

**DORA**  
(Digital Operational Resilience Act)

July 2024





*This brochure contains:*

*The Digital Operational Resilience Act ("**DORA**") (i.e. 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) together with:*

- *Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities;*
- *Commission Delegated Regulation (EU) 2024/1505 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid;*
- *Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents;*
- *Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers;*
- *Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework*

*(the "**Commission Delegated Regulations**");*

- *Draft Implementing Technical Standards from the Final Report on Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554 (JC 2023 85 – published on 10 January 2024);*
- *RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyberthreats;*
- *RTS on subcontracting of critical or important functions (The ESAs indicated in their press release of 17 July 2024 that these RTS will be published in due course);*
- *RTS on the harmonisation of conditions enabling the conduct of the oversight activities;*
- *RTS specifying the criteria for determining the composition of the joint examination team (JET);*

- *RTS on threat-led penetration testing (TLPT)*

*(the "DORA RTS/ITS");*

- *Guidelines on aggregated costs and losses from major incidents;*
- *Guidelines on oversight cooperation between ESAs and competent authorities (Article 32(7) of DORA)*

*(the "DORA GL").*

*Please note that DORA, the Commission Delegated Regulations, the DORA RTS/ITS and the DORA GL will enter into force from 17 January 2025.*

*By using the electronic version, you will have a direct access to the relevant Articles of DORA, the Commission Delegated Regulations, the DORA RTS/ITS and the DORA GL.*

*It can be printed from our website ([www.elvingerhoss.lu](http://www.elvingerhoss.lu)) and/or used as an electronic version.*

*This compilation of the European legislative documents has been prepared by our firm for information purposes only. It may be reviewed and improved from time to time. The latest version will be published on our website: [www.elvingerhoss.lu](http://www.elvingerhoss.lu)*

## TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b> .....	<b>1</b>
<b>DORA Regulation (Digital operational resilience for the financial sector)</b> .....	<b>4</b>
Recitals .....	4
<b>CHAPTER I GENERAL PROVISIONS</b> .....	<b>25</b>
Article 1: Subject matter .....	25
Article 2: Scope.....	26
Article 3: Definitions.....	28
Article 4: Proportionality principle .....	33
<b>CHAPTER II ICT RISK MANAGEMENT</b> .....	<b>34</b>
<b>Section I</b> .....	<b>34</b>
Article 5: Governance and organisation .....	34
<b>Section II</b> .....	<b>36</b>
Article 6: ICT risk management framework.....	36
Article 7: ICT systems, protocols and tools.....	38
Article 8: Identification .....	39
Article 9: Protection and prevention .....	40
Article 10: Detection .....	42
Article 11: Response and recovery .....	43
Article 12: Backup policies and procedures, restoration and recovery procedures and methods .....	45
Article 13: Learning and evolving .....	47
Article 14: Communication.....	48
Article 15: Further harmonisation of ICT risk management tools, methods, processes and policies .....	49
Article 16: Simplified ICT risk management framework.....	50
<b>CHAPTER III ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION AND REPORTING</b> .....	<b>52</b>
Article 17: ICT-related incident management process .....	52
Article 18: Classification of ICT-related incidents and cyber threats.....	53
Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats .	55
Article 20: Harmonisation of reporting content and templates.....	57
Article 21: Centralisation of reporting of major ICT-related incidents.....	58
Article 22: Supervisory feedback.....	59
Article 23: Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions .....	60
<b>CHAPTER IV DIGITAL OPERATIONAL RESILIENCE TESTING</b> .....	<b>61</b>
Article 24: General requirements for the performance of digital operational resilience testing .....	61
Article 25: Testing of ICT tools and systems.....	62
Article 26: Advanced testing of ICT tools, systems and processes based on TLPT .....	63
Article 27: Requirements for testers for the carrying out of TLPT .....	66
<b>CHAPTER V Managing of ICT third-party risk</b> .....	<b>67</b>
<b>Section I Key principles for a sound management of ICT third-party risk</b> .....	<b>67</b>
Article 28: General principles .....	67
Article 29: Preliminary assessment of ICT concentration risk at entity level .....	70
Article 30: Key contractual provisions .....	71
<b>Section II Oversight Framework of critical ICT third-party service providers</b> .....	<b>74</b>
Article 31: Designation of critical ICT third-party service providers.....	74
Article 32: Structure of the Oversight Framework .....	77
Article 33: Tasks of the Lead Overseer .....	79
Article 34: Operational coordination between Lead Overseers .....	81
Article 35: Powers of the Lead Overseer .....	82
Article 36: Exercise of the powers of the Lead Overseer outside the Union .....	85
Article 37: Request for information .....	87
Article 38: General investigations .....	88
Article 39: Inspections .....	89

Article 40: Ongoing oversight .....	90
Article 41: Harmonisation of conditions enabling the conduct of the oversight activities .....	91
Article 42: Follow-up by competent authorities .....	92
Article 43: Oversight fees .....	94
Article 44: International cooperation .....	95
<b>CHAPTER VI Information-sharing arrangements.....</b>	<b>96</b>
Article 45: Information-sharing arrangements on cyber threat information and intelligence .....	96
<b>CHAPTER VII Competent authorities .....</b>	<b>97</b>
Article 46: Competent authorities.....	97
Article 47: Cooperation with structures and authorities established by Directive (EU) 2022/2555 .....	99
Article 48: Cooperation between authorities.....	100
Article 49: Financial cross-sector exercises, communication and cooperation.....	101
Article 50: Administrative penalties and remedial measures .....	102
Article 51: Exercise of the power to impose administrative penalties and remedial measures .....	103
Article 52: Criminal penalties .....	104
Article 53: Notification duties .....	105
Article 54: Publication of administrative penalties .....	106
Article 55: Professional secrecy.....	107
Article 56: Data Protection .....	108
<b>CHAPTER VIII Delegated acts .....</b>	<b>109</b>
Article 57: Exercise of the delegation.....	109
<b>CHAPTER IX Transitional and final provisions .....</b>	<b>110</b>
<b>Section I .....</b>	<b>110</b>
Article 58: Review clause.....	110
<b>Section II Amendments .....</b>	<b>112</b>
Article 59: Amendments to Regulation (EC) No 1060/2009.....	112
Article 60: Amendments to Regulation (EU) No 648/2012 .....	113
Article 61: Amendments to Regulation (EU) No 909/2014 .....	115
Article 62: Amendments to Regulation (EU) No 600/2014 .....	116
Article 63: Amendment to Regulation (EU) 2016/1011 .....	117
Article 64: Entry into force and application .....	118
<b>APPENDIX I: Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities .....</b>	<b>119</b>
<b>APPENDIX II: Commission Delegated Regulation (EU) 2024/1505 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid.....</b>	<b>125</b>
<b>APPENDIX III: Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents .....</b>	<b>129</b>
<b>APPENDIX IV: Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers .....</b>	<b>139</b>
<b>APPENDIX V: Commission Delegated Regulation (EU) 2024/1774 of 13 March 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 .....</b>	<b>148</b>
<b>APPENDIX VI: Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554 .....</b>	<b>188</b>
<b>APPENDIX VII: RTS and ITS on the content, format, templates and timelines for reporting major ICT-related</b>	

<b>incidents and significant cyber threats .....</b>	<b>237</b>
<b>APPENDIX VIII: RTS on subcontracting of critical or important functions .....</b>	<b>286</b>
<b>APPENDIX IX: RTS on harmonisation of conditions enabling the conduct of the oversight activities .....</b>	<b>287</b>
<b>APPENDIX X: RTS specifying the criteria for determining the composition of the joint examination team (JET) .....</b>	<b>298</b>
<b>APPENDIX XI: RTS on threat-led penetration testing (TLPT) .....</b>	<b>304</b>
<b>APPENDIX XII: Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents .....</b>	<b>334</b>
<b>APPENDIX XIII: Guidelines on ESAs-competent authorities oversight cooperation .....</b>	<b>338</b>

## **DORA Regulation (Digital operational resilience for the financial sector)**

**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**

(Text with EEA relevance)

### **Recitals**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank<sup>1</sup>,

Having regard to the opinion of the European Economic and Social Committee<sup>2</sup>,

Acting in accordance with the ordinary legislative procedure<sup>3</sup>,

Whereas:

- (1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.
- (2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance intermediaries offering their services online operating with InsurTech, to digital insurance underwriting. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.
- (3) The European Systemic Risk Board (ESRB) reaffirmed in a 2020 report addressing systemic cyber risk how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, could constitute a

---

<sup>1</sup> OJ C 343, 26.8.2021, p. 1.

<sup>2</sup> OJ C 155, 30.4.2021, p. 38.

<sup>3</sup> Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.



systemic vulnerability because localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches that occur in the financial sector do not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union's financial system, such as generating liquidity runs and an overall loss of confidence and trust in financial markets.

- (4) In recent years, ICT risk has attracted the attention of international, Union and national policy makers, regulators and standard-setting bodies in an attempt to enhance digital resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the Financial Stability Board, the Financial Stability Institute, as well as the G7 and G20 aim to provide competent authorities and market operators across various jurisdictions with tools to bolster the resilience of their financial systems. That work has also been driven by the need to duly consider ICT risk in the context of a highly interconnected global financial system and to seek more consistency of relevant best practices.
- (5) Despite Union and national targeted policy and legislative initiatives, ICT risk continues to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reforms that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed to safeguard the competitiveness and stability of the Union from economic, prudential and market conduct perspectives. Although ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-financial crisis regulatory agenda and have developed in only some areas of the Union's financial services policy and regulatory landscape, or in only a few Member States.
- (6) In its Communication of 8 March 2018 entitled 'FinTech Action plan: For a more competitive and innovative European financial sector', the Commission highlighted the paramount importance of making the Union financial sector more resilient, including from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling the effective and smooth provision of financial services across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence.
- (7) In April 2019, the European Supervisory Authority (European Banking Authority), (EBA) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council<sup>4</sup>, the European Supervisory Authority (European Insurance and Occupational Pensions Authority), ('EIOPA') established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>5</sup> and the European Supervisory Authority (European Securities and Markets Authority), ('ESMA') established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>6</sup> (known collectively as 'European Supervisory Authorities' or 'ESAs') jointly issued technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a sector-specific initiative of the Union.
- (8) The Union financial sector is regulated by a Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not yet fully or consistently harmonised, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than, for example, common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover digital operational resilience, by strengthening the mandates of competent

---

<sup>4</sup> 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).

<sup>5</sup> 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).

<sup>6</sup> 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).

authorities to enable them to supervise the management of ICT risk in the financial sector in order to protect the integrity and efficiency of the internal market, and to facilitate its orderly functioning.

- (9) Legislative disparities and uneven national regulatory or supervisory approaches with regard to ICT risk trigger obstacles to the functioning of the internal market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities operating on a cross-border basis. Competition between the same type of financial entities operating in different Member States could also be distorted. This is the case, in particular, for areas where Union harmonisation has been very limited, such as digital operational resilience testing, or absent, such as the monitoring of ICT third-party risk. Disparities stemming from developments envisaged at national level could generate further obstacles to the functioning of the internal market to the detriment of market participants and financial stability.
- (10) To date, due to the ICT risk related provisions being only partially addressed at Union level, there are gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and inconsistencies as a result of emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user such as the financial sector since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, each issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risk and mitigating adverse impacts of ICT incidents on their own and in a coherent cost-effective way. [↪ Chapter III and Chapter IV](#)
- (11) As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework, further harmonisation of key digital operational resilience requirements for all financial entities is required. The development of ICT capabilities and overall resilience by financial entities, based on those key requirements, with a view to withstanding operational outages, would help preserve the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims to contribute to the smooth functioning of the internal market, it should be based on the provisions of Article 114 of the Treaty on the Functioning of the European Union (TFEU) as interpreted in accordance with the consistent case law of the Court of Justice of the European Union (Court of Justice).
- (12) This Regulation aims to consolidate and upgrade ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts. While those acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they did not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk rules, when further developed in those Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risk) rather than targeted qualitative rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents, or for reporting and digital testing capabilities. Those acts were primarily meant to cover and update essential rules on prudential supervision, market integrity or conduct. By consolidating and upgrading the different rules on ICT risk, all provisions addressing digital risk in the financial sector should for the first time be brought together in a consistent manner in one single legislative act. Therefore, this Regulation fills in the gaps or remedies inconsistencies in some of the prior legal acts, including in relation to the terminology used therein, and explicitly refers to ICT risk via targeted rules on ICT risk-management capabilities, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation should thus also raise awareness of ICT risk and acknowledge that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of financial entities.
- (13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of high reliance on ICT systems, platforms and infrastructures, which entails increased digital risk. Observing basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.

- (14) A Regulation helps reduce regulatory complexity, fosters supervisory convergence and increases legal certainty, and also contributes to limiting compliance costs, especially for financial entities operating across borders, and to reducing competitive distortions. Therefore, the choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities is the most appropriate way to guarantee a homogenous and coherent application of all components of ICT risk management by the Union financial sector.
- (15) Directive (EU) 2016/1148 of the European Parliament and of the Council<sup>7</sup> was the first horizontal cybersecurity framework enacted at Union level, applying also to three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 set out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties that were identified by the Member States, have been brought into its scope in practice, and hence required to comply with the ICT security and incident notification requirements laid down in it. Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>8</sup> sets a uniform criterion to determine the entities falling within its scope of application (size-cap rule) while also keeping the three types of financial entities in its scope.
- (16) However, as this Regulation increases the level of harmonisation of the various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law, this higher level constitutes an increased harmonisation also in comparison with the requirements laid down in Directive (EU) 2022/2555. Consequently, this Regulation constitutes *lex specialis* with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive.  
[↪ Chapter II and Chapter III](#)
- (17) In accordance with Article 4(2) of the Treaty on European Union and without prejudice to the judicial review by the Court of Justice, this Regulation should not affect the responsibility of Member States with regard to essential State functions concerning public security, defence and the safeguarding of national security, for example concerning the supply of information which would be contrary to the safeguarding of national security.
- (18) To enable cross-sector learning and to effectively draw on experiences of other sectors in dealing with cyber threats, the financial entities referred to in Directive (EU) 2022/2555 should remain part of the 'ecosystem' of that Directive (for example, Cooperation Group and computer security incident response teams (CSIRTs)). The ESAs and national competent authorities should be able to participate in the strategic policy discussions and the technical workings of the Cooperation Group under that Directive, and to exchange information and further cooperate with the single points of contact designated or established in accordance with that Directive. The competent authorities under this Regulation should also consult and cooperate with the CSIRTs. The competent authorities should also be able to request technical advice from the competent authorities designated or established in accordance with Directive (EU) 2022/2555 and establish cooperation arrangements that aim to ensure effective and fast-response coordination mechanisms.
- (19) Given the strong interlinkages between the digital resilience and the physical resilience of financial entities, a coherent approach with regard to the resilience of critical entities is necessary in this Regulation and Directive (EU) 2022/2557 of the European Parliament and the Council<sup>9</sup>. Given that the physical resilience of financial entities is addressed in a comprehensive manner by the ICT risk management and reporting obligations covered by this Regulation, the obligations laid down in Chapters III and IV of

<sup>7</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

<sup>8</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (see page 80 of this Official Journal).

<sup>9</sup> Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (see page 164 of this Official Journal).

Directive (EU) 2022/2557 should not apply to financial entities falling within the scope of that Directive. [↶ Chapter IV](#)

- (20) Cloud computing service providers are one category of digital infrastructure covered by Directive (EU) 2022/2555. The Union Oversight Framework ('Oversight Framework') established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers providing ICT services to financial entities, and should be considered complementary to the supervision carried out pursuant to Directive (EU) 2022/2555. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal framework establishing a digital oversight authority.
- (21) In order to maintain full control over ICT risk, financial entities need to have comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Likewise, financial entities should have policies in place for the testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. The digital operational resilience baseline for financial entities should be increased while also allowing for a proportionate application of requirements for certain financial entities, particularly microenterprises, as well as financial entities subject to a simplified ICT risk management framework. To facilitate an efficient supervision of institutions for occupational retirement provision that is proportionate and addresses the need to reduce administrative burdens on the competent authorities, the relevant national supervisory arrangements in respect of such financial entities should take into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations even when the relevant thresholds established in Article 5 of Directive (EU) 2016/2341 of the European Parliament and of the Council<sup>10</sup> are exceeded. In particular, supervisory activities should focus primarily on the need to address serious risks associated with the ICT risk management of a particular entity. [↶ Chapter II](#)

Competent authorities should also maintain a vigilant but proportionate approach in relation to the supervision of institutions for occupational retirement provision which, in accordance with Article 31 of Directive (EU) 2016/2341, outsource a significant part of their core business, such as asset management, actuarial calculations, accounting and data management, to service providers.

- (22) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through the relevant work undertaken by the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>11</sup> and the Cooperation Group under Directive (EU) 2022/2555, divergent approaches on setting the thresholds and use of taxonomies still exist, or can emerge, for the remainder of financial entities. Due to those divergences, there are multiple requirements that financial entities must comply with, especially when operating across several Member States and when part of a financial group. Moreover, such divergences have the potential to hinder the creation of further uniform or centralised Union mechanisms that speed up the reporting process and support a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risk in the event of large-scale attacks with potentially systemic consequences. [↶ Chapter III](#)
- (23) To reduce the administrative burden and potentially duplicative reporting obligations for certain financial entities, the requirement for the incident reporting pursuant to Directive (EU) 2015/2366 of the European Parliament and of the Council<sup>12</sup> should cease to apply to payment service providers that fall within the scope of this Regulation. Consequently, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of that Directive, should, from the date of application of this Regulation, report pursuant to this Regulation, all operational or security

---

<sup>10</sup> Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).

<sup>11</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

<sup>12</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

payment-related incidents which have been previously reported pursuant to that Directive, irrespective of whether such incidents are ICT-related. [↪ Chapter III](#)

- (24) To enable competent authorities to fulfil supervisory roles by acquiring a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to enhance the exchange of information between relevant public authorities, including law enforcement authorities and resolution authorities, this Regulation should lay down a robust ICT-related incident reporting regime whereby the relevant requirements address current gaps in financial services law, and remove existing overlaps and duplications to alleviate costs. It is essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities through a single streamlined framework as set out in this Regulation. In addition, the ESAs should be empowered to further specify relevant elements for the ICT-related incident reporting framework, such as taxonomy, timeframes, data sets, templates and applicable thresholds. To ensure full consistency with Directive (EU) 2022/2555, financial entities should be allowed, on a voluntary basis, to notify significant cyber threats to the relevant competent authority, when they consider that the cyber threat is of relevance to the financial system, service users or clients. [↪ Chapter III](#)
- (25) Digital operational resilience testing requirements have been developed in certain financial subsectors setting out frameworks that are not always fully aligned. This leads to a potential duplication of costs for cross-border financial entities and makes the mutual recognition of the results of digital operational resilience testing complex which, in turn, can fragment the internal market. [↪ Chapter IV](#)
- (26) In addition, where no ICT testing is required, vulnerabilities remain undetected and result in exposing a financial entity to ICT risk and ultimately create a higher risk to the stability and integrity of the financial sector. Without Union intervention, digital operational resilience testing would continue to be inconsistent and would lack a system of mutual recognition of ICT testing results across different jurisdictions. In addition, as it is unlikely that other financial subsectors would adopt testing schemes on a meaningful scale, they would miss out on the potential benefits of a testing framework, in terms of revealing ICT vulnerabilities and risks, and testing defence capabilities and business continuity, which contributes to increasing the trust of customers, suppliers and business partners. To remedy those overlaps, divergences and gaps, it is necessary to lay down rules for a coordinated testing regime and thereby facilitate the mutual recognition of advanced testing for financial entities meeting the criteria set out in this Regulation. [↪ Chapter IV](#)
- (27) Financial entities' reliance on the use of ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in recent years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.
- (28) The extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements to which they are subject, or otherwise in enforcing specific rights, such as access or audit rights, even when the latter are enshrined in their contractual arrangements. Moreover, many of those contractual arrangements do not provide for sufficient safeguards allowing for the fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess the associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors. [↪ Chapter V](#)
- (29) Even though Union financial services law contains certain general rules on outsourcing, monitoring of the contractual dimension is not fully anchored into Union law. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. Those principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contractual arrangements with a view to providing certain minimum safeguards in order to strengthen financial entities' ability to

effectively monitor all ICT risk emerging at the level of third-party service providers. Those principles are complementary to the sectoral law applicable to outsourcing. [↪ Chapter V](#)

- (30) A certain lack of homogeneity and convergence regarding the monitoring of ICT third-party risk and ICT third-party dependencies is evident today. Despite efforts to address outsourcing, such as EBA Guidelines on outsourcing of 2019 and ESMA Guidelines on outsourcing to cloud service providers of 2021 the broader issue of counteracting systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is not sufficiently addressed by Union law. The lack of rules at Union level is compounded by the absence of national rules on mandates and tools that allow financial supervisors to acquire a good understanding of ICT third-party dependencies and to monitor adequately risks arising from the concentration of ICT third-party dependencies. [↪ Chapter V](#)
- (31) Taking into account the potential systemic risk entailed by increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms in providing financial supervisors with adequate tools to quantify, qualify and redress the consequences of ICT risk occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical ICT third-party service providers to financial entities, while ensuring that the confidentiality and security of customers other than financial entities is preserved. While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment. [↪ Chapter V](#)
- (32) With ICT risk becoming more and more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and to recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust and liability rules. [↪ Chapter VI](#)
- (33) In addition, doubts about the type of information that can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead to useful information being withheld. Therefore, the extent and quality of information sharing currently remains limited and fragmented, with relevant exchanges mostly being local (by way of national initiatives) and with no consistent Union-wide information-sharing arrangements tailored to the needs of an integrated financial system. It is therefore important to strengthen those communication channels. [↪ Chapter VI](#)
- (34) Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, and to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements. It is therefore necessary to enable the emergence at Union level of mechanisms for voluntary information-sharing arrangements which, when conducted in trusted environments, would help the community of the financial industry to prevent and collectively respond to cyber threats by quickly limiting the spread of ICT risk and impeding potential contagion throughout the financial channels. Those mechanisms should comply with the applicable competition law rules of the Union set out in the Communication from the Commission of 14 January 2011 entitled 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements', as well as with Union data protection rules, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>13</sup>. They should operate based on the use of one or more of the legal bases that are laid down in Article 6 of

---

<sup>13</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).



that Regulation, such as in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in Article 6(1), point (f), of that Regulation, as well as in the context of the processing of personal data necessary for compliance with a legal obligation to which the controller is subject, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as referred to in Article 6(1), points (c) and (e), respectively, of that Regulation. [↪ Chapter VI](#)

