regulation should encrypt date in use only where that would be appropriate in light of the results of the ICT risk assessment. Financial entities referred to in Title II of this Regulation should, however, be able, where encryption of data in use is not feasible or is too complex, to protect the confidentiality, integrity, and availability of the data concerned 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. Financial entities referred to in Title II of this Regulation should hence follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, including threats from quantum advancements.

(10) ICT operations security and operational policies, procedures, protocols, and tools are essential to ensure the confidentiality, integrity, and availability of data. One pivotal aspect is the strict separation of ICT production environments from the environments where ICT systems are developed and tested or from other non-production environments. That separation should serve as an important ICT security measure against unintended and unauthorised access to, modifications of, and deletions of data in the production environment, which could result in major disruptions in the business operations of financial entities referred to in Title II of this Regulation. However, considering current ICT system development practices, in exceptional circumstances, financial entities should be allowed to test in production environments, provided that they justify such testing and obtain the required approval.

(11) The fast-evolving nature of ICT landscapes, ICT vulnerabilities and cyber threats necessitates a proactive and comprehensive approach to identifying, evaluating, and addressing ICT vulnerabilities. Without such an approach, financial entities, their customers, users, or counterparties may be severely exposed to risks, which would put at risk their digital operational resilience, the security of their networks, and the availability, authenticity, integrity, and confidentiality of data that ICT security policies and procedures should protect. Financial entities referred to in Title II of this Regulation should therefore identify and remedy vulnerabilities in their ICT environment, and both the financial entities and their ICT third-party service providers should adhere to a coherent, transparent, and responsible vulnerability management framework. For the same reason, financial entities should monitor ICT vulnerabilities using reliable resources and automated tools, verifying that ICT third-party service providers ensure prompt action on vulnerabilities in provided ICT services.

(12) Patch management should be a crucial part of those ICT security policies and procedures that, through testing and deployment in a controlled environment, are to resolve identified vulnerabilities and to prevent disruptions from the installation of patches.

(13) To ensure timely and transparent communication of potential security threats that could impact the financial entity and its stakeholders, financial entities should establish procedures for the responsible disclosure of ICT vulnerabilities to clients,

counterparts, and the public. When establishing those procedures, financial entities should consider factors, including the severity of the vulnerability, the potential impact of such vulnerability on stakeholders, and the readiness of a fix or mitigation measures.

(14) To allow for the assignment of user access rights, financial entities referred to in Title II of this Regulation should establish strong measures to ascertain the unique identification of individuals and systems that will access the financial entity's information. A failure to do so would expose financial entities to potential unauthorised 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 exceptionally be permitted under circumstances specified by financial entities, financial entities should ensure that the accountability for actions taken through those accounts is maintained. Without that safeguard, potential malicious users would be able to hinder investigative and corrective measures, leaving financial entities vulnerable to undetected malicious activities or non-compliance penalties.

(15) 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 to maintain data availability, authenticity, integrity, and confidentiality. Those ICT project management policies and procedures should identify the elements that are necessary to successfully manage ICT projects, including changes to, acquisitions of, the maintenance of, and developments of the financial entity's ICT systems, regardless of the ICT project management methodology chosen by the financial entity. In the context of those 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. To guarantee the secure implementation of an ICT project, financial entities should ensure that staff from specific business sectors or roles influenced or impacted by that ICT project can provide the necessary information and expertise. To ensure effective oversight, reports on ICT projects, in particular about projects that affect critical or important functions and about their associated risks, should be submitted to the management body. Financial entities should tailor the frequency and details of the systematic and ongoing reviews and reports to the importance and the size of the ICT projects concerned.

(16) It is necessary to ensure that software packages that financial entities referred to in Title II of this Regulation acquire and develop are effectively and securely integrated into the existing ICT environment, in accordance with established business and information security objectives. Financial entities should therefore thoroughly evaluate such software packages. For that purpose, and to identify vulnerabilities and potential security gaps within both software packages and the broader ICT systems, financial entities should carry out ICT security testing. To assess the integrity of the software and to ensure that the use of that software does not pose ICT security risks, financial entities should also review source codes of software acquired, including, where feasible, of proprietary software provided by ICT third-party service providers, using both static and dynamic testing methods.

(17) Changes, regardless of their scale, carry inherent risks and may pose significant risks of loss of confidentiality, integrity, and availability of data, and could thus lead to severe business disruptions. To safeguard financial entities from potential ICT vulnerabilities and weaknesses that could expose them to significant risks, a rigorous

verification process is necessary to confirm that all changes meet the necessary ICT security requirements. Financial entities referred to in Title II of this Regulation should therefore, as an essential element of their ICT security policies and procedures, have in place sound ICT change management policies and procedures. To uphold the objectivity and effectiveness of the ICT change management process, to prevent conflicts of interest, and to ensure that ICT changes are evaluated objectively, it is necessary to separate the functions responsible for approving those changes from the functions that request and implement those changes. To achieve effective transitions, controlled ICT change implementation, and minimal disruptions to the operation of the ICT systems, financial entities should assign clear roles and responsibilities that ensure that ICT changes are planned, adequately tested, and that quality is ensured. To ensure that ICT systems continue to operate effectively, and to provide a safety net for financial entities, financial entities should also develop and implement fall-back procedures. Financial entities should clearly identify those fall-back procedures and assign responsibilities to ensure a swift and effective response in the event of unsuccessful ICT changes.

(18) To detect, manage, and report ICT-related incidents, financial entities referred to in Title II of this Regulation should establish an ICT-related incident policy encompassing the components of an ICT-related incident management process. For that purpose, financial entities should identify all relevant contacts inside and outside the organisation that can facilitate the correct coordination and implementation of the different phases within that process. To optimise the detection of, and response to, ICT-related incidents, and to identify trends among those incidents, which are a valuable source of information enabling financial entities to identify and address root causes and problems in an effective manner, financial entities should in particular analyse in detail the ICT-related incidents that they consider to be most significant, *inter alia* because of their regular reoccurrence.