- (35) In order to maintain a high level of digital operational resilience for the whole financial sector, and at the same time to keep pace with technological developments, this Regulation should address risk stemming from all types of ICT services. To that end, the definition of ICT services in the context of this Regulation should be understood in a broad manner, encompassing digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. That definition should, for instance, include so called 'over the top' services, which fall within the category of electronic communications services. It should exclude only the limited category of traditional analogue telephone services qualifying as Public Switched Telephone Network (PSTN) services, landline services, Plain Old Telephone Service (POTS), or fixed-line telephone services. [↪ Art. 3\(21\)](#)
- (36) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into account the significant differences between financial entities in terms of their size and overall risk profile. As a general principle, when distributing resources and capabilities for the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations, while competent authorities should continue to assess and review the approach of such distribution. [↪ Art. 4](#)
- (37) Account information service providers, referred to in Article 33(1) of Directive (EU) 2015/2366, are explicitly included in the scope of this Regulation, taking into account the specific nature of their activities and the risks arising therefrom. In addition, electronic money institutions and payment institutions exempted pursuant to Article 9(1) of Directive 2009/110/EC of the European Parliament and of the Council<sup>14</sup> and Article 32(1) of Directive (EU) 2015/2366 are included in the scope of this Regulation even if they have not been granted authorisation in accordance Directive 2009/110/EC to issue electronic money, or if they have not been granted authorisation in accordance with Directive (EU) 2015/2366 to provide and execute payment services. However, post office giro institutions, referred to in Article 2(5), point (3), of Directive 2013/36/EU of the European Parliament and of the Council<sup>15</sup>, are excluded from the scope of this Regulation. The competent authority for payment institutions exempted pursuant to Directive (EU) 2015/2366, electronic money institutions exempted pursuant to Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, should be the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366. [↪ Art. 2\(3\)](#)
- (38) As larger financial entities might enjoy wider resources and can swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities that are not microenterprises in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to set up an internal risk management and control model, and to submit their ICT risk management framework to internal audits. [↪ Art. 2\(3\)](#)
- (39) Some financial entities benefit from exemptions or are subject to a very light regulatory framework under the relevant sector-specific Union law. Such financial entities include managers of alternative investment

<sup>14</sup> Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

<sup>15</sup> Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

funds referred to in Article 3(2) of Directive 2011/61/EU of the European Parliament and of the Council<sup>16</sup>, insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC of the European Parliament and of the Council<sup>17</sup>, and institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total. In light of those exemptions it would not be proportionate to include such financial entities in the scope of this Regulation. In addition, this Regulation acknowledges the specificities of the insurance intermediation market structure, with the result that insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries qualifying as microenterprises or as small or medium-sized enterprises should not be subject to this Regulation. [↪ Art. 2\(3\)](#)

- (40) Since the entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU are excluded from the scope of that Directive, Member States should consequently be able to choose to exempt from the application of this Regulation such entities located within their respective territories. [↪ Art. 2\(3\)](#)
- (41) Similarly, in order to align this Regulation to the scope of Directive 2014/65/EU of the European Parliament and of the Council<sup>18</sup>, it is also appropriate to exclude from the scope of this Regulation natural and legal persons referred in Articles 2 and 3 of that Directive which are allowed to provide investment services without having to obtain an authorisation under Directive 2014/65/EU. However, Article 2 of Directive 2014/65/EU also excludes from the scope of that Directive entities which qualify as financial entities for the purposes of this Regulation such as, central securities depositories, collective investment undertakings or insurance and reinsurance undertakings. The exclusion from the scope of this Regulation of the persons and entities referred to in Articles 2 and 3 of that Directive should not encompass those central securities depositories, collective investment undertakings or insurance and reinsurance undertakings. [↪ Art. 2\(3\)](#)
- (42) Under sector-specific Union law, some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. That category of financial entities includes small and non-interconnected investment firms, small institutions for occupational retirement provision which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total, as well as institutions exempted pursuant to Directive 2013/36/EU. Therefore, in accordance with the principle of proportionality and to preserve the spirit of sector-specific Union law, it is also appropriate to subject those financial entities to a simplified ICT risk management framework under this Regulation. The proportionate character of the ICT risk management framework covering those financial entities should not be altered by the regulatory technical standards that are to be developed by the ESAs. Moreover, in accordance with the principle of proportionality, it is appropriate to also subject payment institutions referred to in Article 32(1) of Directive (EU) 2015/2366 and electronic money institutions referred to in Article 9 of Directive 2009/110/EC exempted in accordance with national law transposing those Union legal acts to a simplified ICT risk management framework under this Regulation, while payment institutions and electronic money institutions which have not been exempted in accordance with their respective national law transposing sectoral Union law should comply with the general framework laid down by this Regulation. [↪ Art. 3\(34\)](#), [Art 3\(53\)](#) and [Art. 4](#)
- (43) Similarly, financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework under this Regulation should not be required to establish a role to monitor their arrangements concluded with ICT third-party service providers on the use of ICT services; or to designate a member of senior management to be responsible for overseeing the related risk exposure and relevant documentation; to assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest; to document and review at least once a year the ICT risk management framework; to subject to internal audit on a regular basis the ICT risk management framework; to perform in-depth assessments after major changes in their network and information system infrastructures and processes; to regularly conduct risk analyses on legacy ICT systems; to subject the implementation of the ICT Response and

<sup>16</sup> Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).

<sup>17</sup> Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

<sup>18</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).



Recovery plans to independent internal audit reviews; to have a crisis management function, to expand the testing of business continuity and response and recovery plans to capture switchover scenarios between primary ICT infrastructure and redundant facilities; to report to competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents, to maintain redundant ICT capacities; to communicate to national competent authorities implemented changes following post ICT-related incident reviews; to monitor on a continuous basis relevant technological developments, to establish a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework provided for in this Regulation, or to adopt and regularly review a strategy on ICT third-party risk. In addition, microenterprises should only be required to assess the need to maintain such redundant ICT capacities based on their risk profile. Microenterprises should benefit from a more flexible regime as regards digital operational resilience testing programmes. When considering the type and frequency of testing to be performed, they should properly balance the objective of maintaining a high digital operational resilience, the available resources and their overall risk profile. Microenterprises and financial entities subject to the simplified ICT risk management framework under this Regulation should be exempted from the requirement to perform advanced testing of ICT tools, systems and processes based on threat-led penetration testing (TLPT), as only financial entities meeting the criteria set out in this Regulation should be required to carry out such testing. In light of their limited capabilities, microenterprises should be able to agree with the ICT third-party service provider to delegate the financial entity's rights of access, inspection and audit to an independent third-party, to be appointed by the ICT third-party service provider, provided that the financial entity is able to request, at any time, all relevant information and assurance on the ICT third-party service provider's performance from the respective independent third-party. [↪ Art. 4](#)

- (44) As only those financial entities identified for the purposes of the advanced digital resilience testing should be required to conduct threat-led penetration tests, the administrative processes and financial costs entailed in the performance of such tests should be borne by a small percentage of financial entities. [↪ Art. 26](#)
- (45) To ensure full alignment and overall consistency between financial entities' business strategies, on the one hand, and the conduct of ICT risk management, on the other hand, the financial entities' management bodies should be required to maintain a pivotal and active role in steering and adapting the ICT risk management framework and the overall digital operational resilience strategy. The approach to be taken by management bodies should not only focus on the means of ensuring the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness about cyber risks and a commitment to observe a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risk should be an overarching principle of that comprehensive approach, further translated into the continuous engagement of the management body in the control of the monitoring of the ICT risk management. [↪ Art. 5\(3\)](#)
- (46) Moreover, the principle of the management body's full and ultimate responsibility for the management of the ICT risk of the financial entity goes hand in hand with the need to secure a level of ICT-related investments and an overall budget for the financial entity that would enable the financial entity to achieve a high level of digital operational resilience. [↪ Art. 5](#)
- (47) Inspired by relevant international, national and industry best practices, guidelines, recommendations and approaches to the management of cyber risk, this Regulation promotes a set of principles that facilitate the overall structure of ICT risk management. Consequently, as long as the main capabilities which financial entities put in place address the various functions in the ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities should remain free to use ICT risk management models that are differently framed or categorised. [↪ Chapter II](#)
- (48) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and capable, not only for guaranteeing the processing of data required for their services, but also for ensuring sufficient technological resilience to allow them to deal adequately with additional processing needs due to stressed market conditions or other adverse situations.

- (49) Efficient business continuity and recovery plans are necessary to allow financial entities to promptly and quickly resolve ICT-related incidents, in particular cyber-attacks, by limiting damage and giving priority to the resumption of activities and recovery actions in accordance with their back-up policies. However, such resumption should in no way jeopardise the integrity and security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. [↪ Art. 11](#)
- (50) While this Regulation allows financial entities to determine their recovery time and recovery point objectives in a flexible manner and hence to set such objectives by fully taking into account the nature and the criticality of the relevant functions and any specific business needs, it should nevertheless require them to carry out an assessment of the potential overall impact on market efficiency when determining such objectives. [↪ Art. 11 and Art. 12](#)
- (51) The propagators of cyber-attacks tend to pursue financial gains directly at the source, thus exposing financial entities to significant consequences. To prevent ICT systems from losing integrity or becoming unavailable, and hence to avoid data breaches and damage to physical ICT infrastructure, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined. ICT-related incident reporting should be harmonised through the introduction of a requirement for all financial entities to report directly to their relevant competent authorities. Where a financial entity is subject to supervision by more than one national competent authority, Member States should designate a single competent authority as the addressee of such reporting. Credit institutions classified as significant in accordance with Article 6(4) of Council Regulation (EU) No 1024/2013<sup>19</sup> should submit such reporting to the national competent authorities, which should subsequently transmit the report to the European Central Bank (ECB). [↪ Chapter III](#)
- (52) The direct reporting should enable financial supervisors to have immediate access to information about major ICT-related incidents. Financial supervisors should in turn pass on details of major ICT-related incidents to public non-financial authorities (such as competent authorities and single points of contact under Directive (EU) 2022/2555, national data protection authorities, and to law enforcement authorities for major ICT-related incidents of a criminal nature) in order to enhance such authorities awareness of such incidents and, in the case of CSIRTs, to facilitate prompt assistance that may be given to financial entities, as appropriate. Member States should, in addition, be able to determine that financial entities themselves should provide such information to public authorities outside the financial services area. Those information flows should allow financial entities to swiftly benefit from any relevant technical input, advice about remedies, and subsequent follow-up from such authorities. The information on major ICT-related incidents should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity, while the ESAs should share anonymised data on cyber threats and vulnerabilities relating to an incident, to aid wider collective defence. [↪ Chapter III](#)
- (53) While all financial entities should be required to carry out incident reporting, that requirement is not expected to affect all of them in the same manner. Indeed, relevant materiality thresholds, as well as reporting timelines, should be duly adjusted, in the context of delegated acts based on the regulatory technical standards to be developed by the ESAs, with a view to covering only major ICT-related incidents. In addition, the specificities of financial entities should be taken into account when setting timelines for reporting obligations. [↪ Chapter III](#)
- (54) This Regulation should require credit institutions, payment institutions, account information service providers and electronic money institutions to report all operational or security payment-related incidents – previously reported under Directive (EU) 2015/2366 – irrespective of the ICT nature of the incident. [↪ Chapter III](#)
- (55) The ESAs should be tasked with assessing the feasibility and conditions for a possible centralisation of ICT-related incident reports at Union level. Such centralisation could consist of a single EU Hub for major ICT-related incident reporting either directly receiving relevant reports and automatically notifying national competent authorities, or merely centralising relevant reports forwarded by the national competent authorities and thus fulfilling a coordination role. The ESAs should be tasked with preparing, in

---

<sup>19</sup> Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

consultation with the ECB and ENISA, a joint report exploring the feasibility of setting up a single EU Hub.  
[↪ Chapter III](#)

- (56) In order to achieve a high level of digital operational resilience, and in line with both the relevant international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing) and with the frameworks applied in the Union, such as the TIBER-EU, financial entities should regularly test their ICT systems and staff having ICT-related responsibilities with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities. To reflect differences that exist across, and within, the various financial subsectors as regards financial entities' level of cybersecurity preparedness, testing should include a wide variety of tools and actions, ranging from the assessment of basic requirements (e.g. vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing) to more advanced testing by means of TLPT. Such advanced testing should be required only of financial entities that are mature enough from an ICT perspective to reasonably carry it out. The digital operational resilience testing required by this Regulation should thus be more demanding for those financial entities meeting the criteria set out in this Regulation (for example, large, systemic and ICT-mature credit institutions, stock exchanges, central securities depositories and central counterparties) than for other financial entities. At the same time, the digital operational resilience testing by means of TLPT should be more relevant for financial entities operating in core financial services subsectors and playing a systemic role (for example, payments, banking, and clearing and settlement), and less relevant for other subsectors (for example, asset managers and credit rating agencies). [↪ Chapter IV](#)
- (57) Financial entities involved in cross-border activities and exercising the freedoms of establishment, or of provision of services within the Union, should comply with a single set of advanced testing requirements (i.e. TLPT) in their home Member State, which should include the ICT infrastructures in all jurisdictions where the cross-border financial group operates within the Union, thus allowing such cross-border financial groups to incur related ICT testing costs in one jurisdiction only. [↪ Art. 26](#)
- (58) To draw on the expertise already acquired by certain competent authorities, in particular with regard to implementing the TIBER-EU framework, this Regulation should allow Member States to designate a single public authority as responsible in the financial sector, at national level, for all TLPT matters, or competent authorities, to delegate, in the absence of such designation, the exercise of TLPT related tasks to another national financial competent authority. [↪ Art. 26](#)
- (59) Since this Regulation does not require financial entities to cover all critical or important functions in one single threat-led penetration test, financial entities should be free to determine which and how many critical or important functions should be included in the scope of such a test. [↪ Art. 26](#)
- (60) Pooled testing within the meaning of this Regulation – involving the participation of several financial entities in a TLPT and for which an ICT third-party service provider can directly enter into contractual arrangements with an external tester – should be allowed only where the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or the confidentiality of the data related to such services, are reasonably expected to be adversely impacted. Pooled testing should also be subject to safeguards (direction by one designated financial entity, calibration of the number of participating financial entities) to ensure a rigorous testing exercise for the financial entities involved which meet the objectives of the TLPT pursuant to this Regulation. [↪ Art. 26](#)
- (61) In order to take advantage of internal resources available at corporate level, this Regulation should allow the use of internal testers for the purposes of carrying out TLPT, provided there is supervisory approval, no conflicts of interest, and periodical alternation of the use of internal and external testers (every three tests), while also requiring the provider of the threat intelligence in the TLPT to always be external to the financial entity. The responsibility for conducting TLPT should remain fully with the financial entity. Attestations provided by authorities should be solely for the purpose of mutual recognition and should not preclude any follow-up action needed to address the ICT risk to which the financial entity is exposed, nor should they be seen as a supervisory endorsement of a financial entity's ICT risk management and mitigation capabilities. [↪ Art. 26 and Art. 27](#)

- (62) To ensure a sound monitoring of ICT third-party risk in the financial sector, it is necessary to lay down a set of principle-based rules to guide financial entities' when monitoring risk arising in the context of functions outsourced to ICT third-party service providers, particularly for ICT services supporting critical or important functions, as well as more generally in the context of all ICT third-party dependencies. [↪ Chapter V](#)
- (63) To address the complexity of the various sources of ICT risk, while taking into account the multitude and diversity of providers of technological solutions which enable a smooth provision of financial services, this Regulation should cover a wide range of ICT third-party service providers, including providers of cloud computing services, software, data analytics services and providers of data centre services. Similarly, since financial entities should effectively and coherently identify and manage all types of risk, including in the context of ICT services procured within a financial group, it should be clarified that undertakings which are part of a financial group and provide ICT services predominantly to their parent undertaking, or to subsidiaries or branches of their parent undertaking, as well as financial entities providing ICT services to other financial entities, should also be considered as ICT third-party service providers under this Regulation. Lastly, in light of the evolving payment services market becoming increasingly dependent on complex technical solutions, and in view of emerging types of payment services and payment-related solutions, participants in the payment services ecosystem, providing payment-processing activities, or operating payment infrastructures, should also be considered to be ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and public authorities when providing ICT related services in the context of fulfilling State functions. [↪ Chapter V](#)
- (64) A financial entity should at all times remain fully responsible for complying with its obligations set out in this Regulation. Financial entities should apply a proportionate approach to the monitoring of risks emerging at the level of the ICT third-party service providers, by duly considering the nature, scale, complexity and importance of their ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate. [↪ Art. 28](#)
- (65) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated ICT third-party risk strategy, rooted in a continuous screening of all ICT third-party dependencies. To enhance supervisory awareness of ICT third-party dependencies, and with a view to further supporting the work in the context of the Oversight Framework established by this Regulation, all financial entities should be required to maintain a register of information with all contractual arrangements about the use of ICT services provided by ICT third-party service providers. Financial supervisors should be able to request the full register, or to ask for specific sections thereof, and thus to obtain essential information for acquiring a broader understanding of the ICT dependencies of financial entities. [↪ Art. 28\(3\)](#)
- (66) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, in particular by focusing on elements such as the criticality or importance of the services supported by the envisaged ICT contract, the necessary supervisory approvals or other conditions, the possible concentration risk entailed, as well as applying due diligence in the process of selection and assessment of ICT third-party service providers and assessing potential conflicts of interest. For contractual arrangements concerning critical or important functions, financial entities should take into consideration the use by ICT third-party service providers of the most up-to-date and highest information security standards. Termination of contractual arrangements could be prompted at least by a series of circumstances showing shortfalls at the ICT third-party service provider level, in particular significant breaches of laws or contractual terms, circumstances revealing a potential alteration of the performance of the functions provided for in the contractual arrangements, evidence of weaknesses of the ICT third-party service provider in its overall ICT risk management, or circumstances indicating the inability of the relevant competent authority to effectively supervise the financial entity. [↪ Art. 28\(4\)](#)
- (67) To address the systemic impact of ICT third-party concentration risk, this Regulation promotes a balanced solution by means of taking a flexible and gradual approach to such concentration risk since the imposition of any rigid caps or strict limitations might hinder the conduct of business and restrain the contractual freedom. Financial entities should thoroughly assess their envisaged contractual arrangements to identify

the likelihood of such risk emerging, including by means of in-depth analyses of subcontracting arrangements, in particular when concluded with ICT third-party service providers established in a third country. At this stage, and with a view to striking a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to set out rules on strict caps and limits to ICT third-party exposures. In the context of the Oversight Framework, a Lead Overseer, appointed pursuant to this Regulation, should, in respect to critical ICT third-party service providers, pay particular attention to fully grasp the magnitude of interdependences, discover specific instances where a high degree of concentration of critical ICT third-party service providers in the Union is likely to put a strain on the Union financial system's stability and integrity and maintain a dialogue with critical ICT third-party service providers where that specific risk is identified. [↪ Chapter V Section II](#)

- (68) To evaluate and monitor on a regular basis the ability of an ICT third party service provider to securely provide services to a financial entity without adverse effects on a financial entity's digital operational resilience, several key contractual elements with ICT third-party service providers should be harmonised. Such harmonisation should cover minimum areas which are crucial for enabling a full monitoring by the financial entity of the risks that could emerge from the ICT third-party service provider, from the perspective of a financial entity's need to secure its digital resilience because it is deeply dependent on the stability, functionality, availability and security of the ICT services received. [↪ Art. 30](#)
- (69) When renegotiating contractual arrangements to seek alignment with the requirements of this Regulation, financial entities and ICT third-party service providers should ensure the coverage of the key contractual provisions as provided for in this Regulation. [↪ Art. 30\(4\)](#)
- (70) The definition of 'critical or important function' provided for in this Regulation encompasses the 'critical functions' as defined in Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council<sup>20</sup>. Accordingly, functions deemed to be critical pursuant to Directive 2014/59/EU are included in the definition of critical functions within the meaning of this Regulation.
- (71) Irrespective of the criticality or importance of the function supported by the ICT services, contractual arrangements should, in particular, provide for a specification of the complete descriptions of functions and services, of the locations where such functions are provided and where data is to be processed, as well as an indication of service level descriptions. Other essential elements to enable a financial entity's monitoring of ICT third party risk are: contractual provisions specifying how the accessibility, availability, integrity, security and protection of personal data are ensured by the ICT third-party service provider, provisions laying down the relevant guarantees for enabling the access, recovery and return of data in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, as well as provisions requiring the ICT third-party service provider to provide assistance in case of ICT incidents in connection with the services provided, at no additional cost or at a cost determined *ex-ante*; provisions on the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity; and provisions on termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities. [↪ Art. 30](#)
- (72) In addition to such contractual provisions, and with a view to ensuring that financial entities remain in full control of all developments occurring at third-party level which may impair their ICT security, the contracts for the provision of ICT services supporting critical or important functions should also provide for the following: the specification of the full service level descriptions, with precise quantitative and qualitative performance targets, to enable without undue delay appropriate corrective actions when the agreed service levels are not met; the relevant notice periods and reporting obligations of the ICT third-party service provider in the event of developments with a potential material impact on the ICT third-party service provider's ability to effectively provide their respective ICT services; a requirement upon the ICT third-party service provider to implement and test business contingency plans and have ICT security

---

<sup>20</sup> Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).



measures, tools and policies allowing for the secure provision of services, and to participate and fully cooperate in the TLPT carried out by the financial entity. [↪ Art. 30](#)

- (73) Contracts for the provision of ICT services supporting critical or important functions should also contain provisions enabling the rights of access, inspection and audit by the financial entity, or an appointed third party, and the right to take copies as crucial instruments in the financial entities' ongoing monitoring of the ICT third-party service provider's performance, coupled with the service provider's full cooperation during inspections. Similarly, the competent authority of the financial entity should have the right, based on notices, to inspect and audit the ICT third-party service provider, subject to the protection of confidential information. [↪ Art. 30](#)
- (74) Such contractual arrangements should also provide for dedicated exit strategies to enable, in particular, mandatory transition periods during which ICT third-party service providers should continue providing the relevant services with a view to reducing the risk of disruptions at the level of the financial entity, or to allow the latter effectively to switch to the use of other ICT third-party service providers or, alternatively, to change to in-house solutions, consistent with the complexity of the provided ICT service. Moreover, financial entities within the scope of Directive 2014/59/EU should ensure that the relevant contracts for ICT services are robust and fully enforceable in the event of resolution of those financial entities. Therefore, in line with the expectations of the resolution authorities, those financial entities should ensure that the relevant contracts for ICT services are resolution resilient. As long as they continue meeting their payment obligations, those financial entities should ensure, among other requirements, that the relevant contracts for ICT services contain clauses for non-termination, non-suspension and non-modification on grounds of restructuring or resolution. [↪ Art. 30](#)
- (75) Moreover, the voluntary use of standard contractual clauses developed by public authorities or Union institutions, in particular the use of contractual clauses developed by the Commission for cloud computing services could provide further comfort to the financial entities and ICT third-party service providers, by enhancing their level of legal certainty regarding the use of cloud computing services in the financial sector, in full alignment with the requirements and expectations set out by the Union financial services law. The development of standard contractual clauses builds on measures already envisaged in the 2018 Fintech Action Plan that announced the Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders' efforts, which the Commission has facilitated with the help of the financial sector's involvement. [↪ Art. 30](#)
- (76) With a view to promoting convergence and efficiency in relation to supervisory approaches when addressing ICT third-party risk in the financial sector, as well as to strengthening the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the provision of ICT services that support the supply of financial services, and thereby to contributing to the preservation of the Union's financial system stability and the integrity of the internal market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework. While the set-up of the Oversight Framework is justified by the added value of taking action at Union level and by virtue of the inherent role and specificities of the use of ICT services in the provision of financial services, it should be recalled, at the same time, that this solution appears suitable only in the context of this Regulation specifically dealing with digital operational resilience in the financial sector. However, such Oversight Framework should not be regarded as a new model for Union supervision in other areas of financial services and activities. [↪ Chapter V Section II](#)
- (77) The Oversight Framework should apply only to critical ICT third-party service providers. There should therefore be a designation mechanism to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers. That mechanism should involve a set of quantitative and qualitative criteria to set the criticality parameters as a basis for inclusion in the Oversight Framework. In order to ensure the accuracy of that assessment, and regardless of the corporate structure of the ICT third-party service provider, such criteria should, in the case of a ICT third-party service provider that is part of a wider group, take into consideration the entire ICT third-party service provider's group structure. On the one hand, critical ICT third-party service providers, which are not automatically designated by virtue of the application of those criteria, should have the possibility to opt in to the Oversight Framework on a voluntary basis, on the other hand, ICT third-party service providers, that are already subject to oversight mechanism frameworks supporting the fulfilment of the tasks of the