(19) To guarantee an early and effective detection of anomalous activities, financial entities referred to in Title II of this Regulation should collect, monitor, and analyse the different sources of information and should allocate related roles and responsibilities. As regards internal sources of information, logs are an extremely relevant source, but financial entities should not rely on logs alone. Instead, financial entities should consider broader information to include what is reported by other internal functions, as those functions are often a valuable source of relevant information. For the same reason, financial entities should analyse and monitor information gathered from external sources, including information provided by ICT third-party providers on incidents affecting their systems and networks, and other sources of information that financial entities consider relevant. In so far as such information constitutes personal data, the Union data protection law applies. The personal data should be limited to what is necessary for the incident detection.

(20) To facilitate ICT-related incidents detection, financial entities should retain evidence of those incidents. To ensure, on the one hand, that such evidence is retained sufficiently long and to avoid, on the other hand, an excessive regulatory burden, financial entities should determine the retention period considering, among other things, the criticality of the data and retention requirements stemming from Union law.

(21) To ensure that ICT-related incidents are detected in time, financial entities referred to in Title II of this Regulation should consider the criteria identified for triggering the detection of and responses to ICT-related incidents as not exhaustive. Moreover, while financial entities should consider each of those criteria, 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.

(22) When developing an ICT business continuity policy, financial entities referred to in Title II of this Regulation should take into account the essential components of ICT risk management, including ICT-related incident management and communication strategies, the ICT change management process, and risks associated with ICT third-party service providers.

(23) It is necessary to set out the set of scenarios that financial entities referred to in Title II of this Regulation should take into account both for the implementation of ICT response and recovery plans and for the testing of ICT business continuity plans. Those scenarios should serve as a starting point for financial entities to analyse both the relevance and plausibility of each scenario and the need to develop alternative scenarios. Financial entities should focus on those scenarios in which investment in resilience measures could be more efficient and effective. By testing switchovers between the primary ICT infrastructure and any redundant capacity, backups and redundant facilities, financial institutions should assess whether that capacity, backup, and those facilities operate effectively for a sufficient period of time and ensure that the normal functioning of the primary ICT infrastructure is restored in accordance with the recovery objectives.

(24) It is necessary to lay down requirements for operational risk, and more particularly requirements for ICT project and change management and ICT business continuity management building on those that apply already to central counterparties, central securities depositories and trading venues under, respectively, Regulations (EU) No 648/2012[4], (EU) No 600/2014[5] and (EU) No 909/2014[6] of the European Parliament and of the Council.

(25) Article 6(5) of Regulation (EU) 2022/2554 requires financial entities to review their ICT risk management framework and to provide their competent authority with a report on that review. To enable competent authorities to easily process the information in those reports, and to guarantee an adequate transmission of that information, financial entities should submit those reports in a searchable electronic format.

(26) The requirements for financial entities that are subject to the simplified ICT risk management framework referred to in Article 16 of Regulation (EU) 2022/2554 should be focused on those essential areas and elements that, in light of the scale, risk, size, and complexity of those financial entities, are as a minimum necessary to ensure the confidentiality, integrity, availability, and authenticity of the data and services of those financial entities. In that context, those financial entities should have in place an

---

4 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, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

5 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, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

6 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, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

internal governance and control framework with clear responsibilities to enable an effective and sound risk management framework. Furthermore, to reduce the administrative and operational burden, those financial entities should develop and document only one policy, that is an information security policy, that specifies the high-level principles and rules necessary to protect the confidentiality, integrity, availability, and authenticity of data and of the services of those financial entities.

(27) 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 that Regulation. To ensure coherence between the ordinary and the simplified ICT risk management framework, and considering that those provisions should become applicable at the same time, it is appropriate to include those provisions in a single legislative act.

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

(29) 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[7], in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council[8] and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[9] has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential costs and benefits of the proposed standards and requested advice 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.

(30) To the extent to which processing of personal data is required to comply with the obligations set out in this Act, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 should fully apply. For instance, the data minimisation principle should be complied with where personal data are collected

---

7 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

8 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

9 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

to ensure an appropriate incident detection. The European Data Protection Supervisor has also been consulted on the draft text of this Act,

HAS ADOPTED THIS REGULATION:

TITLE I
GENERAL PRINCIPLE

Article 1
Overall risk profile and complexity

When developing and implementing the ICT security policies, procedures, protocols and tools referred to in Title II and the simplified ICT risk management framework referred to in Title III, the size and the overall risk profile of the financial entity, and the nature, scale and elements of increased or reduced complexity of its services, activities and operations shall be taken into account, including elements relating to:

(a) encryption and cryptography;

(b) ICT operations security;

(c) network security;

(d) ICT project and change management;

(e) 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 1

Article 2
General elements of ICT security policies, procedures, protocols, and tools

1. Financial entities shall ensure that their ICT security policies, information security, and related procedures, protocols, and tools as referred to in Article 9(2) of Regulation (EU) 2022/2554 are embedded in their ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols, and tools laid down in this Chapter that:

   (a) ensure the security of networks;

   (b) contain safeguards against intrusions and data misuse;

   (c) preserve the availability, authenticity, integrity, and confidentiality of data, including via the use of cryptographic techniques;

   (d) guarantee an accurate and prompt data transmission without major disruptions and undue delays.