---

European System of Central Banks as referred to in Article 127(2) TFEU, should be exempted. [↪ Chapter V Section II](#)

- (78) Similarly, financial entities providing ICT services to other financial entities, while belonging to the category of ICT third-party service providers under this Regulation, should also be exempted from the Oversight Framework since they are already subject to supervisory mechanisms established by the relevant Union financial services law. Where applicable, competent authorities should take into account, in the context of their supervisory activities, the ICT risk posed to financial entities by financial entities providing ICT services. Likewise, due to the existing risk monitoring mechanisms at group level, the same exemption should be introduced for ICT third-party service providers delivering services predominantly to the entities of their own group. ICT third-party service providers providing ICT services solely in one Member State to financial entities that are active only in that Member State should also be exempted from the designation mechanism because of their limited activities and lack of cross-border impact. [↪ Art. 31\(8\)](#)
- (79) The digital transformation experienced in financial services has brought about an unprecedented level of use of, and reliance upon, ICT services. Since it has become inconceivable to provide financial services without the use of cloud computing services, software solutions and data-related services, the Union financial ecosystem has become intrinsically co-dependent on certain ICT services provided by ICT service suppliers. Some of those suppliers, innovators in developing and applying ICT-based technologies, play a significant role in the delivery of financial services, or have become integrated into the financial services value chain. They have thus become critical to the stability and integrity of the Union financial system. This widespread reliance on services supplied by critical ICT third-party service providers, combined with the interdependence of the information systems of various market operators, create a direct, and potentially severe, risk to the Union financial services system and to the continuity of delivery of financial services if critical ICT third-party service providers were to be affected by operational disruptions or major cyber incidents. Cyber incidents have a distinctive ability to multiply and propagate throughout the financial system at a considerably faster pace than other types of risk monitored in the financial sector and can extend across sectors and beyond geographical borders. They have the potential to evolve into a systemic crisis, where trust in the financial system has been eroded due to the disruption of functions supporting the real economy, or to substantial financial losses, reaching a level which the financial system is unable to withstand, or which requires the deployment of heavy shock absorption measures. To prevent these scenarios from taking place and thereby endangering the financial stability and integrity of the Union, it is essential to provide the convergence of supervisory practices relating to ICT third-party risk in finance, in particular through new rules enabling the Union oversight of critical ICT third-party service providers.
- (80) The Oversight Framework largely depends on the degree of collaboration between the Lead Overseer and the critical ICT third-party service provider delivering to financial entities services affecting the supply of financial services. Successful oversight is predicated, inter alia, upon the ability of the Lead Overseer to effectively conduct monitoring missions and inspections to assess the rules, controls and processes used by the critical ICT third-party service providers, as well as to assess the potential cumulative impact of their activities on financial stability and the integrity of the financial system. At the same time, it is crucial that critical ICT third-party service providers follow the Lead Overseer's recommendations and address its concerns. Since a lack of cooperation by a critical ICT third-party service provider providing services that affect the supply of financial services, such as the refusal to grant access to its premises or to submit information, would ultimately deprive the Lead Overseer of its essential tools in appraising ICT third-party risk, and could adversely impact the financial stability and the integrity of the financial system, it is necessary to also provide for a commensurate sanctioning regime. [↪ Art. 35 and Art. 35\(5\)](#)
- (81) Against this background, the need of the Lead Overseer to impose penalty payments to compel critical ICT third-party service providers to comply with the transparency and access-related obligations set out in this Regulation should not be jeopardised by difficulties raised by the enforcement of those penalty payments in relation to critical ICT third-party service providers established in third countries. In order to ensure the enforceability of such penalties, and to allow a swift roll out of procedures upholding the critical ICT third-party service providers' rights of defence in the context of the designation mechanism and the issuance of recommendations, those critical ICT third-party service providers, providing services to financial entities that affect the supply of financial services, should be required to maintain an adequate business presence in the Union. Due to the nature of the oversight, and the absence of comparable arrangements in other jurisdictions, there are no suitable alternative mechanisms ensuring this objective

by way of effective cooperation with financial supervisors in third countries in relation to the monitoring of the impact of digital operational risks posed by systemic ICT third-party service providers, qualifying as critical ICT third-party service providers established in third countries. Therefore, in order to continue its provision of ICT services to financial entities in the Union, an ICT third-party service provider established in a third country which has been designated as critical in accordance with this Regulation should undertake, within 12 months of such designation, all necessary arrangements to ensure its incorporation within the Union, by means of establishing a subsidiary, as defined throughout the Union *acquis*, namely in Directive 2013/34/EU of the European Parliament and of the Council<sup>21</sup>. [↪ Art. 35\(6\)](#)

- (82) The requirement to set up a subsidiary in the Union should not prevent the critical ICT third-party service provider from supplying ICT services and related technical support from facilities and infrastructure located outside the Union. This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union.
- (83) Critical ICT third-party service providers should be able to provide ICT services from anywhere in the world, not necessarily or not only from premises located in the Union. Oversight activities should be first conducted on premises located in the Union and by interacting with entities located in the Union, including the subsidiaries established by critical ICT third-party service providers pursuant to this Regulation. However, such actions within the Union might be insufficient to allow the Lead Overseer to fully and effectively perform its duties under this Regulation. The Lead Overseer should therefore also be able to exercise its relevant oversight powers in third countries. Exercising those powers in third countries should allow the Lead Overseer to examine the facilities from which the ICT services or the technical support services are actually provided or managed by the critical ICT third-party service provider, and should give the Lead Overseer a comprehensive and operational understanding of the ICT risk management of the critical ICT third-party service provider. The possibility for the Lead Overseer, as a Union agency, to exercise powers outside the territory of the Union should be duly framed by relevant conditions, in particular the consent of the critical ICT third-party service provider concerned. Similarly, the relevant authorities of the third country should be informed of, and not have objected to, the exercise on their own territory of the activities of the Lead Overseer. However, in order to ensure efficient implementation, and without prejudice to the respective competences of the Union institutions and the Member States, such powers also need to be fully anchored in the conclusion of administrative cooperation arrangements with the relevant authorities of the third country concerned. This Regulation should therefore enable the ESAs to conclude administrative cooperation arrangements with the relevant authorities of third countries, which should not otherwise create legal obligations in respect of the Union and its Member States. [↪ Art. 36](#)
- (84) To facilitate communication with the Lead Overseer and to ensure adequate representation, critical ICT third-party service providers which are part of a group should designate one legal person as their coordination point. [↪ Art. 31\(4\)](#)
- (85) The Oversight Framework should be without prejudice to Member States' competence to conduct their own oversight or monitoring missions in respect to ICT third-party service providers which are not designated as critical under this Regulation, but which are regarded as important at national level.
- (86) To leverage the multi-layered institutional architecture in the financial services area, the Joint Committee of the ESAs should continue to ensure overall cross-sectoral coordination in relation to all matters pertaining to ICT risk, in accordance with its tasks on cybersecurity. It should be supported by a new Subcommittee (the 'Oversight Forum') carrying out preparatory work both for the individual decisions addressed to critical ICT third-party service providers, and for the issuing of collective recommendations, in particular in relation to benchmarking the oversight programmes for critical ICT third-party service providers, and identifying best practices for addressing ICT concentration risk issues. [↪ Art. 32](#)
- (87) To ensure that critical ICT third-party service providers are appropriately and effectively overseen on a Union level, this Regulation provides that any of the three ESAs could be designated as a Lead Overseer. The individual assignment of a critical ICT third-party service provider to one of the three ESAs should

---

<sup>21</sup> Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).



result from an assessment of the preponderance of financial entities operating in the financial sectors for which that ESA has responsibilities. This approach should lead to a balanced allocation of tasks and responsibilities between the three ESAs, in the context of exercising the oversight functions, and should make the best use of the human resources and technical expertise available in each of the three ESAs. [↪ Art. 31\(1\) and Art. 31\(2\)](#)

- (88) Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third-party service providers and to obtain complete and updated information. Those powers should enable the Lead Overseer to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to financial entities and ultimately to the Union's financial system. Entrusting the ESAs with the lead oversight role is a prerequisite for understanding and addressing the systemic dimension of ICT risk in finance. The impact of critical ICT third-party service providers on the Union financial sector and the potential issues caused by the ICT concentration risk entailed call for taking a collective approach at Union level. The simultaneous carrying out of multiple audits and access rights, performed separately by numerous competent authorities, with little or no coordination among them, would prevent financial supervisors from obtaining a complete and comprehensive overview of ICT third-party risk in the Union, while also creating redundancy, burden and complexity for critical ICT third-party service providers if they were subject to numerous monitoring and inspection requests. [↪ Art. 35\(1\)](#)
- (89) Due to the significant impact of being designated as critical, this Regulation should ensure that the rights of critical ICT third-party service providers are observed throughout the implementation of the Oversight Framework. Prior to being designated as critical, such providers should, for example, have the right to submit to the Lead Overseer a reasoned statement containing any relevant information for the purposes of the assessment related to their designation. Since the Lead Overseer should be empowered to submit recommendations on ICT risk matters and suitable remedies thereto, which include the power to oppose certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system, critical ICT third-party service providers should also be given the opportunity to provide, prior to the finalisation of those recommendations, explanations regarding the expected impact of the solutions, envisaged in the recommendations, on customers that are entities falling outside the scope of this Regulation and to formulate solutions to mitigate risks. Critical ICT third-party service providers disagreeing with the recommendations should submit a reasoned explanation of their intention not to endorse the recommendation. Where such reasoned explanation is not submitted or where it is considered to be insufficient, the Lead Overseer should issue a public notice summarily describing the matter of non-compliance. [↪ Art. 35\(3\)](#)
- (90) Competent authorities should duly include the task of verifying substantive compliance with recommendations issued by the Lead Overseer in their functions with regard to prudential supervision of financial entities. Competent authorities should be able to require financial entities to take additional measures to address the risks identified in the Lead Overseer's recommendations, and should, in due course, issue notifications to that effect. Where the Lead Overseer addresses recommendations to critical ICT third-party service providers that are supervised under Directive (EU) 2022/2555, the competent authorities should be able, on a voluntary basis and before adopting additional measures, to consult the competent authorities under that Directive in order to foster a coordinated approach to dealing with the critical ICT third-party service providers in question.
- (91) The exercise of the oversight should be guided by three operational principles seeking to ensure: (a) close coordination among the ESAs in their Lead Overseer roles, through a joint oversight network (JON), (b) consistency with the framework established by Directive (EU) 2022/2555 (through a voluntary consultation of bodies under that Directive to avoid duplication of measures directed at critical ICT third-party service providers), and (c) applying diligence to minimise the potential risk of disruption to services provided by the critical ICT third-party service providers to customers that are entities falling outside the scope of this Regulation. [↪ Art. 34](#)
- (92) The Oversight Framework should not replace, or in any way or for any part substitute for, the requirement for financial entities to manage themselves the risks entailed by the use of ICT third-party service providers, including their obligation to maintain an ongoing monitoring of contractual arrangements concluded with critical ICT third-party service providers. Similarly, the Oversight Framework should not

affect the full responsibility of financial entities for complying with, and discharging, all the legal obligations laid down in this Regulation and in the relevant financial services law.

- (93) To avoid duplications and overlaps, competent authorities should refrain from taking individually any measures aiming to monitor the critical ICT third-party service provider's risks and should, in that respect, rely on the relevant Lead Overseer's assessment. Any measures should in any case be coordinated and agreed in advance with the Lead Overseer in the context of the exercise of tasks in the Oversight Framework.
- (94) To promote convergence at international level as regards the use of best practices in the review and monitoring of ICT third-party service providers' digital risk-management, the ESAs should be encouraged to conclude cooperation arrangements with relevant supervisory and regulatory third-country authorities. [↪ Art. 36\(2\) and Art. 44](#)
- (95) To leverage the specific competences, technical skills and expertise of staff specialising in operational and ICT risk within the competent authorities, the three ESAs and, on a voluntary basis, the competent authorities under Directive (EU) 2022/2555, the Lead Overseer should draw on national supervisory capabilities and knowledge and set up dedicated examination teams for each critical ICT third-party service provider, pooling multidisciplinary teams in support of the preparation and execution of oversight activities, including general investigations and inspections of critical ICT third-party service providers, as well as for any necessary follow-up thereto.
- (96) Whereas costs resulting from oversight tasks would be fully funded from fees levied on critical ICT third-party service providers, the ESAs are, however, likely to incur, before the start of the Oversight Framework, costs for the implementation of dedicated ICT systems supporting the upcoming oversight, since dedicated ICT systems would need to be developed and deployed beforehand. This Regulation therefore provides for a hybrid funding model, whereby the Oversight Framework would, as such, be fully fee-funded, while the development of the ESAs' ICT systems would be funded from Union and national competent authorities' contributions. [↪ Art. 43](#)
- (97) Competent authorities should have all required supervisory, investigative and sanctioning powers to ensure the proper exercise of their duties under this Regulation. They should, in principle, publish notices of the administrative penalties they impose. Since financial entities and ICT third-party service providers can be established in different Member States and supervised by different competent authorities, the application of this Regulation should be facilitated by, on the one hand, close cooperation among relevant competent authorities, including the ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013, and, on the other hand, by consultation with the ESAs through the mutual exchange of information and the provision of assistance in the context of relevant supervisory activities. [↪ Art. 50](#)
- (98) In order to further quantify and qualify the criteria for the designation of ICT third-party service providers as critical and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Regulation by further specifying the systemic impact that a failure or operational outage of an ICT third-party service provider could have on the financial entities it provides ICT services to, the number of global systemically important institutions (G-SIIs), or other systemically important institutions (O-SIIs), that rely on the ICT third-party service provider in question, the number of ICT third-party service providers active on a given market, the costs of migrating data and ICT workloads to other ICT third-party service providers, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making<sup>22</sup>. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

---

<sup>22</sup> OJ L 123, 12.5.2016, p. 1.

- (99) Regulatory technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. In their roles as bodies endowed with highly specialised expertise, the ESAs should develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, major ICT-related incident reporting, testing, as well as in relation to key requirements for a sound monitoring of ICT third-party risk. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. The Commission should be empowered to adopt those regulatory technical standards by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. [↪ JC 2023 70, JC 2023 83 and JC 2023 86](#)
- (100) To facilitate the comparability of reports on major ICT-related incidents and major operational or security payment-related incidents, as well as to ensure transparency regarding contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident and a major operational or security payment-related incident, as well as standardised templates for the register of information. When developing those standards, the ESAs should take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. [↪ JC 2023 70](#)
- (101) Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009<sup>23</sup>, (EU) No 648/2012<sup>24</sup>, (EU) No 600/2014<sup>25</sup> and (EU) No 909/2014<sup>26</sup> of the European Parliament and of the Council, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules. [↪ JC 2023 86](#)
- (102) Since this Regulation, together with Directive (EU) 2022/2556 of the European Parliament and of the Council<sup>27</sup>, entails a consolidation of the ICT risk management provisions across multiple regulations and directives of the Union's financial services *acquis*, including Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, and Regulation (EU) 2016/1011 of the European Parliament and of the Council<sup>28</sup>, in order to ensure full consistency, those Regulations should be amended to clarify that the applicable ICT risk-related provisions are laid down in this Regulation.
- (103) Consequently, the scope of the relevant articles related to operational risk, upon which empowerments laid down in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 had mandated the adoption of delegated and implementing acts, should be narrowed down with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those Regulations.
- (104) The potential systemic cyber risk associated with the use of ICT infrastructures that enable the operation of payment systems and the provision of payment processing activities should be duly addressed at Union

<sup>23</sup> Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ L 302, 17.11.2009, p. 1).

<sup>24</sup> 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).

<sup>25</sup> 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).

<sup>26</sup> 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).

<sup>27</sup> Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (see page 153 of this Official Journal).

<sup>28</sup> Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1).

level through harmonised digital resilience rules. To that effect, the Commission should swiftly assess the need for reviewing the scope of this Regulation while aligning such review with the outcome of the comprehensive review envisaged under Directive (EU) 2015/2366. Numerous large-scale attacks over the past decade demonstrate how payment systems have become exposed to cyber threats. Placed at the core of the payment services chain and showing strong interconnections with the overall financial system, payment systems and payment processing activities acquired a critical significance for the functioning of the Union financial markets. Cyber-attacks on such systems can cause severe operational business disruptions with direct repercussions on key economic functions, such as the facilitation of payments, and indirect effects on related economic processes. Until a harmonised regime and the supervision of operators of payment systems and processing entities are put in place at Union level, Member States may, with a view to applying similar market practices, draw inspiration from the digital operational resilience requirements laid down by this Regulation, when applying rules to operators of payment systems and processing entities supervised under their own jurisdictions.

(105) Since the objective of this Regulation, namely to achieve a high level of digital operational resilience for regulated financial entities, cannot be sufficiently achieved by the Member States because it requires harmonisation of various different rules in Union and national law, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(106) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council<sup>29</sup> and delivered an opinion on 10 May 2021<sup>30</sup>,

HAVE ADOPTED THIS REGULATION:

---

<sup>29</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>30</sup> OJ C 229, 15.6.2021, p. 16.

## CHAPTER I

### GENERAL PROVISIONS

#### Article 1

##### Subject matter

1. In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

- (a) requirements applicable to financial entities in relation to:
  - (i) information and communication technology (ICT) risk management;
  - (ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
  - (iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d);
  - (iv) digital operational resilience testing;
  - (v) information and intelligence sharing in relation to cyber threats and vulnerabilities;
  - (vi) measures for the sound management of ICT third-party risk;
- (b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;
- (c) rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities;
- (d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

2. In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive.

3. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

## Article 2

### Scope

1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:

- (a) credit institutions;
- (b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
- (c) account information service providers;
- (d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;
- (e) investment firms;
- (f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;
- (g) central securities depositories;
- (h) central counterparties;
- (i) trading venues;
- (j) trade repositories;
- (k) managers of alternative investment funds;
- (l) management companies;
- (m) data reporting service providers;
- (n) insurance and reinsurance undertakings;
- (o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
- (p) institutions for occupational retirement provision;
- (q) credit rating agencies;
- (r) administrators of critical benchmarks;
- (s) crowdfunding service providers;
- (t) securitisation repositories;
- (u) ICT third-party service providers.

2. For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

3. This Regulation does not apply to:

- (a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU;
- (b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC;
- (c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;
- (d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU;
- (e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises;
- (f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. Member States may exclude from the scope of this Regulation entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes thereto. The Commission shall make that information publicly available on its website or other easily accessible means.

## Article 3

### Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions;

(2) 'network and information system' means a network and information system as defined in Article 6, point 1, of Directive (EU) 2022/2555;

(3) 'legacy ICT system' means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity;

(4) 'security of network and information systems' means security of network and information systems as defined in Article 6, point 2, of Directive (EU) 2022/2555;

(5) 'ICT risk' means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment;

(6) 'information asset' means a collection of information, either tangible or intangible, that is worth protecting;

(7) 'ICT asset' means a software or hardware asset in the network and information systems used by the financial entity;

(8) 'ICT-related incident' means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity;

(9) 'operational or security payment-related incident' means a single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity;

(10) 'major ICT-related incident' means an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity;

(11) 'major operational or security payment-related incident' means an operational or security payment-related incident that has a high adverse impact on the payment-related services provided;

(12) 'cyber threat' means 'cyber threat' as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(13) 'significant cyber threat' means a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident;



(14) 'cyber-attack' means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset;

(15) 'threat intelligence' means information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and to enable relevant and sufficient understanding in order to mitigate the impact of an ICT-related incident or of a cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations;

(16) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited;

(17) 'threat-led penetration testing (TLPT)' means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems;

(18) 'ICT third-party risk' means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements;

(19) 'ICT third-party service provider' means an undertaking providing ICT services;

(20) 'ICT intra-group service provider' means an undertaking that is part of a financial group and that provides predominantly ICT services to financial entities within the same group or to financial entities belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries, branches or other entities that are under common ownership or control;

(21) 'ICT services' means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services;

(22) 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law;

(23) 'critical ICT third-party service provider' means an ICT third-party service provider designated as critical in accordance with Article 31;

(24) 'ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal person established in a third-country and that has entered into a contractual arrangement with a financial entity for the provision of ICT services;

(25) 'subsidiary' means a subsidiary undertaking within the meaning of Article 2, point (10), and Article 22 of Directive 2013/34/EU;

(26) 'group' means a group as defined in Article 2, point (11), of Directive 2013/34/EU;

(27) 'parent undertaking' means a parent undertaking within the meaning of Article 2, point (9), and Article 22 of Directive 2013/34/EU;

(28) 'ICT subcontractor established in a third country' means an ICT subcontractor that is a legal person established in a third-country and that has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;

(29) 'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole;

(30) 'management body' means a management body as defined in Article 4(1), point (36), of Directive 2014/65/EU, Article 3(1), point (7), of Directive 2013/36/EU, Article 2(1), point (s), of Directive 2009/65/EC of the European Parliament and of the Council<sup>31</sup>, Article 2(1), point (45), of Regulation (EU) No 909/2014, Article 3(1), point (20), of Regulation (EU) 2016/1011, and in the relevant provision of the Regulation on markets in crypto-assets, or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law;

(31) 'credit institution' means a credit institution as defined in Article 4(1), point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council<sup>32</sup>;

(32) 'institution exempted pursuant to Directive 2013/36/EU' means an entity as referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU;

(33) 'investment firm' means an investment firm as defined in Article 4(1), point (1), of Directive 2014/65/EU;

(34) 'small and non-interconnected investment firm' means an investment firm that meets the conditions laid out in Article 12(1) of Regulation (EU) 2019/2033 of the European Parliament and of the Council<sup>33</sup>;

(35) 'payment institution' means a payment institution as defined in Article 4, point (4), of Directive (EU) 2015/2366;

(36) 'payment institution exempted pursuant to Directive (EU) 2015/2366' means a payment institution exempted pursuant to Article 32(1) of Directive (EU) 2015/2366;

(37) 'account information service provider' means an account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;

(38) 'electronic money institution' means an electronic money institution as defined in Article 2, point (1), of Directive 2009/110/EC of the European Parliament and of the Council;

(39) 'electronic money institution exempted pursuant to Directive 2009/110/EC' means an electronic money institution benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC;

(40) 'central counterparty' means a central counterparty as defined in Article 2, point (1), of Regulation (EU) No 648/2012;

---

<sup>31</sup> Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (OJ L 302, 17.11.2009, p. 32).

<sup>32</sup> Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

<sup>33</sup> Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (OJ L 314, 5.12.2019, p. 1).

- 
- (41) 'trade repository' means a trade repository as defined in Article 2, point (2), of Regulation (EU) No 648/2012;
- (42) 'central securities depository' means a central securities depository as defined in Article 2(1), point (1), of Regulation (EU) No 909/2014;
- (43) 'trading venue' means a trading venue as defined in Article 4(1), point (24), of Directive 2014/65/EU;
- (44) 'manager of alternative investment funds' means a manager of alternative investment funds as defined in Article 4(1), point (b), of Directive 2011/61/EU;
- (45) 'management company' means a management company as defined in Article 2(1), point (b), of Directive 2009/65/EC;
- (46) 'data reporting service provider' means a data reporting service provider within the meaning of Regulation (EU) No 600/2014, as referred to in Article 2(1), points (34) to (36) thereof;
- (47) 'insurance undertaking' means an insurance undertaking as defined in Article 13, point (1), of Directive 2009/138/EC;
- (48) 'reinsurance undertaking' means a reinsurance undertaking as defined in Article 13, point (4), of Directive 2009/138/EC;
- (49) 'insurance intermediary' means an insurance intermediary as defined in Article 2(1), point (3), of Directive (EU) 2016/97 of the European Parliament and of the Council<sup>34</sup>;
- (50) 'ancillary insurance intermediary' means an ancillary insurance intermediary as defined in Article 2(1), point (4), of Directive (EU) 2016/97;
- (51) 'reinsurance intermediary' means a reinsurance intermediary as defined in Article 2(1), point (5), of Directive (EU) 2016/97;
- (52) 'institution for occupational retirement provision' means an institution for occupational retirement provision as defined in Article 6, point (1), of Directive (EU) 2016/2341;
- (53) 'small institution for occupational retirement provision' means an institution for occupational retirement provision which operates pension schemes which together have less than 100 members in total;
- (54) 'credit rating agency' means a credit rating agency as defined in Article 3(1), point (b), of Regulation (EC) No 1060/2009;
- (55) 'crypto-asset service provider' means a crypto-asset service provider as defined in the relevant provision of the Regulation on markets in crypto-assets;
- (56) 'issuer of asset-referenced tokens' means an issuer of asset-referenced tokens as defined in the relevant provision of the Regulation on markets in crypto-assets;
- (57) 'administrator of critical benchmarks' means an administrator of 'critical benchmarks' as defined in Article 3(1), point (25), of Regulation (EU) 2016/1011;

---

<sup>34</sup> Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).

## ARTICLE 3

---

(58) 'crowdfunding service provider' means a crowdfunding service provider as defined in Article 2(1), point (e), of Regulation (EU) 2020/1503 of the European Parliament and of the Council<sup>35</sup>;

(59) 'securitisation repository' means a securitisation repository as defined in Article 2, point (23), of Regulation (EU) 2017/2402 of the European Parliament and of the Council<sup>36</sup>;

(60) 'microenterprise' means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million;

(61) 'Lead Overseer' means the European Supervisory Authority appointed in accordance with Article 31(1), point (b) of this Regulation;

(62) 'Joint Committee' means the committee referred to in Article 54 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010;

(63) 'small enterprise' means a financial entity that employs 10 or more persons, but fewer than 50 persons, and has an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but does not exceed EUR 10 million;

(64) 'medium-sized enterprise' means a financial entity that is not a small enterprise and employs fewer than 250 persons and has an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million;

(65) 'public authority' means any government or other public administration entity, including national central banks.

---

<sup>35</sup> Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (OJ L 347, 20.10.2020, p. 1).

<sup>36</sup> Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012 (OJ L 347, 28.12.2017, p. 35).

## Article 4

### Proportionality principle

1. Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.
2. In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.
3. The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework on the basis of the reports submitted upon the request of competent authorities pursuant to Article 6(5) and Article 16(2).

## CHAPTER II

### ICT RISK MANAGEMENT

#### Section I

#### Article 5

##### Governance and organisation

1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.

2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).

For the purposes of the first subparagraph, the management body shall:

- (a) bear the ultimate responsibility for managing the financial entity's ICT risk;
- (b) put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;
- (c) set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;
- (d) bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);
- (e) approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan;
- (f) approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;
- (g) allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff;
- (h) approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;
- (i) put in place, at corporate level, reporting channels enabling it to be duly informed of the following:

- (i) arrangements concluded with ICT third-party service providers on the use of ICT services,
- (ii) any relevant planned material changes regarding the ICT third-party service providers,
- (iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.

3. Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

4. Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.

## Section II

### Article 6

#### ICT risk management framework

1. Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.
2. The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.
3. In accordance with their ICT risk management framework, financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.
4. Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.
5. The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.
6. The ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.
7. Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings.
8. The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:
  - (a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;
  - (b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;
  - (c) setting out clear information security objectives, including key performance indicators and key risk metrics;



- (d) explaining the ICT reference architecture and any changes needed to reach specific business objectives;
- (e) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;
- (f) evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;
- (g) implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;
- (h) outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.

9. Financial entities may, in the context of the digital operational resilience strategy referred to in paragraph 8, define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.

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

## Article 7

### ICT systems, protocols and tools

In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are:

- (a) appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4;
- (b) reliable;
- (c) equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced;
- (d) technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.

## Article 8

### Identification

1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
2. Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.
3. Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.
4. Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.
5. Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.
6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.
7. Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.

## Article 9

### Protection and prevention

1. For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.
2. Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.
3. In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4. Those ICT solutions and processes shall:
  - (a) ensure the security of the means of transfer of data;
  - (b) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;
  - (c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;
  - (d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.
4. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:
  - (a) develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable;
  - (b) following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks;
  - (c) implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;
  - (d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;
  - (e) implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;
  - (f) have appropriate and comprehensive documented policies for patches and updates.

For the purposes of the first subparagraph, point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimise and prevent contagion, especially for interconnected financial processes.

For the purposes of the first subparagraph, point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols in place.

## Article 10

### Detection

1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.

All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.

2. The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.

3. Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

4. Data reporting service providers shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports.

## Article 11

### Response and recovery

1. As part of the ICT risk management framework referred to in Article 6(1) and based on the identification requirements set out in Article 8, financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.
2. Financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to:
  - (a) ensure the continuity of the financial entity's critical or important functions;
  - (b) quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions;
  - (c) activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12;
  - (d) estimate preliminary impacts, damages and losses;
  - (e) set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.
3. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to independent internal audit reviews.
4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.
5. As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities shall assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.
6. As part of their comprehensive ICT risk management, financial entities shall:
  - (a) test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions;
  - (b) test the crisis communication plans established in accordance with Article 14.

For the purposes of the first subparagraph, point (a), financial entities, other than microenterprises, shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 12.

Financial entities shall regularly review their ICT business continuity policy and ICT response and recovery plans, taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.

7. Financial entities, other than microenterprises, shall have a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications in accordance with Article 14.

8. Financial entities shall keep readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated.

9. Central securities depositories shall provide the competent authorities with copies of the results of the ICT business continuity tests, or of similar exercises.

10. Financial entities, other than microenterprises, shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.

11. In accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs, through the Joint Committee, shall by 17 July 2024 develop common guidelines on the estimation of aggregated annual costs and losses referred to in paragraph 10.



## Article 12

### Backup policies and procedures, restoration and recovery procedures and methods

1. For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:

(a) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data;

(b) restoration and recovery procedures and methods.

2. Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.

3. When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.

For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.

Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.

4. Financial entities, other than microenterprises, shall maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs. Microenterprises shall assess the need to maintain such redundant ICT capacities based on their risk profile.

5. Central securities depositories shall maintain at least one secondary processing site endowed with adequate resources, capabilities, functions and staffing arrangements to ensure business needs.

The secondary processing site shall be:

(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;

(b) capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;

(c) immediately accessible to the financial entity's staff to ensure continuity of critical or important functions in the event that the primary processing site has become unavailable.

6. In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.

7. When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

## Article 13

### Learning and evolving

1. Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.

2. Financial entities shall put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy referred to in Article 11.

Financial entities, other than microenterprises, shall, upon request, communicate to the competent authorities, the changes that were implemented following post ICT-related incident reviews as referred to in the first subparagraph.

The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to the following:

- (a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;
- (b) the quality and speed of performing a forensic analysis, where deemed appropriate;
- (c) the effectiveness of incident escalation within the financial entity;
- (d) the effectiveness of internal and external communication.

3. Lessons derived from the digital operational resilience testing carried out in accordance with Articles 26 and 27 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans, together with relevant information exchanged with counterparts and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. Those findings shall form the basis for appropriate reviews of relevant components of the ICT risk management framework referred to in Article 6(1).

4. Financial entities shall monitor the effectiveness of the implementation of their digital operational resilience strategy set out in Article 6(8). They shall map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness of the financial entity.

5. Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.

6. Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i).

7. Financial entities, other than microenterprises, shall monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. They shall keep up-to-date with the latest ICT risk management processes, in order to effectively combat current or new forms of cyber-attacks.

## Article 14

### Communication

1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.
2. As part of the ICT risk management framework, financial entities shall implement communication policies for internal staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed.
3. At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose.

## Article 15

### Further harmonisation of ICT risk management tools, methods, processes and policies

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

- (a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2), with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays;
- (b) develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;
- (c) develop further the mechanisms specified in Article 10(1) enabling a prompt detection of anomalous activities and the criteria set out in Article 10(2) triggering ICT-related incident detection and response processes;
- (d) specify further the components of the ICT business continuity policy referred to in Article 11(1);
- (e) specify further the testing of ICT business continuity plans referred to in Article 11(6) to ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;
- (f) specify further the components of the ICT response and recovery plans referred to in Article 11(3);
- (g) specifying further the content and format of the report on the review of the ICT risk management framework referred to in Article 6(5);

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

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

▪ **Appendix V**

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first paragraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 16

### Simplified ICT risk management framework

1. Articles 5 to 15 of this Regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision.

Without prejudice to the first subparagraph, the entities listed in the first subparagraph shall:

- (a) put in place and maintain a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of ICT risk, including for the protection of relevant physical components and infrastructures;
- (b) continuously monitor the security and functioning of all ICT systems;
- (c) minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems;
- (d) allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled;
- (e) identify key dependencies on ICT third-party service providers;
- (f) ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures;
- (g) test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c);
- (h) implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process and develop, according to needs and ICT risk profile, ICT security awareness programmes and digital operational resilience training for staff and management.

2. The ICT risk management framework referred to in paragraph 1, second subparagraph, point (a), shall be documented and reviewed periodically and upon the occurrence of major ICT-related incidents in compliance with supervisory instructions. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.

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

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

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

(d) specify further the rules on the testing of business continuity plans and ensure the effectiveness of the controls referred to in paragraph 1, second subparagraph, point (g) and ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails;

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

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

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

▪ *Appendix V*

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## CHAPTER III

### ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION AND REPORTING

#### Article 17

##### ICT-related incident management process

1. Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.
2. Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.
3. The ICT-related incident management process referred to in paragraph 1 shall:
  - (a) put in place early warning indicators;
  - (b) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted, in accordance with the criteria set out in Article 18(1);
  - (c) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;
  - (d) set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;
  - (e) ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents;
  - (f) establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.



## Article 18

### Classification of ICT-related incidents and cyber threats

1. Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:

(a) the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;

(b) the duration of the ICT-related incident, including the service downtime;

(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;

(d) the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;

(e) the criticality of the services affected, including the financial entity's transactions and operations;

(f) the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.

2. Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.

3. The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards further specifying the following:

▪ **Appendix III**

(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1);

(b) the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to relevant competent authorities in other Member States', and the details of reports of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to be shared with other competent authorities pursuant to Article 19(6) and (7);

(c) the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.

4. When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2), as well as international standards, guidance and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.

The ESAs shall submit those common draft regulatory technical standards to the Commission by 17 January 2024.

## ARTICLE 18

---

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 19

### Reporting of major ICT-related incidents and voluntary notification of significant cyber threats

1. Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article.

Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this Article.

Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall report major ICT-related incidents to the relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit that report to the ECB.

For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, the initial notification and reports referred to in paragraph 4 of this Article using the templates referred to in Article 20 and submit them to the competent authority. In the event that a technical impossibility prevents the submission of the initial notification using the template, financial entities shall notify the competent authority about it via alternative means.

The initial notification and reports referred to in paragraph 4 shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.

Without prejudice to the reporting pursuant to the first subparagraph by the financial entity to the relevant competent authority, Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report referred to in paragraph 4 of this Article using the templates referred to in Article 20 to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555.

2. Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.

Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, may, on a voluntary basis, notify significant cyber threats to relevant national competent authority, designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit the notification to the ECB.

Member States may determine that those financial entities that on a voluntary basis notify in accordance with the first subparagraph may also transmit that notification to the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.

3. Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.

In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.

4. Financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit the following to the relevant competent authority:

- (a) an initial notification;
- (b) an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;
- (c) a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.

5. Financial entities may outsource, in accordance with Union and national sectoral law, the reporting obligations under this Article to a third-party service provider. In case of such outsourcing, the financial entity remains fully responsible for the fulfilment of the incident reporting requirements.

6. Upon receipt of the initial notification and of each report referred to in paragraph 4, the competent authority shall, in a timely manner, provide details of the major ICT-related incident to the following recipients based, as applicable, on their respective competences:

- (a) EBA, ESMA or EIOPA;
- (b) the ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d);
- (c) the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;
- (d) the resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014 of the European Parliament and of the Council<sup>37</sup>, and with respect to entities and groups referred to in Article 7(4)(b) and (5) of Regulation (EU) No 806/2014 if such details concern incidents that pose a risk to ensuring critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU; and
- (e) other relevant public authorities under national law.

7. Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess whether the major ICT-related incident is relevant for competent authorities in other Member States. Following that assessment, EBA, ESMA or EIOPA shall, as soon as possible, notify relevant competent authorities in other Member States accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.

8. The notification to be done by ESMA pursuant to paragraph 7 of this Article shall be without prejudice to the responsibility of the competent authority to urgently transmit the details of the major ICT-related incident to the relevant authority in the host Member State, where a central securities depository has significant cross-border activity in the host Member State, the major ICT-related incident is likely to have severe consequences for the financial markets of the host Member State and where there are cooperation arrangements among competent authorities related to the supervision of financial entities.

---

<sup>37</sup> Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 (OJ L 225, 30.7.2014, p. 1).

## Article 20

### Harmonisation of reporting content and templates

The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop:

(a) common draft regulatory technical standards in order to:

▪ *Appendix VII*

- (i) establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not;
- (ii) determine the time limits for the initial notification and for each report referred to in Article 19(4);
- (iii) establish the content of the notification for significant cyber threats.

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive;

(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.

▪ *Appendix VII*

The ESAs shall submit the common draft regulatory technical standards referred to in the first paragraph, point (a), and the common draft implementing technical standards referred to in the first paragraph, point (b), to the Commission by 17 July 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in the first paragraph, point (a), in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

Power is conferred on the Commission to adopt the common implementing technical standards referred to in the first paragraph, point (b), in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 21

### Centralisation of reporting of major ICT-related incidents

1. The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The joint report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.
2. The joint report referred to in paragraph 1 shall comprise at least the following elements:
  - (a) prerequisites for the establishment of a single EU Hub;
  - (b) benefits, limitations and risks, including risks associated with the high concentration of sensitive information;
  - (c) the necessary capability to ensure interoperability with regard to other relevant reporting schemes;
  - (d) elements of operational management;
  - (e) conditions of membership;
  - (f) technical arrangements for financial entities and national competent authorities to access the single EU Hub;
  - (g) a preliminary assessment of financial costs incurred by setting-up the operational platform supporting the single EU Hub, including the requisite expertise.
3. The ESAs shall submit the report referred to in paragraph 1 to the European Parliament, to the Council and to the Commission by 17 January 2025.

## Article 22

### Supervisory feedback

1. Without prejudice to the technical input, advice or remedies and subsequent follow-up which may be provided, where applicable, in accordance with national law, by the CSIRTs under Directive (EU) 2022/2555, the competent authority shall, upon receipt of the initial notification and of each report as referred to in Article 19(4), acknowledge receipt and may, where feasible, provide in a timely manner relevant and proportionate feedback or high-level guidance to the financial entity, in particular by making available any relevant anonymised information and intelligence on similar threats, and may discuss remedies applied at the level of the financial entity and ways to minimise and mitigate adverse impact across the financial sector. Without prejudice to the supervisory feedback received, financial entities shall remain fully responsible for the handling and for consequences of the ICT-related incidents reported pursuant to Article 19(1).

2. The ESAs shall, through the Joint Committee, on an anonymised and aggregated basis, report yearly on major ICT-related incidents, the details of which shall be provided by competent authorities in accordance with Article 19(6), setting out at least the number of major ICT-related incidents, their nature and their impact on the operations of financial entities or clients, remedial actions taken and costs incurred.

The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.



## **Article 23**

### **Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions**

The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.

---

## CHAPTER IV

### DIGITAL OPERATIONAL RESILIENCE TESTING

#### Article 24

##### General requirements for the performance of digital operational resilience testing

1. For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6.
2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26.
3. When conducting the digital operational resilience testing programme referred to in paragraph 1 of this Article, financial entities, other than microenterprises, shall follow a risk-based approach taking into account the criteria set out in Article 4(2) duly considering the evolving landscape of ICT risk, any specific risks to which the financial entity concerned is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.
4. Financial entities, other than microenterprises, shall ensure that tests are undertaken by independent parties, whether internal or external. Where tests are undertaken by an internal tester, financial entities shall dedicate sufficient resources and ensure that conflicts of interest are avoided throughout the design and execution phases of the test.
5. Financial entities, other than microenterprises, shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.
6. Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.

## Article 25

### Testing of ICT tools and systems

1. The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.
2. Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity.
3. Microenterprises shall perform the tests referred to in paragraph 1 by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.

## Article 26

### Advanced testing of ICT tools, systems and processes based on TLPT

1. Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph, of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency.

2. Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.

Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers.

Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities.

3. Where ICT third-party service providers are included in the scope of TLPT, the financial entity shall take the necessary measures and safeguards to ensure the participation of such ICT third-party service providers in the TLPT and shall retain at all times full responsibility for ensuring compliance with this Regulation.

4. Without prejudice to paragraph 2, first and second subparagraphs, where the participation of an ICT third-party service provider in the TLPT, referred to in paragraph 3, is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services.

That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities participating in the pooled testing.

The number of financial entities participating in the pooled testing shall be duly calibrated taking into account the complexity and types of services involved.

5. Financial entities shall, with the cooperation of ICT third-party service providers and other parties involved, including the testers but excluding the competent authorities, apply effective risk management controls to mitigate the risks of any potential impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts or to the financial sector.

6. At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers shall provide to the authority, designated in accordance with paragraph 9 or 10, a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.

7. Authorities shall provide financial entities with an attestation confirming that the test was performed in accordance with the requirements as evidenced in the documentation in order to allow for mutual recognition of threat led penetration tests between competent authorities. The financial entity shall notify the relevant competent authority of the attestation, the summary of the relevant findings and the remediation plans.

Without prejudice to such attestation, financial entities shall remain at all times fully responsible for the impact of the tests referred to in paragraph 4.

8. Financial entities shall contract testers for the purposes of undertaking TLPT in accordance with Article 27. When financial entities use internal testers for the purposes of undertaking TLPT, they shall contract external testers every three tests.

Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall only use external testers in accordance with Article 27(1), points (a) to (e).

Competent authorities shall identify financial entities that are required to perform TLPT taking into account the criteria set out in Article 4(2), based on an assessment of the following:

- (a) impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;
- (b) possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;
- (c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.

9. Member States may designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level and shall entrust it with all competences and tasks to that effect.

10. In the absence of a designation in accordance with paragraph 9 of this Article, and without prejudice to the power to identify the financial entities that are required to perform TLPT, a competent authority may delegate the exercise of some or all of the tasks referred to in this Article and Article 27 to another national authority in the financial sector.

11. The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:

▪ *Appendix XI*

- (a) the criteria used for the purpose of the application of paragraph 8, second subparagraph;
- (b) the requirements and standards governing the use of internal testers;
- (c) the requirements in relation to:
  - (i) the scope of TLPT referred to in paragraph 2;
  - (ii) the testing methodology and approach to be followed for each specific phase of the testing process;
  - (iii) the results, closure and remediation stages of the testing;
- (d) the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.

When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 27

### Requirements for testers for the carrying out of TLPT

1. Financial entities shall only use testers for the carrying out of TLPT, that:
  - (a) are of the highest suitability and reputability;
  - (b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;
  - (c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;
  - (d) provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity;
  - (e) are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.
2. When using internal testers, financial entities shall ensure that, in addition to the requirements in paragraph 1, the following conditions are met:
  - (a) such use has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);
  - (b) the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test; and
  - (c) the threat intelligence provider is external to the financial entity.
3. Financial entities shall ensure that contracts concluded with external testers require a sound management of the TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the financial entity.



## CHAPTER V

### Managing of ICT third-party risk

#### Section I

#### Key principles for a sound management of ICT third-party risk

#### Article 28

##### General principles

1. Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1), and in accordance with the following principles:

(a) financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law;

(b) financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account:

- (i) the nature, scale, complexity and importance of ICT-related dependencies,
- (ii) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.

2. As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, shall adopt, and regularly review, a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9), where applicable. The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis. The management body shall, on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions.

3. As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.

Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided.

Financial entities shall make available to the competent authority, upon its request, the full register of information or, as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important.

4. Before entering into a contractual arrangement on the use of ICT services, financial entities shall:
  - (a) assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;
  - (b) assess if supervisory conditions for contracting are met;
  - (c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29;
  - (d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;
  - (e) identify and assess conflicts of interest that the contractual arrangement may cause.

5. Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards.

6. In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards.

Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments.

7. Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:

- (a) significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;
- (b) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;
- (c) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;
- (d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.

8. For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.

Financial entities shall ensure that they are able to exit contractual arrangements without:

- (a) disruption to their business activities,
- (b) limiting compliance with regulatory requirements,
- (c) detriment to the continuity and quality of services provided to clients.

Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.

Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house.

Financial entities shall have appropriate contingency measures in place to maintain business continuity in the event of the circumstances referred to in the first subparagraph.

9. The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information referred to in paragraph 3, including information that is common to all contractual arrangements on the use of ICT services. The ESAs shall submit those draft implementing technical standards to the Commission by 17 January 2024.

▪ *Appendix IV*

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

10. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2 in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

▪ *Appendix IV*

When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 29

### Preliminary assessment of ICT concentration risk at entity level

1. When performing the identification and assessment of risks referred to in Article 28(4), point (c), financial entities shall also take into account whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:

- (a) contracting an ICT third-party service provider that is not easily substitutable; or
- (b) having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.

Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.

2. Where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such subcontracting, in particular in the case of an ICT subcontractor established in a third-country.

Where contractual arrangements concern ICT services supporting critical or important functions, financial entities shall duly consider the insolvency law provisions that would apply in the event of the ICT third-party service provider's bankruptcy as well as any constraint that may arise in respect to the urgent recovery of the financial entity's data.

Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third country, financial entities shall, in addition to the considerations referred to in the second subparagraph, also consider the compliance with Union data protection rules and the effective enforcement of the law in that third country.

Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

## Article 30

### Key contractual provisions

1. The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.
2. The contractual arrangements on the use of ICT services shall include at least the following elements:
  - (a) a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;
  - (b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations;
  - (c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;
  - (d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;
  - (e) service level descriptions, including updates and revisions thereof;
  - (f) the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;
  - (g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;
  - (h) termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;
  - (i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).
3. The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following:
  - (a) full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;
  - (b) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service

provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;

(c) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;

(d) the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;

(e) the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:

(i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

(ii) the right to agree on alternative assurance levels if other clients' rights are affected;

(iii) the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and

(iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;

(f) exit strategies, in particular the establishment of a mandatory adequate transition period:

(i) during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;

(ii) allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.