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

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

   (b) indicate the date of the formal approval of the ICT security policies by the management body;

   (c) contain indicators and measures to:

      (i) monitor the implementation of the ICT security policies, procedures, protocols, and tools;

      (ii) record exceptions from that implementation

      (iii) ensure that the digital operational resilience of the financial entity is ensured in case of exceptions as referred to in point (ii);

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

(e) specify the consequences of non-compliance by staff of the financial entity with the ICT security policies, where provisions to that effect are not laid down in other policies of the financial entity;

(f) list the documentation to be maintained;

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

(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 development, implementation and maintenance of ICT security policies, procedures, protocols, and tools;

(j) are reviewed in accordance with 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, to the cyber threat landscape, or to applicable legal obligations.

SECTION 2

Article 3
ICT risk management

Financial entities shall develop, document, and implement ICT risk management policies and procedures that shall contain all of the following:

(a) an indication of the approval of the risk tolerance level for ICT risk established in accordance with Article 6(8), point (b), of Regulation (EU) 2022/2554;

(b) a procedure and a methodology to conduct the ICT risk assessment, identifying:

(i) vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions;

(ii) the quantitative or qualitative indicators to measure the impact and likelihood of the vulnerabilities and threats referred to in point (i);

(c) the procedure to identify, implement, and document ICT risk treatment measures for the ICT risks identified and assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance level referred to in point (a);

(d) for the residual ICT risks that are still present following the implementation of the ICT risk treatment measures referred to in point (c):

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

(ii) the assignment of roles and responsibilities regarding:

(1) the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level referred to in point (a);

(2) for the review process referred to in point (iv) of this point (d);

(iii) the development of an inventory of the accepted residual ICT risks, including a justification for their acceptance;

(iv) provisions on the review of the accepted residual ICT risks at least once a year, including:

(1) the identification of any changes to the residual ICT risks;

(2) the assessment of available mitigation measures;

(3) 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:

(i) any changes to the ICT risk and cyber threat landscape;

(ii) internal and external vulnerabilities and threats:

(iii) ICT risk of the financial entity that enables promp detection of changes that could affect its ICT risk profile;

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

For the purposes of the first paragraph, point (c), the procedure referred to in that point shall ensure:

(a) the monitoring of the effectiveness of the ICT risk treatment measures implemented;

(b) the assessment of whether the established risk tolerance levels of the financial entity have been attained;

(c) the assessment of whether the financial entity has taken actions to correct or improve those measures where necessary.

SECTION 3
ICT ASSET MANAGEMENT

Article 4
ICT asset management policy

1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on management of ICT assets.

2. The policy on management of ICT assets referred to in paragraph 1 shall:

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

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

(i) the 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 referred to in Article 8(1) of Regulation (EU) 2022/2254;

(iv) the identity of ICT asset owners;

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

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

(vii) whether the ICT asset can 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 those ICT assets are no longer supported by their supplier or by an ICT third-party service provider;

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

Article 5
ICT asset management procedure

1. Financial entities shall develop, document, and implement a procedure for the management of ICT assets.

2. The procedure for management of ICT assets referred to in paragraph 1 shall specify the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. That assessment shall take into account:

(a) the ICT risk related to those business functions and their dependencies on the information assets or ICT assets;

(b) how the loss of confidentiality, integrity, and availability of such information assets and ICT assets would impact the business processes and activities of the financial entities.

SECTION 4
ENCRYPTION AND CRYPTOGRAPHY

Article 6
Encryption and cryptographic controls

1. As part of their ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on encryption and cryptographic controls.

2. Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following:

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

(b) the encryption of data in use, where necessary;

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

(d) the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys.

For the purposes of point (b), where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment, or take equivalent measures to ensure the confidentiality, integrity, authenticity, and availability of data.

3. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 criteria for the selection of 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 in accordance with Article 8(1) of Regulation (EU) 2022/2554. Financial entities that are not able to adhere to the leading practices or standards, or to use the most reliable techniques, shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

4. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 provisions for updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis. Those updates or changes shall ensure that the cryptographic technology remains resilient against cyber threats, as required by Article 10(2), point (a). Financial entities that are not able to update or change the cryptographic technology shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

5. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 a requirement 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 include in the cryptographic key management policy referred to in Article 6(2), point (d), requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking, and destroying those cryptographic keys.

2. Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure, and modification. Financial entities shall design those controls on the basis of the results of the approved data classification and the ICT risk assessment.

3. Financial entities shall develop and implement methods to replace the cryptographic keys in the case of loss, or where those keys are compromised or damaged.

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. Financial entities shall keep that register up to date.

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

SECTION 5
ICT OPERATIONS SECURITY

Article 8
Policies and procedures for ICT operations

1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement policies and procedures to manage the ICT operations. Those policies and procedures shall specify 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 contain all of the following:

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

      (i) requirements regarding secure installation, maintenance, configuration, and deinstallation of an ICT system;

      (ii) requirements regarding the management of information assets used by ICT assets, including their processing and handling, both automated and manual;

      (iii) requirements regarding the identification and control of legacy ICT systems;

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

      (i) backup and restore requirements of ICT systems;

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

      (iii) protocols for audit-trail and system log information;

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

      (v) requirements on the separation of ICT production environments from the development, testing, and other non-production environments;

      (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;

   (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.

   For the purposes of point (b)(v), the separation shall consider all of the components of the environment, including accounts, data or connections, as required by Article 13(1), point (a).

For the purposes of point (b)(vii), the policies and procedures referred to in paragraph 1 shall provide that the instances in which testing is performed in a production environment are clearly identified, reasoned, are for limited periods of time, and are approved by the relevant function in accordance with Article 16(6). Financial entities shall ensure the availability, confidentiality, integrity, and authenticity of ICT systems and production data during development and test activities in the production environment.