By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.

4. When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities for specific services.

5. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

▪ *Appendix IV*

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

The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Section II

### Oversight Framework of critical ICT third-party service providers

#### Article 31

##### Designation of critical ICT third-party service providers

1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall:

(a) designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2;

(b) appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible, in accordance with Regulations (EU) No 1093/2010, (EU) No 1094/2010 or (EU) No 1095/2010, for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities using the services of the relevant critical ICT third-party service provider, as evidenced by the sum of the individual balance sheets of those financial entities.

2. The designation referred to in paragraph 1, point (a), shall be based on all of the following criteria in relation to ICT services provided by the ICT third-party service provider:

(a) the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services;

(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, assessed in accordance with the following parameters:

(i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;

(ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities, including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;

(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements;

(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:

(i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;



- (ii) difficulties in relation to partially or fully migrating the relevant data and workloads from the relevant ICT third-party service provider to another ICT third-party service provider, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk or other operational risks to which the financial entity may be exposed through such migration.

3. Where the ICT third-party service provider belongs to a group, the criteria referred to in paragraph 2 shall be considered in relation to the ICT services provided by the group as a whole.

4. Critical ICT third-party service providers which are part of a group shall designate one legal person as a coordination point to ensure adequate representation and communication with the Lead Overseer.

5. The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment leading to the designation referred in paragraph 1, point (a). Within 6 weeks from the date of the notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement with any relevant information for the purposes of the assessment. The Lead Overseer shall consider the reasoned statement and may request additional information to be submitted within 30 calendar days of the receipt of such statement.

After designating an ICT third-party service provider as critical, the ESAs, through the Joint Committee, shall notify the ICT third-party service provider of such designation and the starting date as from which they will effectively be subject to oversight activities. That starting date shall be no later than one month after the notification. The ICT third-party service provider shall notify the financial entities to which they provide services of their designation as critical.

6. The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 of this Article, by 17 July 2024.

7. The designation referred to in paragraph 1, point (a), shall not be used until the Commission has adopted a delegated act in accordance with paragraph 6.

8. The designation referred to in paragraph 1, point (a), shall not apply to the following:

- (i) financial entities providing ICT services to other financial entities;
- (ii) ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union;
- (iii) ICT intra-group service providers;
- (iv) ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State.

9. The ESAs, through the Joint Committee, shall establish, publish and update yearly the list of critical ICT third-party service providers at Union level.

10. For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis, transmit the reports referred to in Article 28(3), third subparagraph, to the Oversight Forum established pursuant to Article 32. The Oversight Forum shall assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.

11. The ICT third-party service providers that are not included in the list referred to in paragraph 9 may request to be designated as critical in accordance with paragraph 1, point (a).

For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to EBA, ESMA or EIOPA, which, through the Joint Committee, shall decide whether to designate that ICT third-party service provider as critical in accordance with paragraph 1, point (a).

The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.

12. Financial entities shall only make use of the services of an ICT third-party service provider established in a third country and which has been designated as critical in accordance with paragraph 1, point (a), if the latter has established a subsidiary in the Union within the 12 months following the designation.

13. The critical ICT third-party service provider referred to in paragraph 12 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.

## Article 32

### Structure of the Oversight Framework

1. The Joint Committee, in accordance with Article 57(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and of the Lead Overseer referred to in Article 31(1), point (b), in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and the draft common acts of the Joint Committee in that area.

The Oversight Forum shall regularly discuss relevant developments on ICT risk and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union level.

2. The Oversight Forum shall, on a yearly basis, undertake a collective assessment of the results and findings of the oversight activities conducted for all critical ICT third-party service providers and promote coordination measures to increase the digital operational resilience of financial entities, foster best practices on addressing ICT concentration risk and explore mitigants for cross-sector risk transfers.

3. The Oversight Forum shall submit comprehensive benchmarks for critical ICT third-party service providers to be adopted by the Joint Committee as joint positions of the ESAs in accordance with Article 56(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

4. The Oversight Forum shall be composed of:

(a) the Chairpersons of the ESAs;

(b) one high-level representative from the current staff of the relevant competent authority referred to in Article 46 from each Member State;

(c) the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA as observers;

(d) where appropriate, one additional representative of a competent authority referred to in Article 46 from each Member State as observer;

(e) where applicable, one representative of the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider, as observer.

The Oversight Forum may, where appropriate, seek the advice of independent experts appointed in accordance with paragraph 6.

5. Each Member State shall designate the relevant competent authority whose staff member shall be the high-level representative referred in paragraph 4, first subparagraph, point (b), and shall inform the Lead Overseer thereof.

The ESAs shall publish on their website the list of high-level representatives from the current staff of the relevant competent authority designated by Member States.

6. The independent experts referred to in paragraph 4, second subparagraph, shall be appointed by the Oversight Forum from a pool of experts selected following a public and transparent application process.

The independent experts shall be appointed on the basis of their expertise in financial stability, digital operational resilience and ICT security matters. They shall act independently and objectively in the sole interest of the Union

as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.

7. In accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs shall by 17 July 2024 issue, for the purposes of this Section, guidelines on the cooperation between the ESAs and the competent authorities covering the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs and the details on the exchanges of information which are necessary for competent authorities to ensure the follow-up of recommendations pursuant to Article 35(1), point (d), addressed to critical ICT third-party service providers.

8. The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2022/2555 and of other Union rules on oversight applicable to providers of cloud computing services.

9. The ESAs, through the Joint Committee and based on preparatory work conducted by the Oversight Forum, shall, on yearly basis, submit a report on the application of this Section to the European Parliament, the Council and the Commission.

## Article 33

### Tasks of the Lead Overseer

1. The Lead Overseer, appointed in accordance with Article 31(1), point (b), shall conduct the oversight of the assigned critical ICT third-party service providers and shall be, for the purposes of all matters related to the oversight, the primary point of contact for those critical ICT third-party service providers.

2. For the purposes of paragraph 1, the Lead Overseer shall assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities.

The assessment referred to in the first subparagraph shall focus mainly on ICT services provided by the critical ICT third-party service provider supporting the critical or important functions of financial entities. Where necessary to address all relevant risks, that assessment shall extend to ICT services supporting functions other than those that are critical or important.

3. The assessment referred to in paragraph 2 shall cover:

(a) ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of availability, authenticity, integrity or confidentiality of data;

(b) the physical security contributing to ensuring the ICT security, including the security of premises, facilities, data centres;

(c) the risk management processes, including ICT risk management policies, ICT business continuity policy and ICT response and recovery plans;

(d) the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling effective ICT risk management;

(e) the identification, monitoring and prompt reporting of material ICT-related incidents to financial entities, the management and resolution of those incidents, in particular cyber-attacks;

(f) the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities;

(g) the testing of ICT systems, infrastructure and controls;

(h) the ICT audits;

(i) the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.

4. Based on the assessment referred to in paragraph 2, and in coordination with the Joint Oversight Network (JON) referred to in Article 34(1), the Lead Overseer shall adopt a clear, detailed and reasoned individual oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider. That plan shall be communicated yearly to the critical ICT third-party service provider.

Prior to the adoption of the oversight plan, the Lead Overseer shall communicate the draft oversight plan to the critical ICT third-party service provider.

Upon receipt of the draft oversight plan, the critical ICT third-party service provider may submit a reasoned statement within 15 calendar days evidencing the expected impact on customers which are entities falling outside of the scope of this Regulation and where appropriate, formulating solutions to mitigate risks.

5. Once the annual oversight plans referred to in paragraph 4 have been adopted and notified to the critical ICT third-party service providers, competent authorities may take measures concerning such critical ICT third-party service providers only in agreement with the Lead Overseer.

## Article 34

### Operational coordination between Lead Overseers

1. To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed in accordance with Article 31(1), point (b), shall set up a JON to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third-party service providers, as well as in the course of any action that may be needed pursuant to Article 42.
2. For the purposes of paragraph 1, the Lead Overseers shall draw up a common oversight protocol specifying the detailed procedures to be followed for carrying out the day-to-day coordination and for ensuring swift exchanges and reactions. The protocol shall be periodically revised to reflect operational needs, in particular the evolution of practical oversight arrangements.
3. The Lead Overseers may, on an ad-hoc basis, call on the ECB and ENISA to provide technical advice, share hands-on experience or join specific coordination meetings of the JON.

## Article 35

### Powers of the Lead Overseer

1. For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers in respect of the critical ICT third-party service providers:

- (a) to request all relevant information and documentation in accordance with Article 37;
- (b) to conduct general investigations and inspections in accordance with Articles 38 and 39, respectively;
- (c) to request, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to the recommendations referred to in point (d) of this paragraph;
- (d) to issue recommendations on the areas referred to in Article 33(3), in particular concerning the following:
  - (i) the use of specific ICT security and quality requirements or processes, in particular in relation to the roll-out of patches, updates, encryption and other security measures which the Lead Overseer deems relevant for ensuring the ICT security of services provided to financial entities;
  - (ii) the use of conditions and terms, including their technical implementation, under which the critical ICT third-party service providers provide ICT services to financial entities, which the Lead Overseer deems relevant for preventing the generation of single points of failure, the amplification thereof, or for minimising the possible systemic impact across the Union's financial sector in the event of ICT concentration risk;
  - (iii) any planned subcontracting, where the Lead Overseer deems that further subcontracting, including subcontracting arrangements which the critical ICT third-party service providers plan to enter into with ICT third-party service providers or with ICT subcontractors established in a third country, may trigger risks for the provision of services by the financial entity, or risks to the financial stability, based on the examination of the information gathered in accordance with Articles 37 and 38;
  - (iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:
    - the envisaged subcontractor is an ICT third-party service provider or an ICT subcontractor established in a third country;
    - the subcontracting concerns critical or important functions of the financial entity; and
    - the Lead Overseer deems that the use of such subcontracting poses a clear and serious risk to the financial stability of the Union or to financial entities, including to the ability of financial entities to comply with supervisory requirements.

For the purpose of point (iv) of this point, ICT third-party service providers shall, using the template referred to in Article 41(1), point (b), transmit the information regarding subcontracting to the Lead Overseer.

2. When exercising the powers referred to in this Article, the Lead Overseer shall:

- (a) ensure regular coordination within the JON, and in particular shall seek consistent approaches, as appropriate, with regard to the oversight of critical ICT third-party service providers;



(b) take due account of the framework established by Directive (EU) 2022/2555 and, where necessary, consult the relevant competent authorities designated or established in accordance with that Directive, in order to avoid duplication of technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that Directive;

(c) seek to minimise, to the extent possible, the risk of disruption to services provided by critical ICT third-party service providers to customers that are entities falling outside the scope of this Regulation.

3. The Lead Overseer shall consult the Oversight Forum before exercising the powers referred to in paragraph 1.

Before issuing recommendations in accordance with paragraph 1, point (d), the Lead Overseer shall give the opportunity to the ICT third-party service provider to provide, within 30 calendar days, relevant information evidencing the expected impact on customers that are entities falling outside the scope of this Regulation and, where appropriate, formulating solutions to mitigate risks.

4. The Lead Overseer shall inform the JON of the outcome of the exercise of the powers referred to in paragraph 1, points (a) and (b). The Lead Overseer shall, without undue delay, transmit the reports referred to in paragraph 1, point (c), to the JON and to the competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider.

5. Critical ICT third-party service providers shall cooperate in good faith with the Lead Overseer, and assist it in the fulfilment of its tasks.

6. In the event of whole or partial non-compliance with the measures required to be taken pursuant to the exercise of the powers under paragraph 1, points (a), (b) and (c), and after the expiry of a period of at least 30 calendar days from the date on which the critical ICT third-party service provider received notification of the respective measures, the Lead Overseer shall adopt a decision imposing a periodic penalty payment to compel the critical ICT third-party service provider to comply with those measures.

7. The periodic penalty payment referred to in paragraph 6 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification of the decision to impose a periodic penalty payment to the critical ICT third-party service provider.

8. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be up to 1 % of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year. When determining the amount of the penalty payment, the Lead Overseer shall take into account the following criteria regarding non-compliance with the measures referred to in paragraph 6:

- (a) the gravity and the duration of non-compliance;
- (b) whether non-compliance has been committed intentionally or negligently;
- (c) the level of cooperation of the ICT third-party service provider with the Lead Overseer.

For the purposes of the first subparagraph, in order to ensure a consistent approach, the Lead Overseer shall engage in consultation within the JON.

9. Penalty payments shall be of an administrative nature and shall be enforceable. Enforcement shall be governed by the rules of civil procedure in force in the Member State on the territory of which inspections and access shall be carried out. Courts of the Member State concerned shall have jurisdiction over complaints related to irregular conduct of enforcement. The amounts of the penalty payments shall be allocated to the general budget of the European Union.

10. The Lead Overseer shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

11. Before imposing a periodic penalty payment under paragraph 6, the Lead Overseer shall give the representatives of the critical ICT third-party service provider subject to the proceedings the opportunity to be heard on the findings and shall base its decisions only on findings on which the critical ICT third-party service provider subject to the proceedings has had an opportunity to comment.

The rights of the defence of the persons subject to the proceedings shall be fully respected in the proceedings. The critical ICT third-party service provider subject to the proceedings shall be entitled to have access to the file, subject to the legitimate interest of other persons in the protection of their business secrets. The right of access to the file shall not extend to confidential information or to the Lead Overseer's internal preparatory documents.

## Article 36

### Exercise of the powers of the Lead Overseer outside the Union

1. When oversight objectives cannot be attained by means of interacting with the subsidiary set up for the purpose of Article 31(12), or by exercising oversight activities on premises located in the Union, the Lead Overseer may exercise the powers, referred to in the following provisions, on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third-party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties:

- (a) in Article 35(1), point (a); and
- (b) in Article 35(1), point (b), in accordance with Article 38(2), points (a), (b) and (d), and in Article 39(1) and (2), point (a).

The powers referred to in the first subparagraph may be exercised subject to all of the following conditions:

- (i) the conduct of an inspection in a third-country is deemed necessary by the Lead Overseer to allow it to fully and effectively perform its duties under this Regulation;
- (ii) the inspection in a third-country is directly related to the provision of ICT services to financial entities in the Union;
- (iii) the critical ICT third-party service provider concerned consents to the conduct of an inspection in a third-country; and
- (iv) the relevant authority of the third-country concerned has been officially notified by the Lead Overseer and raised no objection thereto.

2. Without prejudice to the respective competences of the Union institutions and of Member States, for the purposes of paragraph 1, EBA, ESMA or EIOPA shall conclude administrative cooperation arrangements with the relevant authority of the third country in order to enable the smooth conduct of inspections in the third country concerned by the Lead Overseer and its designated team for its mission in that third country. Those cooperation arrangements shall not create legal obligations in respect of the Union and its Member States nor shall they prevent Member States and their competent authorities from concluding bilateral or multilateral arrangements with those third countries and their relevant authorities.

Those cooperation arrangements shall specify at least the following elements:

- (a) the procedures for the coordination of oversight activities carried out under this Regulation and any analogous monitoring of ICT third-party risk in the financial sector exercised by the relevant authority of the third country concerned, including details for transmitting the agreement of the latter to allow the conduct, by the Lead Overseer and its designated team, of general investigations and on-site inspections as referred to in paragraph 1, first subparagraph, on the territory under its jurisdiction;
- (b) the mechanism for the transmission of any relevant information between EBA, ESMA or EIOPA and the relevant authority of the third country concerned, in particular in connection with information that may be requested by the Lead Overseer pursuant to Article 37;
- (c) the mechanisms for the prompt notification by the relevant authority of the third-country concerned to EBA, ESMA or EIOPA of cases where an ICT third-party service provider established in a third country and designated as critical in accordance with Article 31(1), point (a), is deemed to have infringed the requirements

to which it is obliged to adhere pursuant to the applicable law of the third country concerned when providing services to financial institutions in that third country, as well as the remedies and penalties applied;

(d) the regular transmission of updates on regulatory or supervisory developments on the monitoring of ICT third-party risk of financial institutions in the third country concerned;

(e) the details for allowing, if needed, the participation of one representative of the relevant third-country authority in the inspections conducted by the Lead Overseer and the designated team.

3. When the Lead Overseer is not able to conduct oversight activities outside the Union, referred to in paragraphs 1 and 2, the Lead Overseer shall:

(a) exercise its powers under Article 35 on the basis of all facts and documents available to it;

(b) document and explain any consequence of its inability to conduct the envisaged oversight activities as referred to in this Article.

The potential consequences referred to in point (b) of this paragraph shall be taken into consideration in the Lead Overseer's recommendations issued pursuant to Article 35(1), point (d).

## Article 37

### Request for information

1. The Lead Overseer may, by simple request or by decision, require critical ICT third-party service providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.
2. When sending a simple request for information under paragraph 1, the Lead Overseer shall:
  - (a) refer to this Article as the legal basis of the request;
  - (b) state the purpose of the request;
  - (c) specify what information is required;
  - (d) set a time limit within which the information is to be provided;
  - (e) inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but in the event of a voluntary reply to the request the information provided must not be incorrect or misleading.
3. When requiring by decision to supply information under paragraph 1, the Lead Overseer shall:
  - (a) refer to this Article as the legal basis of the request;
  - (b) state the purpose of the request;
  - (c) specify what information is required;
  - (d) set a time limit within which the information is to be provided;
  - (e) indicate the periodic penalty payments provided for in Article 35(6) where the production of the required information is incomplete or when such information is not provided within the time limit referred to in point (d) of this paragraph;
  - (f) indicate the right to appeal the decision to ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union (Court of Justice) in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.
4. The representatives of the critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.
5. The Lead Overseer shall, without delay, transmit a copy of the decision to supply information to the competent authorities of the financial entities using the services of the relevant critical ICT third-party service providers and to the JON.

## Article 38

### General investigations

1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the joint examination team referred to in Article 40(1), may, where necessary, conduct investigations of critical ICT third-party service providers.
2. The Lead Overseer shall have the power to:
  - (a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;
  - (b) take or obtain certified copies of, or extracts from, such records, data, documented procedures and any other material;
  - (c) summon representatives of the critical ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;
  - (d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;
  - (e) request records of telephone and data traffic.
3. The officials and other persons authorised by the Lead Overseer for the purposes of the investigation referred to in paragraph 1 shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the investigation.

That authorisation shall also indicate the periodic penalty payments provided for in Article 35(6) where the production of the required records, data, documented procedures or any other material, or the answers to questions asked to representatives of the ICT third-party service provider are not provided or are incomplete.

4. The representatives of the critical ICT third-party service providers are required to submit to the investigations on the basis of a decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the investigation, the periodic penalty payments provided for in Article 35(6), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, and the right to have the decision reviewed by the Court of Justice.
5. In good time before the start of the investigation, the Lead Overseer shall inform competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider of the envisaged investigation and of the identity of the authorised persons.

The Lead Overseer shall communicate to the JON all information transmitted pursuant to the first subparagraph.

---

## Article 39

### Inspections

1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the joint examination teams referred to in Article 40(1), may enter in, and conduct all necessary onsite inspections on, any business premises, land or property of the ICT third-party service providers, such as head offices, operation centres, secondary premises, as well as to conduct off-site inspections.

For the purposes of exercising the powers referred to in the first subparagraph, the Lead Overseer shall consult the JON.

2. The officials and other persons authorised by the Lead Overseer to conduct an on-site inspection shall have the power to:

(a) enter any such business premises, land or property; and

(b) seal any such business premises, books or records, for the period of, and to the extent necessary for, the inspection.

The officials and other persons authorised by the Lead Overseer shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection, and the periodic penalty payments provided for in Article 35(6) where the representatives of the critical ICT third-party service providers concerned do not submit to the inspection.

3. In good time before the start of the inspection, the Lead Overseer shall inform the competent authorities of the financial entities using that ICT third-party service provider.

4. Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of ICT services to financial entities.

5. Before any planned on-site inspection, the Lead Overseer shall give reasonable notice to the critical ICT third-party service providers, unless such notice is not possible due to an emergency or crisis situation, or if it would lead to a situation where the inspection or audit would no longer be effective.

6. The critical ICT third-party service provider shall submit to on-site inspections ordered by decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the inspection, fix the date on which the inspection shall begin and shall indicate the periodic penalty payments provided for in Article 35(6), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, as well as the right to have the decision reviewed by the Court of Justice.

7. Where the officials and other persons authorised by the Lead Overseer find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the Lead Overseer shall inform the critical ICT third-party service provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to require financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

## Article 40

### Ongoing oversight

1. When conducting oversight activities, in particular general investigations or inspections, the Lead Overseer shall be assisted by a joint examination team established for each critical ICT third-party service provider.
2. The joint examination team referred to in paragraph 1 shall be composed of staff members from:
  - (a) the ESAs;
  - (b) the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides ICT services;
  - (c) the national competent authority referred to in Article 32(4), point (e), on a voluntary basis;
  - (d) one national competent authority from the Member State where the critical ICT third-party service provider is established, on a voluntary basis.

Members of the joint examination team shall have expertise in ICT matters and in operational risk. The joint examination team shall work under the coordination of a designated Lead Overseer staff member (the 'Lead Overseer coordinator').

3. Within 3 months of the completion of an investigation or inspection, the Lead Overseer, after consulting the Oversight Forum, shall adopt recommendations to be addressed to the critical ICT third-party service provider pursuant to the powers referred to in Article 35.
4. The recommendations referred to in paragraph 3 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides ICT services.

For the purposes of fulfilling the oversight activities, the Lead Overseer may take into consideration any relevant third-party certifications and ICT third-party internal or external audit reports made available by the critical ICT third-party service provider.



## Article 41

### Harmonisation of conditions enabling the conduct of the oversight activities

1. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify:

▪ *Appendix IX*

(a) the information to be provided by an ICT third-party service provider in the application for a voluntary request to be designated as critical under Article 31(11);

(b) the content, structure and format of the information to be submitted, disclosed or reported by the ICT third-party service providers pursuant to Article 35(1), including the template for providing information on subcontracting arrangements;

(c) the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements.

(d) the details of the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer pursuant to Article 42(3).

2. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 1 in accordance with the procedure laid down in Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

## Article 42

### Follow-up by competent authorities

1. Within 60 calendar days of the receipt of the recommendations issued by the Lead Overseer pursuant to Article 35(1), point (d), critical ICT third-party service providers shall either notify the Lead Overseer of their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations. The Lead Overseer shall immediately transmit this information to the competent authorities of the financial entities concerned.

2. The Lead Overseer shall publicly disclose where a critical ICT third-party service provider fails to notify the Lead Overseer in accordance with paragraph 1 or where the explanation provided by the critical ICT third-party service provider is not deemed sufficient. The information published shall disclose the identity of the critical ICT third-party service provider as well as information on the type and nature of the non-compliance. Such information shall be limited to what is relevant and proportionate for the purpose of ensuring public awareness, unless such publication would cause disproportionate damage to the parties involved or could seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system of the Union.

The Lead Overseer shall notify the ICT third-party service provider of that public disclosure.

3. Competent authorities shall inform the relevant financial entities of the risks identified in the recommendations addressed to critical ICT third-party service providers in accordance with Article 35(1), point (d).

When managing ICT third-party risk, financial entities shall take into account the risks referred to in the first subparagraph.

4. Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations, it shall notify the financial entity of the possibility of a decision being taken, within 60 calendar days of the receipt of such notification, pursuant to paragraph 6, in the absence of appropriate contractual arrangements aiming to address such risks.

5. Upon receiving the reports referred to in Article 35(1), point (c), and prior to taking a decision as referred to in paragraph 6 of this Article, competent authorities may, on a voluntary basis, consult the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider.

6. Competent authorities may, as a measure of last resort, following the notification and, if appropriate, the consultation as set out in paragraph 4 and 5 of this Article, in accordance with Article 50, take a decision requiring financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party service provider until the risks identified in the recommendations addressed to critical ICT third-party service providers have been addressed. Where necessary, they may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.

7. Where a critical ICT third-party service provider refuses to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer, and such a divergent approach may adversely impact a large number of financial entities, or a significant part of the financial sector, and individual warnings issued by competent authorities have not resulted in consistent approaches mitigating the potential risk to financial stability, the Lead Overseer may, after consulting the Oversight Forum, issue non-binding and non-public opinions to competent authorities, in order to promote consistent and convergent supervisory follow-up measures, as appropriate.

8. Upon receiving the reports referred to in Article 35(1), point (c), competent authorities, when taking a decision as referred to in paragraph 6 of this Article, shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

- (a) the gravity and the duration of the non-compliance;
- (b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;
- (c) whether a financial crime was facilitated, occasioned or is otherwise attributable to the non-compliance;
- (d) whether the non-compliance has been intentional or negligent;
- (e) whether the suspension or termination of the contractual arrangements introduces a risk for continuity of the financial entity's business operations notwithstanding the financial entity's efforts to avoid disruption in the provision of its services;
- (f) where applicable, the opinion of the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider, requested on a voluntary basis in accordance with paragraph 5 of this Article.

Competent authorities shall grant financial entities the necessary period of time to enable them to adjust the contractual arrangements with critical ICT third-party service providers in order to avoid detrimental effects on their digital operational resilience and to allow them to deploy exit strategies and transition plans as referred to in Article 28.

9. The decision referred to in paragraph 6 of this Article shall be notified to the members of the Oversight Forum referred to in Article 32(4), points (a), (b) and (c), and to the JON.

The critical ICT third-party service providers affected by the decisions provided for in paragraph 6 shall fully cooperate with the financial entities impacted, in particular in the context of the process of suspension or termination of their contractual arrangements.

10. Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third-party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.

11. The Lead Overseer may, upon request, provide further clarifications on the recommendations issued to guide the competent authorities on the follow-up measures.

## Article 43

### Oversight fees

1. The Lead Overseer shall, in accordance with the delegated act referred to in paragraph 2 of this Article, charge critical ICT third-party service providers fees that fully cover the Lead Overseer's necessary expenditure in relation to the conduct of oversight tasks pursuant to this Regulation, including the reimbursement of any costs which may be incurred as a result of work carried out by the joint examination team referred to in Article 40, as well as the costs of advice provided by the independent experts as referred to in Article 32(4), second subparagraph, in relation to matters falling under the remit of direct oversight activities.

The amount of a fee charged to a critical ICT third-party service provider shall cover all costs derived from the execution of the duties set out in this Section and shall be proportionate to its turnover.

2. The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid by 17 July 2024.

## Article 44

### International cooperation

1. Without prejudice to Article 36, EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, in particular by developing best practices for the review of ICT risk management practices and controls, mitigation measures and incident responses.
2. The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission, summarising the findings of relevant discussions held with the third countries' authorities referred to in paragraph 1, focusing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection and the functioning of the internal market.

## CHAPTER VI

### Information-sharing arrangements

#### Article 45

##### Information-sharing arrangements on cyber threat information and intelligence

1. Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:

(a) aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;

(b) takes place within trusted communities of financial entities;

(c) is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy.

2. For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which they may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.

3. Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once it takes effect.

---

## CHAPTER VII

### Competent authorities

#### Article 46

#### Competent authorities

Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Chapter V, Section II, of this Regulation, compliance with this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:

- (a) for credit institutions and for institutions exempted pursuant to Directive 2013/36/EU, the competent authority designated in accordance with Article 4 of that Directive, and for credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, the ECB in accordance with the powers and tasks conferred by that Regulation;
- (b) for payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366, electronic money institutions, including those exempted pursuant to Directive 2009/110/EC, and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366;
- (c) for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034 of the European Parliament and of the Council<sup>38</sup>;
- (d) for crypto-asset service providers as authorised under the Regulation on markets in crypto-assets and issuers of asset-referenced tokens, the competent authority designated in accordance with the relevant provision of that Regulation;
- (e) for central securities depositories, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;
- (f) for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;
- (g) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU, and the competent authority as defined in Article 2(1), point (18), of Regulation (EU) No 600/2014;
- (h) for trade repositories, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;
- (i) for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;

---

<sup>38</sup> Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU (OJ L 314, 5.12.2019, p. 64).

- (j) for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;
- (k) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;
- (l) for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;
- (m) for institutions for occupational retirement provision, the competent authority designated in accordance with Article 47 of Directive (EU) 2016/2341;
- (n) for credit rating agencies, the competent authority designated in accordance with Article 21 of Regulation (EC) No 1060/2009;
- (o) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of Regulation (EU) 2016/1011;
- (p) for crowdfunding service providers, the competent authority designated in accordance with Article 29 of Regulation (EU) 2020/1503;
- (q) for securitisation repositories, the competent authority designated in accordance with Articles 10 and 14(1) of Regulation (EU) 2017/2402.



## Article 47

### Cooperation with structures and authorities established by Directive (EU)

#### 2022/2555

1. To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 14 of Directive (EU) 2022/2555, the ESAs and the competent authorities may participate in the activities of the Cooperation Group for matters that concern their supervisory activities in relation to financial entities. The ESAs and the competent authorities may request to be invited to participate in the activities of the Cooperation Group for matters in relation to essential or important entities subject to Directive (EU) 2022/2555 that have also been designated as critical ICT third-party service providers pursuant to Article 31 of this Regulation.

2. Where appropriate, competent authorities may consult and share information with the single points of contact and the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.

3. Where appropriate, competent authorities may request any relevant technical advice and assistance from the competent authorities designated or established in accordance with Directive (EU) 2022/2555 and establish cooperation arrangements to allow effective and fast-response coordination mechanisms to be set up.

4. The arrangements referred to in paragraph 3 of this Article may, inter alia, specify the procedures for the coordination of supervisory and oversight activities in relation to essential or important entities subject to Directive (EU) 2022/2555 that have been designated as critical ICT third-party service providers pursuant to Article 31 of this Regulation, including for the conduct, in accordance with national law, of investigations and on-site inspections, as well as for mechanisms for the exchange of information between the competent authorities under this Regulation and the competent authorities designated or established in accordance with that Directive which includes access to information requested by the latter authorities.

## Article 48

### Cooperation between authorities

1. Competent authorities shall cooperate closely among themselves and, where applicable, with the Lead Overseer.
2. Competent authorities and the Lead Overseer shall, in a timely manner, mutually exchange all relevant information concerning critical ICT third-party service providers which is necessary for them to carry out their respective duties under this Regulation, in particular in relation to identified risks, approaches and measures taken as part of the Lead Overseer's oversight tasks.

## Article 49

### Financial cross-sector exercises, communication and cooperation

1. The ESAs, through the Joint Committee and in collaboration with competent authorities, resolution authorities as referred to in Article 3 of Directive 2014/59/EU, the ECB, the Single Resolution Board as regards information relating to entities falling under the scope of Regulation (EU) No 806/2014, the ESRB and ENISA, as appropriate, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors.

They may develop crisis management and contingency exercises involving cyber-attack scenarios with a view to developing communication channels and gradually enabling an effective coordinated response at Union level in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the Union's financial sector as a whole.

Those exercises may, as appropriate, also test the financial sector's dependencies on other economic sectors.

2. Competent authorities, ESAs and the ECB shall cooperate closely with each other and exchange information to carry out their duties pursuant to Articles 47 to 54. They shall closely coordinate their supervision in order to identify and remedy breaches of this Regulation, develop and promote best practices, facilitate collaboration, foster consistency of interpretation and provide cross-jurisdictional assessments in the event of any disagreements.

## Article 50

### Administrative penalties and remedial measures

1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.
2. The powers referred to in paragraph 1 shall include at least the following powers to:
  - (a) have access to any document or data held in any form that the competent authority considers relevant for the performance of its duties and receive or take a copy of it;
  - (b) carry out on-site inspections or investigations, which shall include but shall not be limited to;
    - (i) summoning representatives of the financial entities for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;
    - (ii) interviewing any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;
  - (c) require corrective and remedial measures for breaches of the requirements of this Regulation.
3. Without prejudice to the right of Member States to impose criminal penalties in accordance with Article 52, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.

Those penalties and measures shall be effective, proportionate and dissuasive.
4. Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation:
  - (a) issue an order requiring the natural or legal person to cease conduct that is in breach of this Regulation and to desist from a repetition of that conduct;
  - (b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;
  - (c) adopt any type of measure, including of pecuniary nature, to ensure that financial entities continue to comply with legal requirements;
  - (d) require, insofar as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and
  - (e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.
5. Where paragraph 2, point (c), and paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.
6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in paragraph 2, point (c), is properly reasoned and is subject to a right of appeal.

## Article 51

### Exercise of the power to impose administrative penalties and remedial measures

1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 50 in accordance with their national legal frameworks, where appropriate, as follows:

- (a) directly;
- (b) in collaboration with other authorities;
- (c) under their responsibility by delegation to other authorities; or
- (d) by application to the competent judicial authorities.

2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 50, shall take into account the extent to which the breach is intentional or results from negligence, and all other relevant circumstances, including the following, where appropriate:

- (a) the materiality, gravity and the duration of the breach;
- (b) the degree of responsibility of the natural or legal person responsible for the breach;
- (c) the financial strength of the responsible natural or legal person;
- (d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;
- (e) the losses for third parties caused by the breach, insofar as they can be determined;
- (f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses avoided by that natural or legal person;
- (g) previous breaches by the responsible natural or legal person.

## Article 52

### Criminal penalties

1. Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches that are subject to criminal penalties under their national law.
2. Where Member States have chosen to lay down criminal penalties for breaches of this Regulation, they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other competent authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.

## Article 53

### Notification duties

Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by 17 January 2025. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.

## Article 54

### Publication of administrative penalties

1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the addressee of the penalty has been notified of that decision.
2. The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the identity of the persons responsible and the penalties imposed.
3. Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, including risks in relation to the protection of personal data, jeopardise the stability of financial markets or the pursuit of an ongoing criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt one of the following solutions in respect of the decision imposing an administrative penalty:
  - (a) defer its publication until all reasons for non-publication cease to exist;
  - (b) publish it on an anonymous basis, in accordance with national law; or
  - (c) refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportionate to the leniency of the imposed penalty.
4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with paragraph 3, point (b), the publication of the relevant data may be postponed.
5. Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and, at later stages, any subsequent related information on the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.
6. Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website only for the period which is necessary to bring forth this Article. This period shall not exceed five years after its publication.



## Article 55

### Professional secrecy

1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.
2. The obligation of professional secrecy applies to all persons who work, or who have worked, for the competent authorities pursuant to this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.
3. Information covered by professional secrecy, including the exchange of information among competent authorities under this Regulation and competent authorities designated or established in accordance with Directive (EU) 2022/2555, shall not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law;
4. All information exchanged between the competent authorities pursuant to this Regulation that concerns business or operational conditions and other economic or personal affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states, at the time of communication, that such information may be disclosed or where such disclosure is necessary for legal proceedings.

## Article 56

### Data Protection

1. The ESAs and the competent authorities shall be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations and duties pursuant to this Regulation, in particular for investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight plans. The personal data shall be processed in accordance with Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, whichever is applicable.
2. Except where otherwise provided in other sectoral acts, the personal data referred to in paragraph 1 shall be retained until the discharge of the applicable supervisory duties and in any case for a maximum period of 15 years, except in the event of pending court proceedings requiring further retention of such data.

## CHAPTER VIII

### Delegated acts

#### Article 57

##### Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Articles 31(6) and 43(2) shall be conferred on the Commission for a period of five years from 17 January 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
3. The delegation of power referred to in Articles 31(6) and 43(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Articles 31(6) and 43(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

## CHAPTER IX

### Transitional and final provisions

#### Section I

#### Article 58

##### Review clause

1. By 17 January 2028, the Commission shall, after consulting the ESAs and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal. The review shall include at least the following:

- (a) the criteria for the designation of critical ICT third-party service providers in accordance with Article 31(2);
- (b) the voluntary nature of the notification of significant cyber threats referred to in Article 19;
- (c) the regime referred to in Article 31(12) and the powers of the Lead Overseer provided for in Article 35(1), point (d), point (iv), first indent, with a view to evaluating the effectiveness of those provisions with regard to ensuring effective oversight of critical ICT third-party service providers established in a third country, and the necessity to establish a subsidiary in the Union.

For the purposes of the first subparagraph of this point, the review shall include an analysis of the regime referred to in Article 31(12), including in terms of access for Union financial entities to services from third countries and availability of such services on the Union market and it shall take into account further developments in the markets for the services covered by this Regulation, the practical experience of financial entities and financial supervisors with regard to the application and, respectively, supervision of that regime, and any relevant regulatory and supervisory developments taking place at international level.

- (d) the appropriateness of including in the scope of this Regulation financial entities referred to in Article 2(3), point (e), making use of automated sales systems, in light of future market developments on the use of such systems;
- (e) the functioning and effectiveness of the JON in supporting the consistency of the oversight and the efficiency of the exchange of information within the Oversight Framework.

2. In the context of the review of Directive (EU) 2015/2366, the Commission shall assess the need for increased cyber resilience of payment systems and payment-processing activities and the appropriateness of extending the scope of this Regulation to operators of payment systems and entities involved in payment-processing activities. In light of this assessment, the Commission shall submit, as part of the review of Directive (EU) 2015/2366, a report to the European Parliament and the Council no later than 17 July 2023.

Based on that review report, and after consulting ESAs, ECB and the ESRB, the Commission may submit, where appropriate and as part of the legislative proposal that it may adopt pursuant to Article 108, second paragraph, of Directive (EU) 2015/2366, a proposal to ensure that all operators of payment systems and entities involved in payment-processing activities are subject to an appropriate oversight, while taking into account existing oversight by the central bank.

3. By 17 January 2026, the Commission shall, after consulting the ESAs and the Committee of European Auditing Oversight Bodies, carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal, on the appropriateness of strengthened requirements for statutory auditors and audit firms as regards digital operational resilience, by means of the inclusion of statutory auditors and audit firms into the scope of this Regulation or by means of amendments to Directive 2006/43/EC of the European Parliament and of the Council<sup>39</sup>.

---

<sup>39</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).

## Section II

### Amendments

#### Article 59

#### Amendments to Regulation (EC) No 1060/2009

Regulation (EC) No 1060/2009 is amended as follows:

(1) in Annex I, Section A, point 4, the first subparagraph is replaced by the following:

'A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (\*1).

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

(2) in Annex III, point 12 is replaced by the following:

'12. The credit rating agency infringes Article 6(2), in conjunction with point 4 of Section A of Annex I, by not having sound administrative or accounting procedures, internal control mechanisms, effective procedures for risk assessment, or effective control or safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554; or by not implementing or maintaining decision-making procedures or organisational structures as required by that point.'

## Article 60

### Amendments to Regulation (EU) No 648/2012

Regulation (EU) No 648/2012 is amended as follows:

(1) Article 26 is amended as follows:

(a) paragraph 3 is replaced by the following:

'3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (\*2).

(\*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).';"

(b) paragraph 6 is deleted;

(2) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity policy and ICT response and recovery plans put in place and implemented in accordance with Regulation (EU) 2022/2554, aiming to ensure the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.';

(b) in paragraph 3, the first subparagraph is replaced by the following:

'3. In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity policy and disaster recovery plans.';

(3) in Article 56(3), the first subparagraph is replaced by the following:

'3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for registration referred to in paragraph 1.';

(4) in Article 79, paragraphs 1 and 2 are replaced by the following:

'1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU) 2022/2554.

2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity policy and ICT response and recovery plans established in accordance with Regulation (EU) 2022/2554, aiming to ensure the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations.';

(5) in Article 80, paragraph 1 is deleted.

(6) in Annex I, Section II is amended as follows:

(a) points (a) and (b) are replaced by the following:

'(a) a trade repository infringes Article 79(1) by not identifying sources of operational risk or by not minimising those risks through the development of appropriate systems, controls and procedures including ICT systems managed in accordance with Regulation (EU) 2022/2554;

(b) a trade repository infringes Article 79(2) by not establishing, implementing or maintaining an adequate business continuity policy and disaster recovery plan established in accordance with Regulation (EU) 2022/2554, aiming to ensure the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations;';

(b) point (c) is deleted.

(7) Annex III is amended as follows:

(a) Section II is amended as follows:

(i) point (c) is replaced by the following:

'(c) a Tier 2 CCP infringes Article 26(3) by not maintaining or operating an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities or by not employing appropriate and proportionate systems, resources or procedures including ICT systems managed in accordance with Regulation (EU) 2022/2554;';

(ii) point (f) is deleted.

(b) in Section III, point (a) is replaced by the following:

'(a) a Tier 2 CCP infringes Article 34(1) by not establishing, implementing or maintaining an adequate business continuity policy and response and recovery plan set up in accordance with Regulation (EU) 2022/2554, aiming to ensure the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations, which at least allows for the recovery of all transactions at the time of disruption to allow the CCP to continue to operate with certainty and to complete settlement on the scheduled date;';



## Article 61

### Amendments to Regulation (EU) No 909/2014

Article 45 of Regulation (EU) No 909/2014 is amended as follows:

(1) paragraph 1 is replaced by the following:

'1. A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (\*3), as well as through any other relevant appropriate tools, controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.

(\*3) 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).';"

(2) paragraph 2 is deleted;

(3) paragraphs 3 and 4 are replaced by the following:

'3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, including ICT business continuity policy and ICT response and recovery plans established in accordance with Regulation (EU) 2022/2554, to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk to disrupting operations.

4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in Article 12(5) and (7) of Regulation (EU) 2022/2554.';

(4) paragraph 6 is replaced by the following:

'6. A CSD shall identify, monitor and manage the risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of any operational incidents, other than in relation to ICT risk, resulting from such risks.';

(5) in paragraph 7, the first subparagraph is replaced by the following:

'7. ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risk, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.'.

## Article 62

### Amendments to Regulation (EU) No 600/2014

Regulation (EU) No 600/2014 is amended as follows:

(1) Article 27g is amended as follows:

(a) paragraph 4 is replaced by the following:

'4. An APA shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554 of the European Parliament and of the Council (\*4).

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

(b) in paragraph 8, point (c) is replaced by the following:

'(c) the concrete organisational requirements laid down in paragraphs 3 and 5.';

(2) Article 27h is amended as follows:

(a) paragraph 5 is replaced by the following:

'5. A CTP shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554.'

(b) in paragraph 8, point (e) is replaced by the following:

'(e) the concrete organisational requirements laid down in paragraph 4.';

(3) Article 27i is amended as follows:

(a) paragraph 3 is replaced by the following:

'3. An ARM shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2022/2554.';

(b) in paragraph 5, point (b) is replaced by the following:

'(b) the concrete organisational requirements laid down in paragraphs 2 and 4.'

## Article 63

### Amendment to Regulation (EU) 2016/1011

In Article 6 of Regulation (EU) 2016/1011, the following paragraph is added:

'6. For critical benchmarks, an administrator shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (\*5).

## Article 64

### Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 17 January 2025.

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

Done at Strasbourg, 14 December 2022.

## **APPENDIX I: Commission Delegated Regulation (EU) 2024/1502**

**of 22 February 2024**

### **supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities**

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 (1), and in particular Article 31(6) thereof,

Whereas:

- (1) To assess whether an ICT third-party service provider is critical for financial entities, and taking into account the criteria set out in Article 31(2) of Regulation (EU) 2022/2554, the European Supervisory Authorities (ESAs) should use sub-criteria in a two-step approach assessment. Considering the important number of ICT services and the diversity and number of financial institutions using those services, such a two-step approach should be undertaken to filter the population of ICT third-party service providers and identify the most critical ICT third-party service providers. The quantitative sub-criteria that are to be considered as part of the first step of the assessment are necessary to carry out a first selection of the population of ICT third-party service providers for which it is relevant to carry out a further in-depth analysis in light of the qualitative sub-criteria that are to be considered as part of the second step of the assessment.
- (2) The extent to which an ICT service provided by an ICT third-party service provider supports critical or important functions of the financial entity is considered a crucial element of the criticality assessment in general. Therefore, the importance of the activities of the financial entities that are supported by ICT services should be integrated in all sub-criteria considered as part of the first step. Consequently, there should not be a distinct quantitative assessment related to the criticality of the functions of the financial entities as part of the first step of the assessment. Instead, it is appropriate that the ESAs consider the criticality and importance of the functions of the financial entities supported by ICT services as part of the qualitative second step of the assessment.
- (3) The assessment should be carried out per individual ICT third-party service provider or, where applicable, per group of ICT third-party services providers in case the ICT third-party service provider belongs to a group as per Article 31(3) of Regulation (EU) 2022/2554. In order to enable a comprehensive assessment of the potential systemic impact on the Union financial sector, ICT subcontractors of ICT third-party service providers should also be subject to the assessment by the ESAs, and where applicable, designated as critical ICT third-party service providers.
- (4) To determine the systemic impact of the ICT third-party service provider on the stability, continuity or quality of the provision of financial services it is of paramount importance to develop a clear view on the extent and nature of systemic impact which a large-scale operational failure of an ICT third-party service provider would have on financial entities, which rely on services provided by an ICT third-party service provider, and on the financial system. Therefore, it is appropriate to consider the number of financial entities of a specific category of financial entities using the same ICT services, as well as the value of their assets to assess whether it is relevant to consider the ICT third-party service provider offering those ICT

services as critical. Furthermore, a qualitative assessment of the systemic importance and interconnectedness of ICT third-party service providers, as well as the importance of the services provided by an ICT third-party provider on financial entities' provision of financial services taking into account the stability and the continuity of the services should be carried out to determine the systemic impact of the ICT third-party service provider on the activities of financial entities.

- (5) To determine the systemic character and importance of the financial entities relying on the ICT services, it is necessary to take into account the nature of those financial entities. Where financial entities that are classified as G-SIIs and O-SIIs or that are identified as 'systemic' rely on the same ICT services to support their critical or important functions, it is appropriate to assess whether the ICT third-party service provider providing those services should be considered as critical for the Union financial sector. The interconnectedness between financial entities within the Union financial sector that rely on ICT services provided by the same ICT third-party service provider should also be assessed to determine the reliance of financial entities on that ICT third-party service provider.
- (6) The ICT services supporting critical or important functions of the financial entities should be assessed in respect of their type and critical nature that are necessary for the financial entities to run their activities without any disruptions.
- (7) To determine the degree of substitutability of the ICT third party service provider, it is necessary to take into account the number of ICT third-party service providers active on a given market, the existence of alternative solutions for the same ICT service, as well as at the costs of migrating data and ICT workloads to other ICT third-party service providers as part of the assessment to be carried out by the ESAs.
- (8) In order to ensure the soundness of the assessment process, it is important that the ESAs rely on the data from the registers of information referred to in Article 28(3) of Regulation (EU) 2022/2554, and any other readily available information, when assessing whether the ICT third-party service providers should be designated as critical,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

#### **Assessment approach**

1. When considering the criteria set out in Article 31(2) of Regulation (EU) 2022/2554 to designate an ICT third-party service provider that is critical for financial entities, the ESAs shall apply the following approach:

- (a) as a first step, the ESAs shall assess whether the ICT third-party service provider fulfils all of the 'step 1' sub-criteria set out in Articles 2(1), 3(1), and 5(1);
- (b) as a second step, for those ICT third-party service providers that fulfil all of the 'step 1' sub-criteria referred to in point (a), the ESAs shall carry out their assessment in the light of the 'step 2' sub-criteria referred to in Articles 2(5), 3(4), 4(1), and 5(5).