Article 9
Capacity and performance management

1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement capacity and performance management procedures for the following:

   (a) the identification of capacity requirements of their ICT systems;

   (b) the application of resource optimisation;

   (c) the monitoring procedures for maintaining and improving:

      (i) the availability of data and ICT systems;

      (ii) the efficiency of ICT systems;

      (iii) the prevention of ICT capacity shortages.

2. The capacity and performance management procedures referred to in paragraph 1 shall ensure that financial entities take measures that are appropriate to cater for the specificities of ICT systems with long or complex procurement or approval processes or ICT systems that are resource-intensive.

Article 10
Vulnerability and patch management

1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement vulnerability management procedures.

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, whereby the frequency and scope of those activities shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset;

   (c) verify whether:

      (i) ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity;

      (ii) whether those service providers report to the financial entity at least the critical vulnerabilities and statistics and trends in a timely manner;

   (d) track the usage of:

(i) third-party libraries, including open-source libraries, used by ICT services supporting critical or important functions;

(ii) ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider;

(e) establish procedures for the responsible disclosure of vulnerabilities to clients, counterparties, and to the public;

(f) prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified;

(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.

For the purposes of point (b), financial entities shall perform the automated vulnerability scanning and assessments on ICT assets for the ICT assets supporting critical or important functions on at least a weekly basis.

For the purposes of point (c), financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes, and implement appropriate mitigating action.

For the purposes of point (d), financial entities shall, where appropriate in collaboration with the ICT third-party service provider, 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, financial entities shall track the usage to the extent possible of third-party libraries, including open-source libraries.

For the purposes of point (f), financial entities shall consider the criticality of the vulnerability, the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554, and the risk profile of the ICT assets affected by the identified vulnerabilities.

3. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document and implement patch management procedures.

4. The patch management procedures referred to in paragraph 3 shall:

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

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

(c) test and deploy the software and hardware patches and the updates referred to in Article 8(2), points (b)(v), (vi) and (vii);

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

Article 11
Data and system security

1. As part of the ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a data and system security procedure.

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

   (a) the access restrictions referred to in Article 21 of this Regulation, supporting the protection requirements for each level of classification;

   (b) the identification of a secure configuration baseline for ICT assets that minimise exposure of those ICT assets to cyber threats and measures to verify regularly that those baselines are effectively deployed;

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

   (d) the identification of security measures against malicious codes;

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

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

      (i) the requirement to use a management solution to remotely manage the endpoint devices and remotely wipe the financial entity's data;

      (ii) the requirement to use security mechanisms that cannot be modified, removed or bypassed by staff members or ICT third-party service providers in an unauthorised manner;

      (iii) the requirement 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(1), point (a);

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

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

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

   (k) for 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.

For the purposes of point (b), the secure configuration baseline referred to in that point shall take into account leading practices and appropriate techniques laid down in the standards defined in Article 2, point (1), of Regulation (EU) No 1025/2012.

For the purposes of point (k), financial entities shall consider the following:

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

(b) a 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 over its ICT third-party service provider referred to in Article 28(1), point (a), of Regulation (EU) 2022/2554, and for financial entities referred to in Article 28(2) of that Regulation, and in accordance with the financial entity's policy on the use of ICT services supporting critical or important functions;

(c) the need to ensure and maintain adequate competences within the financial entity in the management and security of the service used;

(d) 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. Financial entities shall, as part of the safeguards against intrusions and data misuse, develop, document, and implement logging procedures, protocols and tools.

2. The logging procedures, protocols, and tools referred to in paragraph 1 shall contain 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;

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

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

(i) logical and physical access control, as referred to in Article 21, and identity management;

(ii) capacity management;

(iii) change management;

(iv) ICT operations, including ICT system activities;

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

(d) 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 a failure of logging systems;

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

For the purposes of point (a), financial entities shall establish the retention period, 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.

SECTION 6
NETWORK SECURITY

Article 13
Network security management

1. Financial entities shall, as part of the safeguards ensuring the security of networks against intrusions and data misuse, develop, document, and implement policies, procedures, protocols, and tools on network security management, including all of the following:

(a) the segregation and segmentation of ICT systems and networks taking into account:

(i) the criticality or importance of the function those ICT systems and networks support;

(ii) the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554;

(iii) the overall risk profile of ICT assets using those ICT systems and networks;

(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, the results of the ICT risk assessment and the encryption of network connections referred to in Article 6(2);

(f) the design of networks in line with the ICT security requirements established by the financial entity, 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 specification, implementation, approval, change, and review of firewall rules and connections filters;

(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 the hardening of the network and of network devices in line with any vendor instructions, 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 specified period of inactivity;

(m) for network services agreements:

(i) the identification and specification of ICT and information security measures, service levels, and management requirements of all network services;

(ii) whether those services are provided by an ICT intra-group service provider or by ICT third-party service providers.

For the purposes of point (h), financial entities shall perform the review of firewall rules and connections filters on a regular basis in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of ICT systems involved. For ICT systems that support critical or important functions, financial entities shall verify the adequacy of the existing firewall rules and connection filters at least every 6 months.

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. Financial entities shall in particular ensure all of the following:

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

(b) the prevention and detection of data leakages 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. Financial entities shall design the policies, procedures, protocols, and tools to protect the information in transit referred to in paragraph 1 on the basis of the results of the approved data classification and of the ICT risk assessment.

SECTION 7
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 referred to in paragraph 1 shall specify the elements that 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 referred to in paragraph 1 shall contain all of the following:

   (a) ICT project objectives;

   (b) ICT project governance, including roles and responsibilities;

   (c) ICT project planning, timeframe, and steps;

   (d) ICT project risk assessment;

   (e) relevant milestones;

   (f) change management requirements;

   (g) the 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 referred to in paragraph 1 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. In accordance with the ICT project risk assessment referred to in paragraph 3, point (d), the ICT project management policy referred to in paragraph 1 shall provide that the establishment and progress of ICT projects impacting critical or important functions of the financial entity and their associated risks are reported to the management body as follows:

   (a) individually or in aggregation, depending on the importance and size of the ICT projects;

   (b) periodically and, where necessary, on an event-driven basis.