By way of derogation from the first sub paragraph, for the assessment of the criterion (c) of Article 31(2) of Regulation (EU) 2022/2554, the first step shall be covered by the assessment to be carried out for the criteria (a), (b) and (d) of Article 31(2) of Regulation (EU) 2022/2554.

2. After the end of the time period for the submission of a reasoned statement referred to in Article 31(5), first subparagraph, of Regulation (EU) 2022/2554, the ESAs, through the Joint Committee and upon recommendation from the Oversight Forum, shall designate an ICT third-party service provider as critical for financial entities if it fulfils all the 'step 1' sub-criteria referred to in paragraph 1, point (a), and following a positive outcome of the assessment carried out in relation to the 'step 2' sub-criteria referred to in paragraph 1, point (b).

## Article 2

**Systemic impact of ICT third-party service providers on the stability, continuity or quality of the provision of financial services**

1. When considering the criterion set out in Article 31(2), point (a), of Regulation (EU) 2022/2554, the ESAs shall assess whether the ICT third-party service provider fulfils the following 'step 1' sub-criteria:

(a) sub-criterion 1.1: share of the number of financial entities, broken down by categories of financial entities as listed in Article 2(1) of Regulation (EU) 2022/2554, to which ICT services are provided by the same ICT third-party service provider where the ICT services support critical or important functions;

(b) sub-criterion 1.2: share of the total value of assets of financial entities, broken down by categories of financial entities as listed in Article 2(1) of Regulation (EU) 2022/2554, to which ICT services are provided by the same ICT third-party provider where the ICT services support critical or important functions of financial entities.

2. The sub-criterion 1.1 set out in paragraph 1, point (a), shall be calculated as follows:

<p>number of financial entities of a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554, to which ICT services are provided by the same ICT third party services provider where the ICT services support critical or important functions of financial entities</p>
--

<p>total number of financial entities of a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554</p>
---

3. The sub-criterion 1.2 set out in paragraph 1, point (b), shall be calculated as follows:

<p>total value of assets of financial entities of a category of financial entities as listed in Article 2(1) of Regulation (EU) 2022/2554, to which ICT services are provided by the same ICT third party provider where the ICT services support critical or important functions of financial entities</p>
---

<p>total value of assets of all EU financial entities of the same category as set out in Article 2(1) of Regulation (EU) 2022/2554</p>
--

4. An ICT third-party service provider shall be considered as having fulfilled the 'step 1' sub-criteria referred to in paragraph 1 where both of the shares as calculated in accordance with paragraphs 2 and 3 are of at least 10 % of the total number for at least one category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554.

5. When considering the criterion set out in Article 31(2), point (a), of Regulation (EU) 2022/2554 and where the ICT third-party service provider fulfils the 'step 1' sub-criteria referred to in paragraph 1 of this Article, the ESAs shall carry out their assessment in the light of the following 'step 2' sub-criteria:

(a) sub-criterion 1.3: the intensity of the impact of discontinuing the ICT services provided by the ICT third-party service provider on the activities and operations of financial entities identified in the 'step 1' sub-criteria referred to in paragraph 1 of this Article and the number of those financial entities affected;

(b) sub-criterion 1.4: the dependence of the critical ICT third-party service provider on the same subcontractors providing ICT services supporting critical or important functions of financial entities.

### *Article 3*

#### **Systemic character and importance of the ICT services provided to financial entities**

1. When considering the criterion set out in Article 31(2), point (b), of Regulation (EU) 2022/2554, the ESAs shall assess whether the ICT third-party service provider fulfils the following 'step 1' sub-criteria:

(a) sub-criterion 2.1: number of global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs) that are credit institutions to which ICT services are provided by the same ICT third-party service provider where the ICT services support critical or important functions;

(b) sub-criterion 2.2: number of financial entities, other than credit institutions and G-SIIs and O-SIIs referred to in point (a) above, identified as systemic by competent authorities referred to under Article 46 of Regulation (EU) 2022/2554 to which ICT services are provided by the same ICT third-party service provider where the ICT services support critical or important functions.

2. An ICT third-party service provider shall be considered as having fulfilled the sub-criterion set out in paragraph 1, point (a), if the ICT services it provides are used at least by either of the following:

(a) one G-SII;

(b) at least three O-SIIs;

(c) at least one O-SII with an O-SII score above 3 000 calculated in accordance with Article 131(3) of Directive 2013/36/EU of the European Parliament and of the Council (2).

3. An ICT third-party service provider shall be considered as having fulfilled the sub-criterion set out in paragraph 1, point (b), if the ICT services that it provides are used at least by either of the following:

(a) one financial entity that is a financial entity as referred to in Article 2(1), points (g), (h), (i) or (j) of Regulation (EU) 2022/2554 and which is identified as 'systemic' by competent authorities;

(b) at least three financial entities, other than credit institutions and than financial entities referred to in Article 2(1), points (g), (h), (i) or (j) of Regulation (EU) 2022/2554 and which are identified as 'systemic' by competent authorities.

4. When considering the criterion set out in Article 31(2), point (b), of Regulation (EU) 2022/2554 and where the ICT third-party service provider fulfils the 'step 1' sub-criteria referred to in paragraph 1 of this Article, the ESAs shall carry out their assessment in the light of the following 'step 2' sub-criterion:

- sub-criterion 2.3: G-SIIs or O-SIIs and other financial entities included in the assessment in the 'step 1' sub criteria referred to in paragraph 1 of this Article, including where those G-SIIs or O-SIIs provide financial infrastructure services to other financial entities, relying on an ICT service provided by the same ICT third-party service provider, are interdependent.



Article 4

**Criticality or importance of the functions**

When considering the criterion set out in Article 31(2), point (c), of Regulation (EU) 2022/2554, the ESAs shall carry out their assessment in the light of the following 'step 2' sub-criterion:

- sub-criterion 3.1: the ICT service provided ultimately by the same ICT third-party service provider supporting critical or important functions of financial entities is of a critical nature for the activities of the financial entities.

Article 5

**Degree of substitutability**

1. When considering the criterion set out in Article 31(2), point (d), of Regulation (EU) 2022/2554, the ESAs shall assess whether the ICT third-party service provider fulfils the following 'step 1' sub-criteria:

(a) sub-criterion 4.1: the share of the total number of financial entities, broken down by categories of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554, for which no alternative ICT third-party service provider is available which has the required capacity to provide the same ICT services that support critical or important functions of financial entities as the one provided by the relevant ICT third-party service provider;

(b) sub-criterion 4.2: the share of the total number of financial entities, broken down by categories of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554, for which it is highly difficult to migrate an ICT service provided by the relevant ICT third-party service provider that supports critical or important functions of financial entities to another ICT third-party service provider.

2. The sub-criterion 4.1 set out in paragraph 1, point (a), shall be calculated as follows:

number of financial entities of a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554, for which no alternative ICT third party service provider is available which has the required capacity to provide the same ICT services that support critical or important functions of financial entities as the one provided by the relevant ICT third party service provider
total number of financial entities of that category of financial entities as set out in Article 2(1)of Regulation 2022/2554

3. The sub-criterion set out in paragraph 1, point (b), shall be calculated as follows:

number of financial entities of a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554, for which it is highly difficult to migrate or reintegrate an ICT service provided
---

<p>by the ICT third party provider that support critical or important functions to another ICT third party provider</p>
<p>total number of EU financial entities of that category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554</p>

4. An ICT third-party service provider shall be considered as having fulfilled both sub-criteria 4.1 and 4.2 where either of the following is met:

(a) the share of the total number of financial entities referred to in paragraph 1, point (a), is of at least 10 % of the total number of financial entities for a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554;

(b) the share of the total number of financial entities referred to in paragraph 1, point (b), is of at least 10 % of the total number of financial entities or a category of financial entities as set out in Article 2(1) of Regulation (EU) 2022/2554.

5. When considering the criterion set out in Article 31(2), point (d), of Regulation (EU) 2022/2554 and where the ICT third-party service provider fulfils the 'step 1' sub-criteria referred to in paragraph 1 of this Article, the ESAs shall carry out their assessment in the light of the step two sub-criterion specified in Article 31(2), point (d)(i) of Regulation (EU) 2022/2554.

#### Article 6

##### Information sources to enable criticality assessment

1. The ESAs shall use the data provided by the registers of information referred to in Article 28(3) of Regulation (EU) 2022/2554, for the assessment of the sub-criteria listed in Articles 2 to 5. The ESAs may also use additional available data they have at their disposal from all sources of information to perform the criticality assessment.

2. The ESAs shall take into account the most recent data available to them during the assessment year, or where applicable, the data that has been made available to them at the latest by 31 December of the year preceding the criticality assessment.

#### Article 7

##### Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

However, the Lead Overseer shall apply the sub-criterion 1.4 referred to in Article 2, paragraph 5, point (b) as of 16 January 2025.

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

Done at Brussels, 22 February 2024.

## **APPENDIX II: Commission Delegated Regulation (EU) 2024/1505**

**of 22 February 2024**

### **supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid**

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<sup>40</sup>, and in particular Article 43(2) thereof,

Whereas:

- (1) An annual oversight fee should be established to fully cover the Lead Overseer's and the other European Supervisory Authorities' necessary expenditure when performing oversight tasks in the context of Regulation (EU) 2022/2554. The annual oversight fee should also cover the estimated costs by competent authorities to whom tasks are delegated by the European Supervisory Authorities.
- (2) In line with the principle of annuality and the principle of full cost recovery, the annual oversight fees should be calculated on the basis of the direct and indirect costs estimated by the ESAs to perform their oversight tasks. The annual oversight fees should be adjusted every year to match the estimated costs.
- (3) To ensure the fair allocation of oversight fees which, at the same time, reflects the actual administrative effort devoted to each overseen provider, the annual oversight fee should be proportionate to the turnover generated by the ICT third-party service provider in the Union from the provision of the ICT services to financial services clients.
- (4) To ensure the accuracy of the financial information needed to calculate the applicable turnover, all figures provided by the ICT third-party service providers should be audited. Considering that information on the applicable turnover is necessary for the Lead Overseer to establish the amount of the oversight fee charged to each critical ICT third-party service provider yearly to cover the costs of the oversight, the Lead Overseer should consider the worldwide revenues of ICT third-party service provider generated irrespective of the types of clients in the case where the critical ICT third-party service provider does not provide for tailored information on the revenues generated in the Union from the provision of the ICT services to financial entities.
- (5) A minimum annual oversight fee should be imposed on each critical ICT third-party service provider, given that certain fixed administrative costs apply for the oversight of all critical ICT third-party service providers, irrespective of the amount of turnover accrued.
- (6) To cater for the specific costs incurred during the first year of designation and oversight of critical ICT third-party service providers, related among others to the designation process and the appointment of

---

<sup>40</sup> OJ L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>

the Lead Overseer, a fixed fee should be established. To reflect the costs incurred for the oversight following the designation of the critical ICT third-party service provider, this fee should be adjusted to the period of time in that first year during which the critical ICT third-party service provider has been designated. It should replace the annual oversight fee for that year.

- (7) To cover the additional costs related to the designation of critical ICT third-party service providers that voluntarily request to be designated as critical in accordance with Article 31(11) of Regulation (EU) 2022/2554, an additional fixed fee should be established. In order to discourage unfounded requests, such additional fixed fee should not be reimbursed if an ICT third-party service provider withdraws its request during the registration process, nor if the request is rejected.
- (8) To ensure the timely payment of oversight fees, those fees should be paid within 30 days from the date of issuance of the Lead Overseer's debit note. To simplify the fee payment flows, and to ensure ESAs have the necessary funds to carry out their planned supervisory activities, annual oversight fees should be paid in a single instalment during the first four months of the calendar year for which such fees are due by critical ICT third-party service providers subject to oversight activities on 1 January of that year or, in the case of critical ICT third-party service providers designated throughout that year, at the latest by the end of that year.
- (9) All the fees charged should be set at a level such as to avoid a deficit or a significant accumulation of surplus. Where a significant positive or negative budget result becomes recurrent, the level of the fees should be revised,

HAS ADOPTED THIS REGULATION:

*Article 1*

**Estimation of the expenditures of the Lead Overseers when performing their oversight duties**

1. In each year, the Lead Overseer and the other European Supervisory Authorities shall estimate the overall annual costs that are expected to be incurred for the performance of their oversight duties. The amount of the overall annual costs estimated shall be the basis for determining the overall amount of oversight fees charged.
2. When estimating the annual overall costs, the Lead Overseer shall take into account the following direct and indirect costs:
  - (a) costs related to the designation of ICT third-party service providers as critical;
  - (b) costs related to the appointment of the Lead Overseer;
  - (c) costs related to the actual oversight of critical ICT third-party service providers, including the following:
    - (i) costs related to the work carried out by the joint examination team;
    - (ii) costs of advice provided by independent experts;
  - (d) costs related to the follow-up of the recommendations issued by the Lead Overseers in accordance with Article 35(1), point (d), of Regulation (EU) 2022/2554;
  - (e) costs related to the governance of the oversight framework.

*Article 2*

**Applicable turnover of critical ICT third-party service providers for the calculation of the oversight fees**

1. For the purposes of Article 3, the turnover of a critical ICT third-party service provider shall be its revenues generated in the Union from the provision of the ICT services listed in the implementing technical standards

adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554 and provided to the financial entities listed in Article 2(1) of Regulation (EU) 2022/2554.

2. Critical ICT third-party service providers shall provide the Lead Overseer on an annual basis in year n-1 with audited figures specifying the turnover referred to in paragraph 1 for year n-2. Critical ICT third-party service providers shall provide those figures to the Lead Overseer by 31 December each year.

3. Where the critical ICT third-party service provider does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to or entirely include revenues generated from the provision of services to financial entities listed in Article 2(1) of Regulation (EU) 2022/2554, the Lead Overseer shall consider the turnover generated in the Union from the provision of the ICT services listed in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554 irrespective of the type of clients of the critical ICT third-party service provider.

Where the critical ICT third-party service provider does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to or entirely include revenues generated in the Union from the provision of ICT services referred to in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554, the Lead Overseer shall consider the worldwide turnover generated from the provision of those ICT services.

Where the critical ICT third-party service provider does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to or entirely include revenues generated from the provision of ICT services to financial entities listed in Article 2(1) of Regulation (EU) 2022/2554, and it does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to revenues generated in the Union, the Lead Overseer shall consider the worldwide turnover irrespective of the type of clients of the critical ICT third-party service provider.

4. Where critical ICT third-party service providers report the revenues in a currency other than the euro, the Lead Overseer shall convert those revenues into euro using the average euro foreign exchange rate applicable to the period during which the revenues were recorded, as published by the European Central Bank.

### *Article 3*

#### **Calculation of the oversight fees**

1. For each critical ICT third-party service, the annual oversight fee for a given year (n) shall be the overall annual costs estimated referred to in Article 1 adjusted by the turnover coefficient referred to in paragraph 2 based on its applicable turnover for the year n-2.

2. For each critical ICT third-party service provider, the turnover coefficient shall be based on the applicable turnover referred to in Article 2 and shall be calculated as follows:

$$\text{Turnover coefficient in year (n)} = \frac{\text{applicable turnover of critical ICT third party service provider concerned in year (n-2)}}{\text{applicable turnover of all critical ICT third party service providers in year (n-2)}}$$

3. In no case shall the critical ICT third-party service provider pay an annual oversight fee that is less than EUR 50 000.

### *Article 4*

#### **Oversight fees in year of designation and 'opt-in' requests**

1. By way of derogation from Article 3, for the first published list of designated critical ICT third-party service providers as per Article 31(9) of Regulation (EU) 2022/2554, the oversight fees shall be equally split among the designated critical ICT third-party service providers. The fee to be charged to each critical ICT third-party service provider shall be calculated by dividing the overall estimated expenditure of the Lead Overseers with the number of designated critical ICT third-party service providers.

2. By way of derogation from Article 3 and paragraph 1 above, for the first year in which an ICT third-party service provider is designated as critical, it shall pay a fixed oversight fee which is equal to the amount paid by each ICT third party service provider under paragraph 1. Where the period of the oversight activities of such critical ICT third-party service provider does not correspond to a full year, that oversight fee shall be equal to the amount paid by each ICT third-party service provider under paragraph 1, multiplied by the number of calendar days from the designation of the ICT third-party service provider as critical until the end of that year and divided by the total number of days in that year.

3. Where an ICT third-party service provider requests to be designated as critical in accordance with Article 31(11) of Regulation (EU) 2022/2554, it shall pay a fixed opt-in fee of EUR 50 000. The recipient ESA shall not reimburse that fixed opt-in fee where the request to be designated as critical is rejected or withdrawn by the ICT third-party service provider.

#### *Article 5*

#### **Payment of the oversight fees**

1. Critical ICT third-party service providers shall pay the oversight fees referred to in Article 43 of Regulation (EU) 2022/2554 to the Lead Overseer on an annual basis.

2. All oversight fees shall be invoiced and paid in euro. Debit notes for oversight fees shall set payment terms of at least 30 days.

3. All oversight fees shall be paid based on a single instalment basis. Critical ICT third-party service providers which will be subject to oversight activities on 1 January of a given year shall pay the debit note by 30 April of that year. Critical ICT third-party service providers designated throughout the year shall pay the fees referred to in Article 4 in a single instalment by 31 December of that year.

4. Any late payment shall incur the default interest laid down in Article 99 of Regulation (EU, Euratom) 2018/1046.

#### *Article 6*

#### **Communication between the Lead Overseer and critical ICT third-party service providers**

For the purposes of this Regulation, all communication between the European Supervisory Authorities and critical ICT third-party service providers shall take place by electronic means.

#### *Article 7*

#### **Entry into force and date of application**

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, 22 February 2024.

## **APPENDIX III: Commission Delegated Regulation (EU) 2024/1772**

**of 13 March 2024**

### **supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents**

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<sup>41</sup>, and in particular Article 18(4), third subparagraph, thereof,

Whereas:

- (1) Regulation (EU) 2022/2554 aims to harmonise and streamline reporting requirements for ICT-related incidents and for operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions ('incidents'). Considering that the reporting requirements cover 20 different types of financial entities, the classification criteria and the materiality thresholds for determining major incidents and significant cyber threats should be specified in a simple, harmonised and consistent way that takes into account the specificities of the services and activities of all relevant financial entities.
- (2) In order to ensure proportionality, the classification criteria and the materiality thresholds should reflect the size and overall risk profile, and the nature, scale and complexity of the services of all financial entities. Moreover, the criteria and materiality thresholds should be designed in such a way that they apply consistently to all financial entities, irrespective of their size and risk profile, and do not pose unproportional reporting burden to smaller financial entities. However, in order to address situations where a significant number of clients are affected by an incident which as such does not exceed the applicable threshold, an absolute threshold mainly targeted at larger financial entities should be set out.
- (3) In relation to incident reporting frameworks, which have existed prior to the entry into force of Regulation (EU) 2022/2554, continuity for financial entities should be ensured. Therefore, the classification criteria and materiality thresholds should be aligned with and inspired by the EBA Guidelines on major incident reporting under Directive (EU) 2366/2015 of the European Parliament and of the Council<sup>42</sup>, the Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories, the ECB/SSM Cyber Incident Reporting Framework and other relevant guidance. The

---

<sup>41</sup> OJ L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

<sup>42</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35, ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

classification criteria and thresholds should also be suitable for the financial entities that have not been subject to incident reporting requirements prior to Regulation (EU) 2022/2554.

- (4) With regard to the classification criterion 'amount and number of transactions affected', the notion of transactions is broad and covers different activities and services across the sectorial acts applicable to financial entities. For the purposes of that classification criterion, payment transactions and all forms of exchange of financial instruments, crypto-assets, commodities, or any other assets, also in form of margin, collateral or pledge, both against cash and against any other asset, should be covered. All transactions that involve assets whose value can be expressed in a monetary amount should be considered for classification purposes.
- (5) The classification criteria should ensure that all relevant types of major incidents are captured. Cyber attacks related to intrusion into network or information systems may not necessarily be captured by many classification criteria. However, they are important since any intrusion in network and information systems may harm the financial entity. Accordingly, the classification criteria 'critical services affected' and 'data losses' should be specified in such a way as to capture these types of major incidents, in particular unauthorised intrusions which, even if the impacts are not immediately known, may lead to serious consequences, in particular data breaches and data leakages.
- (6) Since credit institutions are subject both to the framework for classification of incidents under Article 18 of Regulation (EU) 2022/2554 and to the operational risk framework under Commission Delegated Regulation (EU) 2018/959<sup>43</sup>, the approach for assessing the economic impact of an incident based on the calculation of costs and losses should, to the greatest possible extent, be consistent across both frameworks to avoid introducing incompatible or contradicting requirements.
- (7) The criterion in relation to the geographical spread of an incident set out in Article 18(1), point (c), of Regulation (EU) 2022/2554 should focus on the cross-border impact of the incident, since the impact of an incident on the activities of a financial entity within a single jurisdiction will be captured by the other criteria set out in that Article.
- (8) Given that the classification criteria are interdependent and linked to each other, the approach for identifying major incidents which are to be reported in accordance with Article 19(1) of Regulation (EU) 2022/2554 should be based on a combination of criteria, where some criteria that are closely related to the definitions of an ICT-related incident and a major ICT-related incident set out in Article 3(8) and (10) of Regulation (EU) 2022/2554 should have more prominence in the classification of major incidents than other criteria.
- (9) With a view to ensure that the reports on and notifications of major incidents received by competent authorities under Article 19(1) of Regulation (EU) 2022/2554 serve both for supervisory purposes and for the prevention of contagion across the financial sector, the materiality thresholds should make it possible to capture major incidents, by focusing, inter alia, on the impact on entity specific critical services, the specific absolute and relative thresholds of clients or financial counterparts, transactions that indicate a material impact on the financial entity, and the significance of the impact in other Member States.
- (10) Incidents that affect ICT services or network and information systems that support critical or important functions, or financial services requiring authorisation or malicious unauthorised access to network and information systems that support critical or important functions, should be considered as incidents affecting critical services of the financial entities. Malicious, unauthorised access to network and information systems that support critical or important functions of financial entities poses serious risks to the financial entity and, as they may affect other financial entities, should always be considered as major incidents which are to be reported.
- (11) Recurring incidents that are linked through a similar apparent root cause, which individually are not major incidents, can indicate significant deficiencies and weaknesses in the financial entity's incident and risk

---

<sup>43</sup> Commission Delegated Regulation (EU) 2018/959 of 14 March 2018 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council with regard to regulatory technical standards of the specification of the assessment methodology under which competent authorities permit institutions to use Advanced Measurement Approaches for operational risk (OJ L 169, 6.7.2018, p. 1, ELI: [http://data.europa.eu/eli/reg\\_del/2018/959/oj](http://data.europa.eu/eli/reg_del/2018/959/oj)).



management procedures. Therefore, recurring incidents should be considered as major collectively where they occur repeatedly over a certain period of time.