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. That policy shall:

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

(b) require the identification of:

(i) technical specifications and ICT technical specifications, as defined in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012;

(ii) requirements relating to the 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 in accordance with the financial entity's internal governance arrangements;

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

2. Financial entities shall develop, document, and implement an ICT systems' acquisition, development, and maintenance procedure for the testing and approval of 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 business procedures and ICT assets concerned. 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.

Central counterparties shall, in addition to the requirements laid down in the first subparagraph, involve, as appropriate, in the design and conduct of the testing referred to in the first subparagraph:

(a) clearing members and clients;

(b) interoperable central counterparties;

(c) other interested parties.

Central securities depositories shall, in addition to the requirements laid down in the first subparagraph, involve, as appropriate, in the design and conduct of the testing referred to in the first subparagraph:

(a) users;

(b) critical utilities and critical service providers;

(c) other central securities depositories;

(d) other market infrastructures;

(e) any other institutions with which central securities depositories have identified interdependencies in their business continuity policy.

3. The procedure referred to in paragraph 2 shall contain the performance of source code reviews covering both static and dynamic testing. That testing shall contain security testing for internet-exposed systems and applications in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall:

(a) identify and analyse vulnerabilities and anomalies in the source code;

(b) adopt an action plan to address those vulnerabilities and anomalies;

(c) monitor the implementation of that action plan.

4. The procedure referred to in paragraph 2 shall contain security testing of software packages no later than at the integration phase, in accordance with Article 8(2), points (b)(v), (vi) and(vii).

5. The procedure referred to in paragraph 2 shall provide that:

   (a) non-production environments only store anonymised, pseudonymised, or randomised production data;

   (b) financial entities are to protect the integrity and confidentiality of data in non-production environments.

6. By way of derogation from paragraph 5, the procedure referred to in paragraph 2 may provide that production data are stored only for specific testing occasions, for limited periods of time, and following the approval by the relevant function and the reporting of such occasions to the ICT risk management function.

7. The procedure referred to in paragraph 2 shall contain the implementation of 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.

8. The procedure referred to in paragraph 2 shall provide that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, are to be analysed and tested in accordance with paragraph 3 prior to their deployment in the production environment.

9. Paragraph 1 to 8 of 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 include in the ICT change management procedures referred to in Article 9(4), point (e), of Regulation (EU) 2022/2554, in respect of all changes to software, hardware, firmware components, systems, or security parameters, all of the following elements:

   (a) a verification of whether the ICT security requirements have been met;

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

   (c) a clear description of the roles and responsibilities to ensure that:

      (i) changes are specified and planned;

      (ii) an adequate transition is designed;

      (iii) the changes are tested and finalised in a controlled manner;

      (iv) there is an effective quality assurance;

   (d) the documentation and communication of change details, including:

      (i) the purpose and scope of the change;

      (ii) the timeline for the implementation of the change;

      (iii) the expected outcomes;

(e) the 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 emergency changes after their implementation, including workarounds and patches;

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

2. After having made significant changes to their ICT systems, central counterparties and central securities depositories shall submit their ICT systems to stringent testing by simulating stressed conditions.

Central counterparties shall involve, as appropriate, in the design and conduct of the testing referred to in the first subparagraph:

(a) clearing members and clients;

(b) interoperable central counterparties;

(c) other interested parties;

Central securities depositories shall, as appropriate, involve in the design and conduct of the testing referred to in the first subparagraph:

(a) users;

(b) critical utilities and critical service providers;

(c) other central securities depositories;

(d) other market infrastructures;

(e) any other institutions with which central securities depositories have identified interdependencies in their ICT business continuity policy.

SECTION 8

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 specify, document, and implement a physical and environmental security policy. Financial entities shall design that policy i light of the cyber threat landscape, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554, and in light of the overall risk profile of ICT assets and accessible information assets.

2. The physical and environmental security policy referred to in paragraph 1 shall contain 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 from attacks, accidents, and environmental threats and hazards, the premises, data centres of the financial entity, and sensitive

designated areas identified by the financial entity, where ICT assets and information assets reside;

(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;

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

(e) measures to preserve the availability, authenticity, integrity, and confidentiality of the data, including:

(i) a clear desk policy for papers;

(ii) a clear screen policy for information processing facilities.

For the purposes of point (b), 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 therein.

For the purposes of point (c), the physical and environmental security policy referred to in paragraph 1 shall contain measures to provide appropriate protection to unattended ICT assets.

Chapter II
HUMAN RESOURCES POLICY AND ACCESS CONTROL

Article 19
Human resources policy

Financial entities shall include in their human resource policy or other relevant policies all of the following ICT security related elements:

(a) the 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 detection of anomalous behaviour, including, where applicable, the reporting channels established in line with Directive (EU) 2019/1937 of the European Parliament and of the Council[10];

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

[10] 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, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

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 that 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. The identity management policies and procedures referred to in paragraph 1 shall contain all of the following:

   (a) without prejudice to Article 21(1), point (c), a unique identity corresponding to a unique user account shall be assigned to each staff member of the financial entity or staff of the ICT third-party service providers accessing the information assets and ICT assets of the financial entity;

   (b) a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation, and termination of all accounts.

   For the purposes of point (a), financial entities shall maintain records of all identity assignments. Those 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 laid down in applicable Union and national law.

   For the purposes of point (b), financial entities shall, where feasible and appropriate, deploy automated solutions for the lifecycle identity management process.

Article 21
Access control

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

(a) the 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) the 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) a 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) a 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, including provision on all of the following:

   (i) assignment of roles and responsibilities for granting, reviewing, and revoking access rights;

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

(iii) withdrawal of access rights without undue delay upon termination of the 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 6 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 in accordance with 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 ICT assets that are publicly accessible;

(g) physical access controls measures including:

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

(ii) the granting of physical access rights to critical ICT assets to authorised persons only, in accordance with the need-to-know and least privilege principles, and on an ad-hoc basis;

(iii) the 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;

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

For the purposes of point (e)(i), financial entities shall establish the retention period taking into account the business and information security objectives, the reasons for recording the event in the logs, and the results of the ICT risk assessment.

For the purposes of point (e)(ii), financial entities shall, where possible, use dedicated accounts for the performance of administrative tasks on ICT systems. Where feasible and appropriate, financial entities shall deploy automated solutions for the privilege access management.

For the purposes of point (g)(i), the 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 therein.

For the purposes of point (g)(iii), the monitoring shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the criticality of the area accessed.

CHAPTER III
ICT-RELATED INCIDENT DETECTION AND RESPONSE

Article 22
ICT-related incident management policy

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:

  (i) the detection and monitoring of cyber threats;

  (ii) the detection of anomalous activities;

  (iii) 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 of this Regulation;

(d) retain all evidence relating to ICT-related incidents for a period that shall be no longer than necessary for the purposes for which the data are 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][11] and with any applicable retention requirement pursuant to Union law;

(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.

For the purposes of point (d), financial entities shall retain the evidence referred to in that point in a secure manner.

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. The mechanism to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, as referred to in Article 10(1) of Regulation (EU) 2022/2554, shall enable financial entities to:

  (a) collect, monitor, and analyse all of the following:

[11] (OP: Please insert [reference and title to this CDR])

(i) internal and external factors, including at least the logs collected in accordance with Article 12 of this Regulation, 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 that 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;

(c) prioritise the alerts referred to in point (b) to allow for the management of the detected ICT-related incidents within the expected resolution time, as specified 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.

For the purposes of point (b), the tools referred to in that point shall contain the tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and integrity of the data sources or log collection.

3. Financial entities shall protect any recording of the anomalous activities against tampering and unauthorised access at rest, in transit and, where relevant, in use.

4. Financial entities shall log all relevant information for each detected anomalous activity enabling:

(a) the identification of the date and time of occurrence of the anomalous activity;

(b) the identification of the date and time of detection of the anomalous activity;

(c) the identification of the type of the anomalous activity.

5. Financial entities shall consider all of the following criteria to trigger the ICT-related incident detection and response processes referred to in Article 10(2) of Regulation (EU) 2022/2554:

(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. For the purposes of paragraph 5, financial entities shall also 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 referred to in Article 11(1) of Regulation (EU) 2022/2554 all of the following:

(a) a description of:

(i) the objectives of the ICT business continuity policy, 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;

(ii) the scope of the ICT business continuity arrangements, plans, procedures, and mechanisms, including limitations and exclusions;

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

(iv) the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans, and crisis communications plans;

(b) provisions on:

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

(ii) the alignment between the ICT business continuity plans and the overall business continuity plans, concerning at least all of the following:

(1) potential failure scenarios, including the scenarios referred to in Article 26(2) of this Regulation;

(2) 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;

(iii) the development of ICT business continuity plans for severe business disruptions as part of those plans, and the prioritisation of ICT business continuity actions using a risk-based approach;

(iv) the development, testing and review of ICT response and recovery plans, in accordance with Articles 25 and 26 of this Regulation;

(v) the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26 of this Regulation;

(vi) the alignment of the ICT business continuity policy to:

(1) the communication policy referred to in Article 14(2) of Regulation (EU) 2022/2554;

(2) 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) contains a maximum recovery time for their critical functions that is not longer than 2 hours;

(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 critical or important functions of the central counterparty based on disaster scenarios;

(ii) maintain a secondary processing site capable of ensuring continuity of critical or important functions of the central counterparty identical to 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 where 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.

For the purposes of point (a), central counterparties shall complete end of day procedures and payments on the required time and day in all circumstances.

For the purposes of point (c)(i), arrangements referred to in that point shall address the availability of adequate human resources, the maximum downtime of critical functions, and fail over and recovery to a secondary site.

For the purposes of point (c)(ii), the secondary processing site referred to in that point shall have a geographical risk profile which is distinct from that of the primary site.

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 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 2 hours.

4. In addition to the requirements referred to in paragraph 1, trading venues shall ensure that their ICT business continuity policy ensures that:

(a) trading can be resumed within or close to 2 hours of a disruptive incident;

(b) the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is close to zero.

Article 25
Testing of the ICT business continuity plans

1. When testing the ICT business continuity plans in accordance with Article 11(6), of Regulation (EU) 2022/2554, financial entities shall take into account the financial entity's business impact analysis (BIA) and the ICT risk assessment referred to in Article 3(1), point (b), of this Regulation.

2. Financial entities shall assess through the testing of their ICT business continuity plans referred to in paragraph 1 whether they are able to ensure the continuity of the financial entity's critical or important functions. That testing shall:

   (a) be performed on the basis of test scenarios that simulate potential disruptions, including an adequate set of severe but plausible scenarios;

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

   (c) for financial entities, other than microenterprises, as referred to in Article 11(6), second subparagraph, of Regulation (EU) 2022/2554, contain scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities;

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

   (e) contain procedures to verify the ability of the financial entities' staff, of ICT third-party service providers, of ICT systems, and ICT services to respond adequately to the scenarios duly taken into account in accordance with Article 26(2).

   For the purposes of point (a), financial entities shall always include in the testing the scenarios considered for the development of the business continuity plans.

   For the purposes of point (b), financial entities shall duly consider scenarios linked to insolvency or failures of the ICT third-party service providers or linked to political risks in the ICT third-party service providers' jurisdictions, where relevant.

   For the purposes of point (c), 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.

3. In addition to the requirements referred to in paragraph 2, central counterparties shall involve in the testing of their ICT business continuity plans referred to in paragraph 1:

   (a) clearing members;

   (b) external providers;

   (c) relevant institutions in the financial infrastructure with which central counterparties have identified interdependencies in their business continuity policies.

4. In addition to the requirements referred to in paragraph 2, central securities depositories shall involve in the testing of their ICT business continuity plans referred to in paragraph 1, as appropriate:

(a) users of the central securities depositories;

(b) critical utilities and critical service providers;

(c) other central securities depositories;

(d) other market infrastructures;

(e) any other institutions with which central securities depositories have identified interdependencies in their business continuity policy.

5. Financial entities shall document the results of the testing referred to in paragraph 1. Any identified deficiencies resulting from that testing shall be analysed, addressed, and reported to the management body.

Article 26
ICT response and recovery plans

1. When developing the ICT response and recovery plans referred to in Article 11(3) of Regulation (EU) 2022/2554, financial entities shall take into account the results of the financial entity's business impact analysis (BIA). Those ICT response and recovery plans shall:

(a) specify the conditions prompting their activation or deactivation, and any exceptions for such activation or deactivation;

(b) describe what actions are to 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 entity;

(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 the execution of ICT response and recovery plans and be readily accessible in case of emergency;

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

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

For the purposes of point (d), financial entities shall clearly specify roles and responsibilities.

2. The ICT response and recovery plans referred to in paragraph 1 shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. Those 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, pandemics, and physical attacks, including intrusions and terrorist attacks;

(g) insider attacks;

(h) political and social instability, including, where relevant, in the ICT third-party service provider's jurisdiction and the location where the data are stored and processed;

(i) widespread power outages.

3. Where the primary recovery measures may not be feasible in the short term because of costs, risks, logistics, or unforeseen circumstances, the ICT response and recovery plans referred to in paragraph 1 shall consider alternative options.

4. As part of the ICT response and recovery plans referred to in paragraph 1, 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 of the financial entity.

CHAPTER V
REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW

Article 27

Format and content of the report on the review of the ICT risk management framework

1. Financial entities shall submit the report on the review of the ICT risk management framework 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 referred to in paragraph 1:

(a) an introductory section that:

(i) clearly identifies the financial entity that is 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 submitted;

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

(c) a description of the reason for the review of the ICT risk management framework in accordance with Article 6(5) of Regulation (EU) 2022/2554.;

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

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

(f) a description of the major changes and improvements to the ICT risk management framework since the previous review;

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

(i) a summary of measures taken to remediate to identified weaknesses, deficiencies and gaps;

(ii) an expected date for implementing the measures and dates related to the internal control of the implementation, including information on the state of progress of the implementation of those measures 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 the identification of the function responsible for carrying out the measures, detailing whether the tools and functions are internal or external;

(iv) a 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 any corrective measures;

(v) information on the process for informing the competent authority, where appropriate;

(vi) where the weaknesses, deficiencies, or gaps identified are not subject to corrective measures, a detailed explanation of the criteria used to analyse the impact of those weaknesses, deficiencies, or gaps, to evaluate the related residual ICT risk, and of the criteria used to accept the related residual risk;

(i) information on planned further developments of the ICT risk management framework;

(j) conclusions resulting from the review of the ICT risk management framework;

(k) information on past reviews, including:

(i) a list of past reviews to date;

(ii) where applicable, a state of implementation of the corrective measures identified by the last report;

(iii) where the proposed corrective measures in past reviews have proven ineffective or have created unexpected challenges, a description of how those corrective measures could be improved or of those unexpected challenges;

(l) sources of information used in the preparation of the report, including all of the following:

(i) for financial entities other than microenterprises as referred to in Article 6(6) of Regulation (EU) 2022/2554, the results of internal audits;

(ii) the results of compliance assessments;

(iii) results of digital operational resilience testing, and where applicable the results of advanced testing, based on threat-led penetration testing (TLPT), of ICT tools, systems, and processes;

(iv) external sources.

For the purposes of point (c), 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 instructions or conclusions, 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.

For the purposes of point (f), the description shall contain 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.

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. The 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. The financial entities referred to in paragraph 1 shall, as part of their simplified ICT risk management framework, ensure that their management body:

   (a) bears the overall responsibility for ensuring that the simplified ICT risk management framework allows for the achievement of the financial entity's business strategy in accordance with the risk appetite of that financial entity, and ensures that ICT risk is considered in that 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:

      (i) the classification of information assets of the financial entity as referred to in Article 30(1) of this Regulation, the list of main risks identified, and the business impact analysis and related policies;

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

   (e) allocates and reviews at least once a year the budget necessary 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) specifies and implements the policies and 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. The 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, financial entities shall remain fully responsible for the verification of compliance with the ICT risk management requirements.

4. The financial entities referred to in paragraph 1 shall ensure an appropriate segregation and the independence of control functions and internal audit functions.

5. The financial entities referred to in paragraph 1 shall ensure that their simplified ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. The auditors shall have sufficient knowledge, skills, and expertise in ICT risk, and shall be independent. 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, the 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. The 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 simplified ICT risk management framework. That information security policy shall specify the high-level principles and rules to protect the confidentiality, integrity, availability, and authenticity of data and of the services those financial entities provide.

2. Based on their information security policy referred to in paragraph 1, the 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.

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 simplified ICT risk management framework referred to in Article 16(1), point (a), of Regulation (EU) 2022/2554, the financial entities referred to in paragraph 1 of that Article 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 that identification and classification as needed.

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

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

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

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

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

   (e) the identification and assessment of any ICT and information security risks resulting from any major change in ICT system or ICT services, processes, or procedures, and from ICT security testing results and after any major ICT-related incident.

2. The financial entities referred to in paragraph 1 shall carry out and document the ICT risk assessment periodically commensurate to the financial entities' ICT risk profile.

3. The financial entities referred to in paragraph 1 shall continuously monitor threats and vulnerabilities that are relevant to their critical or important functions, and information assets and ICT assets, and shall regularly review the risk scenarios impacting those critical or important functions.

4. The financial entities referred to in paragraph 1 shall set out alert thresholds and criteria to trigger and initiate ICT-related incident response processes.

Article 32
Physical and environmental security

1. The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify and implement physical security measures designed on the basis of the threat landscape and in accordance with the classification referred to in Article 30(1) of this Regulation, the overall risk profile of ICT assets, and accessible information assets.

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

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

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

Article 33
Access Control

1. The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document, and implement procedures for the control of logical and physical access and shall enforce, monitor, and periodically review those procedures. Those procedures shall contain the following elements of control of logical and physical access:

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

   (b) user accountability, which ensures 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;

   (d) authentication methods that are commensurate to the classification referred to in Article 30(1) and to the overall risk profile of ICT assets, and which are based on leading practices;

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

   For the purposes of point (c), the financial entity shall assign privileged, emergency, and administrator access on a need-to-use or an *ad-hoc* basis for all ICT systems, and shall be logged in accordance with Article 34(1), point (f).

   For the purposes of point (d), financial entities shall use strong authentication methods that are based on 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.

Article 34
ICT operations security

The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall, as part of their systems, protocols, and tools, and for all ICT assets:

(a) monitor and manage the lifecycle of all ICT assets;

(b) monitor whether the ICT assets are supported by ICT third-party service providers of financial entities, where applicable;

(c) identify capacity requirements of their ICT assets 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 as referred to in Article 30(1) and to the overall risk profile of the ICT asset, and deploy patches to address identified vulnerabilities;

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

(f) log events related to logical and physical access control, ICT operations, including system and network traffic activities, and ICT change management;

(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 check for corresponding new security updates.

For the purposes of point (f), financial entities shall align the level of detail of the logs with their purpose and usage of the ICT asset producing those logs.

Article 35
Data, system and network security

The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall, as part of their systems, protocols, and tools, develop and implement safeguards that ensure the security of networks against intrusions and data misuse and that preserve the availability, authenticity, integrity, and confidentiality of data. In particular, financial entities shall, taking into account the classification referred to in Article 30(1) of this Regulation, establish all of the following:

(a) the identification and implementation of measures to protect data in use, in transit, and at rest;

(b) the identification and implementation of security measures regarding the use of software, data storage media, systems and endpoint devices that transfer and store data of the financial entity;

(c) the 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) the identification and implementation of measures that ensure the availability, authenticity, integrity, and confidentiality of data during network transmissions;

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

(f) a process to securely dispose of, or decommission, data storage devices on premises, or data storage devices that are stored externally, that contain confidential information;

(g) the identification and 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. The 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, 34 and 35 and Articles 37 and 38 of this Regulation. Financial entities shall ensure that that plan considers threats and vulnerabilities identified as part of the simplified ICT risk management framework referred to in Article 31 of this Regulation.

2. The financial entities referred to in paragraph 1 shall review, asses and test ICT security measures, taking into consideration the overall risk profile of the ICT assets of the financial entity.

3. The 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

The 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. That procedure 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 specified and approved by the business function concerned;

(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. The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document, and implement an ICT project management procedure and shall specify the roles and responsibilities for its implementation. That procedure shall cover all stages of the ICT projects from their initiation to their closure.

2. The 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. The 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 referred to in paragraph 1 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 for their execution;

   (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 ICT business continuity plans and what actions are to 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;

   (g) identify backup procedures and measures that specify the scope of the data that are 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.

   For the purposes of point (f), the measures referred to in that point shall provide for the mitigation of failures of critical third-party providers.

Article 40
Testing of business continuity plans

1. The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall test their business continuity plans referred to in Article 39 of this Regulation, including the scenarios referred to in that Article, 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 business continuity plans referred to in paragraph 1 shall demonstrate that the financial entities referred to in that paragraph are able to sustain the viability of their businesses until critical operations are re-established and identify any deficiencies in those plans.

3. The financial entities referred to in paragraph 1 shall document the results of the testing of business continuity plans and any identified deficiencies resulting from that testing shall be analysed, addressed, and reported to the management body.

CHAPTER IV
REPORT ON THE REVIEW OF THE SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK

Article 41
Format and content of the report on the review of the simplified ICT risk management framework

1. The financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall submit the report on the review of the ICT risk management framework referred to in paragraph 2 of that Article in a searchable electronic format.

2. The report referred to in paragraph 1 shall contain 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, the financial entity’s organisation, identified critical functions, strategy, major ongoing projects or activities, and relationships, and the financial entity’s 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 summary of the major changes in the ICT risk management framework since the previous report;

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

   (b) where applicable, the 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) where the review has been initiated following supervisory instructions, evidence of such instructions;

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

(d) the 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 simplified ICT risk management framework, and the expected date for implementing those measures, including the follow-up on weaknesses, deficiencies, and gaps identified in previous reports, where those weaknesses, deficiencies, and gaps have not yet been remedied;

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

TITLE IV – FINAL PROVISIONS

Article 42
Entry into force

This Regulation shall enter into force on the twentieth day following that of 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, 13.3.2024

For the Commission
The President
Ursula VON DER LEYEN