- (12) Considering that cyber threats can have a negative impact on the financial entity and sector, the significant cyber threats which financial entities may submit should indicate the probability of materialisation and the criticality of the potential impact. Accordingly, to ensure a clear and consistent assessment of the significance of cyber threats, the classification of a cyber threat as significant should be dependent on the likelihood that the classification criteria for major incidents and their threshold would be met if the threat had materialised, on the type of cyber threat and on the information available to the financial entity.
- (13) Considering that competent authorities in other Member States are to be notified of incidents that impact financial entities and customers in their jurisdiction, the assessment of the impact in another jurisdiction in accordance with Article 19(7) of Regulation (EU) 2022/2554 should be based on the root cause of the incident, on potential contagion through third-party providers and on financial market infrastructures, as well as on the impact of the incident on significant groups of clients or financial counterparts.
- (14) The reporting and notification processes referred to in Article 19(6) and (7) of Regulation (EU) 2022/2554 should allow the respective recipients to assess the impact of the incidents. Therefore, the transmitted information should cover all details contained in the incident reports submitted by the financial entity to the competent authority.
- (15) Where an incident constitutes a personal data breach according to Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>44</sup> and Directive 2002/58/EC of the European Parliament and of the Council<sup>45</sup>, this Regulation should not affect the recording and notification obligations for personal data breaches set out in those Union laws. The competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.
- (16) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities, in consultation with the European Union Agency for Cybersecurity (ENISA) and the European Central bank (ECB).
- (17) 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<sup>46</sup>, in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>47</sup> and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>48</sup> 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, (18) The European Data

---

<sup>44</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

<sup>45</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

<sup>46</sup> 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>).

<sup>47</sup> 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>).

<sup>48</sup> 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>).

Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council<sup>49</sup>

and delivered an opinion on 24 January 2024.

HAS ADOPTED THIS REGULATION:

## **Chapter I**

### **Classification criteria**

#### *Article 1*

#### **Clients, financial counterparts and transactions**

1. The number of clients affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, shall reflect the number of all affected clients, whether natural or legal persons, that are or were unable to make use of the service provided by the financial entity during the incident or that were adversely impacted by the incident. That number shall also include third parties explicitly covered by the contractual agreement between the financial entity and the client as beneficiaries of the affected service.
2. The number of financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554 shall reflect the number of all affected financial counterparts that have concluded a contractual arrangement with the financial entity.
3. In relation to the relevance of clients and financial counterparts affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial entity shall take into account the extent to which the impact on a client or a financial counterpart will affect the implementation of the business objectives of the financial entity, as well as the potential impact of the incident on market efficiency.
4. In relation to the amount or number of transactions affected by the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, the financial entity shall take into account all affected transactions involving a monetary amount where at least one part of the transaction is carried out in the Union.
5. Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estimate those numbers or amounts based on available data from comparable reference periods.

#### *Article 2*

#### **Reputational impact**

1. For the purposes of determining the reputational impact of the incident as referred to in Article 18(1), point (a), of Regulation (EU) 2022/2554, financial entities shall consider that a reputational impact has occurred where at least one of the following criteria is met:
  - (a) the incident has been reflected in the media;
  - (b) the incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business relationships;

---

<sup>49</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(c) the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident;

(d) the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the incident.

2. When assessing the reputational impact of the incident, financial entities shall take into account the level of visibility that the incident has gained or is likely to gain in relation to each criterion listed in paragraph 1.

### *Article 3*

#### **Duration and service downtime**

1. Financial entities shall measure the duration of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the incident occurs until the moment when it is resolved.

Where financial entities are unable to determine the moment when the incident occurred, they shall measure the duration of the incident from the moment it was detected. Where financial entities become aware that the incident occurred prior to its detection, they shall measure the duration from the moment the incident is recorded in network or system logs or other data sources.

Where financial entities do not yet know when the incident will be resolved or are unable to verify records in logs or other data sources, they shall apply estimates.

2. Financial entities shall measure the service downtime of an incident as referred to in Article 18(1), point (b), of Regulation (EU) 2022/2554, from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where the service downtime causes a delay in the provision of service after regular activities or operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is fully provided.

Where financial entities are unable to determine the moment when the service downtime started, they shall measure the service downtime from the moment it was detected.

### *Article 4*

#### **Geographical spread**

For the purpose of determining the geographical spread with regard to the areas affected by the incident as referred to in Article 18(1), point (c), of Regulation (EU) 2022/2554, financial entities shall assess whether the incident has or had an impact in other Member States, and in particular the significance of the impact in relation to any of the following:

(a) clients and financial counterparts in other Member States;

(b) branches or other financial entities within the group carrying out activities in other Member States;

(c) financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services, to the extent such information is available.

*Article 5*

**Data losses**

For the purpose of determining the data losses that the incident entails as referred to in Article 18(1), point (d), of Regulation (EU) 2022/2554, financial entities shall take into account the following:

- (a) in relation to the availability of data, whether the incident has rendered the data on demand by the financial entity, its clients or its counterparts temporarily or permanently inaccessible or unusable;
- (b) in relation to the authenticity of data, whether the incident has compromised the trustworthiness of the source of data;
- (c) in relation to the integrity of data, whether the incident has resulted in non-authorized modification of data that has rendered it inaccurate or incomplete;
- (d) in relation to the confidentiality of data, whether the incident has resulted in data having been accessed by or disclosed to an unauthorised party or system.

*Article 6*

**Criticality of services affected**

For the purpose of determining the criticality of the services affected as referred to in Article 18(1), point (e), of Regulation (EU) 2022/2554, financial entities shall assess whether the incident:

- (a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;
- (b) affects or has affected financial services provided by the financial entity that require authorisation, registration or that are supervised by competent authorities;
- (c) constitutes or has constituted a successful, malicious and unauthorised access to the network and information systems of the financial entity.

*Article 7*

**Economic impact**

1. For the purpose of determining the economic impact of the incident as referred to in Article 18(1), point (f), of Regulation (EU) 2022/2554, financial entities shall, without accounting for financial recoveries, take into account the following types of direct and indirect costs and losses which they have incurred as a result of the incident:

- (a) expropriated funds or financial assets for which they are liable, including assets lost to theft;
- (b) costs for replacement or relocation of software, hardware or infrastructure;
- (c) staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills;
- (d) fees due to non-compliance with contractual obligations;
- (e) costs for redress and compensation to customers;

- (f) losses due to forgone revenues;
  - (g) costs associated with internal and external communication;
  - (h) advisory costs, including costs associated with legal counselling, forensic services and remediation services.
2. Costs and losses referred to in paragraph 1 shall not include costs that are necessary for the day-to-day operation of the business, in particular the following:
- (a) costs for general maintenance of infrastructure, equipment, hardware and software, and costs for keeping skills of staff up to date;
  - (b) internal or external costs to enhance the business after the incident, including upgrades, improvements and risk assessment initiatives;
  - (c) insurance premiums.
3. Financial entities shall calculate the amounts of costs and losses based on data available at the time of reporting. Where the actual amounts of costs and losses cannot be determined, financial entities shall estimate those amounts.
4. When assessing the economic impact of the incident, financial entities shall sum up the costs and losses referred to in paragraph 1.

## Chapter II

### Major incidents and materiality thresholds

#### Article 8

#### Major incidents

1. An incident shall be considered a major incident for the purposes of Article 19(1) of Regulation (EU) 2022/2554 where it has affected critical services as referred to in Article 6 and where either of the following conditions is fulfilled:
- (a) the materiality threshold referred to in Article 9(5), point (b), is met;
  - (b) two or more of the other materiality thresholds referred to in Articles 9(1) to (6) are met.
2. Recurring incidents that individually are not considered a major incident in accordance with paragraph 1 shall be considered as one major incident where they meet all of the following conditions:
- (a) they have occurred at least twice within 6 months;
  - (b) they have the same apparent root cause as referred to in Article 20, first subparagraph, point (b) of Regulation (EU) 2022/2554;
  - (c) they collectively fulfil the criteria for being considered a major incident set out in paragraph 1.

Financial entities shall assess the existence of recurring incidents on a monthly basis.

This paragraph does not apply to microenterprises and to financial entities listed in Article 16(1) of Regulation (EU) 2022/2554.

*Article 9*

**Materiality thresholds for determining major incidents**

1. The materiality threshold for the criterion 'clients, financial counterparts and transactions' is met where any of the following conditions are fulfilled:

- (a) the number of affected clients is higher than 10 % of all clients using the affected service;
- (b) the number of affected clients using the affected service is higher than 100 000;
- (c) the number of affected financial counterparts is higher than 30 % of all financial counterparts carrying out activities related to the provision of the affected service;
- (d) the number of affected transactions is higher than 10 % of the daily average number of transactions carried out by the financial entity related to the affected service;
- (e) the amount of affected transactions is higher than 10 % of the daily average value of transactions carried out by the financial entity related to the affected service;
- (f) clients or financial counterparts which have been identified as relevant in accordance with Article 1(3) have been affected.

Where the actual number of clients or financial counterparts affected or the actual number or amount of transactions affected cannot be determined, the financial entity shall estimate those numbers or amounts based on available data from comparable reference periods.

2. The materiality threshold for the criterion 'reputational impact' is met where any of the conditions set out in Article 2, points (a) to (d), are fulfilled.

3. The materiality threshold for the criterion 'duration and service downtime' is met where any of the following conditions are fulfilled:

- (a) the duration of the incident is longer than 24 hours;
- (b) the service downtime is longer than 2 hours for ICT services that support critical or important functions.

4. The materiality threshold for the criterion 'geographical spread' is met where the incident has an impact in two or more Member States in accordance with Article 4.

5. The materiality threshold for the criterion 'data losses' is met where any of the following conditions are fulfilled:

- (a) any impact as referred to in Article 5 on the availability, authenticity, integrity or confidentiality of data has or will have an adverse impact on the implementation of the business objectives of the financial entity or on its ability to meet regulatory requirements;
- (b) any successful, malicious and unauthorised access not covered by point (a) occurs to network and information systems, where such access may result in data losses.

6. The materiality threshold for the criterion 'economic impact' is met where the costs and losses incurred by the financial entity due to the incident have exceeded or are likely to exceed 100 000 euro.

### Chapter III

#### Significant Cyber threats

##### Article 10

#### High materiality thresholds for determining significant cyber threats

For the purposes of Article 18(2) of Regulation (EU) 2022/2554, a cyber threat shall be considered significant where all of the following conditions are fulfilled:

- (a) the cyber threat, if materialised, could affect or could have affected critical or important functions of the financial entity, or could affect other financial entities, third-party providers, clients or financial counterparts, based on information available to the financial entity;
- (b) the cyber threat has a high probability of materialisation at the financial entity or at other financial entities, taking into account at least the following elements:
  - (i) applicable risks related to the cyber threat referred to in point (a), including potential vulnerabilities of the systems of the financial entity that can be exploited;
  - (ii) the capabilities and intent of threat actors to the extent known by the financial entity;
  - (iii) the persistence of the threat and any accrued knowledge about incidents that have impacted the financial entity or its third-party provider, clients or financial counterparts;
- (c) the cyber threat could, if materialised, meet any of the following:
  - (i) the criterion regarding criticality of services set out in Article 18(1), point (e), of Regulation (EU) 2022/2554, as specified in Article 6 of this Regulation;
  - (ii) the materiality threshold set out in Article 9(1);
  - (iii) the materiality threshold set out in Article 9(4).

Where, depending on the type of cyber threat and available information, the financial entity concludes that the materiality thresholds set out in Article 9(2), (3), (5) and (6) could be met, those thresholds may also be considered.

### Chapter IV

#### Relevance of major incidents to competent authorities in other Member States and details of reports to be shared with other competent authorities

##### Article 11

#### Relevance of major incidents to competent authorities in other Member States

The assessment of whether the major incident is relevant for competent authorities in other Member States as referred to in Article 19(7) of Regulation (EU) 2022/2554 shall be based on whether the incident has a root cause originating from another Member State or whether the incident has or has had a significant impact in another Member State in relation to any of the following:

- (a) clients or financial counterparts;

- (b) a branch of the financial entity or another financial entity within the group;
- (c) a financial market infrastructure or a third-party provider which may affect financial entities to which they provide services.

*Article 12*

**Details of major incidents to be shared with other competent authorities**

The details of major incidents to be submitted by competent authorities to other competent authorities in accordance with Article 19(6) of Regulation (EU) 2022/2554 and the notifications to be submitted by EBA, ESMA or EIOPA and the ECB to the relevant competent authorities in other Member States in accordance with Article 19(7) of that Regulation shall contain the same level of information, without any anonymisation, as the notifications and reports of major incidents received from financial entities in accordance with Article 19(4) of Regulation (EU) 2022/2554.

**Chapter V**

**final provisions**

*Article 13*

**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 March 2024



## **APPENDIX IV: Commission Delegated Regulation (EU) 2024/1773**

**of 13 March 2024**

### **supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers**

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<sup>50</sup>, and in particular Article 28(10), third subparagraph, thereof,

Whereas:

- (1) The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 requires that financial entities set out certain key principles to manage ICT third-party risk, which are of particular importance when financial entities engage with ICT third-party service providers to support their critical or important functions.
- (2) Financial entities, as part of their ICT risk management framework, are to adopt, and regularly review, a strategy on ICT third-party risk. In accordance with Article 28(2) of Regulation (EU) 2022/2554, that strategy is to include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. It is to apply on an individual and, where relevant, on a sub-consolidated and consolidated basis.
- (3) Financial entities vary widely in size, structure, and internal organisation and in the nature and complexity of their activities and operations. It is necessary to take into account that diversity while imposing certain fundamental regulatory requirements which are appropriate for all financial entities when developing the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions by ICT third-party providers ('the policy'), and to ensure that those requirements are applied in a manner that is proportionate.
- (4) Where financial entities belong to a group, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group should therefore ensure that the policy is applied in a consistent and coherent way within the group.
- (5) When applying the policy, ICT intra-group service providers, including those fully or collectively owned by financial entities within the same institutional protection scheme, should be considered as ICT third-party services providers. The risks posed by ICT intra-group service providers may be different but the requirements applicable to them are the same under Regulation (EU) 2022/2554. In a similar way, the policy should apply to subcontractors that provide ICT services supporting critical or important functions

---

<sup>50</sup> OJ L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

- or material parts thereof to ICT third-party service providers, where a chain of ICT third-party service providers exists.
- (6) The ultimate responsibility of the management body in managing a financial entity's ICT risk is an overarching principle which is also applicable regarding the use of ICT third-party service providers. This responsibility should be further translated into the continuous engagement of the management body in the control and monitoring of ICT risk management, including in the adoption and review, at least once per year, of the policy.
  - (7) To ensure appropriate reporting to the management body, the policy should clearly specify and identify the internal responsibilities for the approval, management, control and documentation of contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers ('contractual arrangements'), including the ICT services provided under contractual arrangements referred to in Article 28(1), point (a), of Regulation (EU) 2022/2554.
  - (8) In order to take into account all possible risks that may arise when contracting ICT services supporting critical or important function, the structure of the policy should follow all the steps of the each main phase of the life cycle for contractual arrangements with third-party providers.
  - (9) To mitigate the risks identified, the policy should specify the planning of contractual arrangements, including the risk assessment, the due diligence, and the approval process for new or material changes to those contractual arrangements. In order to manage the risks that may arise before entering into a contractual arrangement with an ICT third-party service provider, the policy should specify an appropriate and proportionate process to select and assess the suitability of prospective ICT third-party service providers and require that the financial entity takes into account a non-exhaustive list of elements that the ICT third-party service providers should have in place. The list should include elements related to the business reputation of the service providers, their financial, human and technical resources, their information-security, their organisational structure, including risk management, and their internal controls.
  - (10) To ensure a sound risk management in the provision of ICT services supporting critical or important functions by ICT third-party service providers, the policy should contain information about the implementation, monitoring and management of the contractual arrangements, including at consolidated and sub-consolidated level, where applicable. This includes requirements for the contractual clauses on mutual obligations of the financial entities and the ICT third-party service providers, which should be set out in writing. In order to ensure an efficient supervision and foster resilience in case of changes in the business model or business environment, the policy should ensure the financial entities' or appointed third parties' and competent authorities' rights to inspections and access to information and should also further specify the exit strategies and termination processes.
  - (11) To the extent personal data are processed by ICT third-party service providers, this policy and any contractual arrangements are without prejudice to and should complement the obligations under Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>51</sup>, such as to have a written contract in place describing the personal data processing, requirement to ensure security of personal data processing and setting out all other elements required under that regulation.
  - (12) 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<sup>52</sup>, in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>53</sup> and in Article 54 of Regulation (EU)

---

<sup>51</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

<sup>52</sup> 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>).

<sup>53</sup> 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>).

No 1095/2010 of the European Parliament and of the Council<sup>54</sup> 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,

- (13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council<sup>55</sup> and delivered an opinion on 24 January 2024,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

##### **Overall risk profile and complexity**

The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'policy') shall take into account 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, including elements relating to:

- (a) the type of ICT services included in the contractual arrangement on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'contractual arrangement') between the financial entity and the ICT third-party service provider;
- (b) the location of the ICT third-party service provider or the location of its parent company;
- (c) whether the ICT services supporting critical or important functions are provided by an ICT third-party service provider located within a Member State or in a third country, also considering the location from where the ICT services are provided and the location where the data is processed and stored;
- (d) the nature of the data shared with the ICT third-party service provider;
- (e) whether the ICT third-party service provider is part of the same group as the financial entity to which the services are provided;
- (f) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a competent authority in a Member State or subject to the oversight framework under Chapter V, Section II, of Regulation (EU) 2022/2554, and the use of ICT third-party service providers that are not;
- (g) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a supervisory authority in a third country, and the use of ICT third-party service providers that are not;

---

<sup>54</sup> 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>).

<sup>55</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

- (h) whether the provision of ICT services supporting critical or important functions are concentrated to a single ICT third-party service provider or a small number of such service providers;
- (i) the transferability of the ICT services supporting critical or important functions to another ICT third-party service provider, including as a result of technology specificities;
- (j) the potential impact of disruptions in the provision of the ICT services supporting critical or important functions on the continuity of the financial entity's activities and on the availability of its services.

*Article 2*

**Group application**

Where this Regulation applies on a sub-consolidated or consolidated basis, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall ensure that the policy is implemented consistently in all financial entities that are part of the group and is adequate for the effective application of this Regulation at all relevant levels of the group.

*Article 3*

**Governance arrangements**

1. The management body shall review the policy at least once a year and update it where necessary. Changes made to the policy shall be implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. The financial entity shall document the planned timeline for the implementation.
2. The policy shall establish or refer to a methodology for determining which ICT services support critical or important functions. The policy shall also specify when this assessment is to be conducted and reviewed.
3. The policy shall clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and shall ensure that appropriate skills, experience and knowledge are maintained within the financial entity to effectively oversee the relevant contractual arrangements, including the ICT services provided under those arrangements.
4. Without prejudice to the final responsibility of the financial entity to effectively oversee relevant contractual arrangements, the policy shall require that the ICT third party service provider is assessed to have sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements regarding the ICT services supporting critical or important functions that are provided.
5. The policy shall clearly identify the role or member of senior management responsible for monitoring the relevant contractual arrangements. The policy shall specify how that role or member of senior management shall cooperate with the control functions, unless it is part of it, and shall set out the reporting lines to the management body, including the nature of the information to report and the documents to provide. It shall also set out the frequency of such reporting.
6. The policy shall ensure that the contractual arrangements are consistent with the following:
  - (a) the ICT risk management framework referred to in Article 6 of Regulation (EU) 2022/2554;
  - (b) the information security policy referred to in Article 9(4) of Regulation (EU) 2022/2554;
  - (c) the ICT business continuity policy referred to in Article 11 of Regulation (EU) 2022/2554;
  - (d) the requirements on incident reporting set out in Article 19 of Regulation (EU) 2022/2554.

7. The policy shall require that ICT services supporting critical or important functions provided by ICT third party service providers are subject to independent review and are included in the audit plan.
8. The policy shall explicitly specify that the contractual arrangements:
  - (a) do not relieve the financial entity and its management body of its regulatory obligations and its responsibilities to its clients;
  - (b) are not to prevent effective supervision of a financial entity and are not to contravene any supervisory restrictions on services and activities;
  - (c) are to require that the ICT third party service providers cooperate with the competent authorities;
  - (d) are to require that the financial entity, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting critical or important functions.

#### *Article 4*

#### **Main phases of the life cycle for the adoption and use of contractual arrangements**

The policy shall specify the requirements, including the rules, the responsibilities and the processes, for each main phase of the lifecycle of the contractual arrangement, covering at least the following:

- (a) the responsibilities of the management body, including its involvement, as appropriate, in the decision-making process on the use of ICT services supporting critical or important functions provided by ICT third-party service providers;
- (b) the planning of contractual arrangements, including the risk assessment, the due diligence as set out in Articles 5 and 6 and the approval process regarding new or material changes to contractual arrangements as set out in Article 8(4);
- (c) the involvement of business units, internal controls and other relevant units in respect of contractual arrangements;
- (d) the implementation, monitoring and management of contractual arrangements as referred to in Articles 7, 8 and 9, including at consolidated and sub-consolidated level, where applicable;
- (e) the documentation and record-keeping, taking into account the requirements with regard to the register of information laid down in Article 28(3) of Regulation (EU) 2022/2554;
- (f) the exit strategies and termination processes as set out in Article 10.

#### *Article 5*

#### **Ex-ante risk assessment**

1. The policy shall require that the business needs of the financial entity are defined before a contractual arrangement is concluded.
2. The policy shall require that a risk assessment is conducted at financial entity level and, where applicable, at consolidated and sub-consolidated level before a contractual arrangement is concluded.

The risk assessment shall take into account all the relevant requirements laid down in Regulation (EU) 2022/2554 and applicable sectoral Union legislation. It shall consider, in particular, the impact of the provision of ICT services supporting critical or important functions by ICT third-party service providers on the financial entity and all the

risks posed by the provision of those ICT services supporting critical or important functions by ICT third-party service providers, including the following:

- (a) operational risks;
- (b) legal risks;
- (c) ICT risks;
- (d) reputational risks;
- (e) risks linked to the protection of confidential or personal data;
- (f) risks linked to the availability of data;
- (g) risks linked to the location where the data is processed and stored;
- (h) risks linked to the location of the ICT third-party service provider;
- (i) ICT concentration risks at entity level.

#### *Article 6*

#### **Due diligence**

1. The policy shall set out an appropriate and proportionate process for selecting and assessing the prospective ICT third-party service providers taking into account whether or not the ICT third party service provider is an intragroup ICT service provider, and shall require that the financial entity assesses, before entering into a contractual arrangement, whether the ICT third-party service provider:

- (a) has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure, risk management and internal controls and, if applicable, the required authorisations or registrations to provide the ICT services supporting the critical or important function in a reliable and professional manner;
- (b) has the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;
- (c) uses or intends to use ICT sub-contractors to perform the ICT services supporting critical or important functions or material parts thereof;
- (d) (is located, or processes or stores the data in a third country and, if this is the case, whether this practice affects the level of operational or reputational risks or the risk of being affected by restrictive measures, including embargos and sanctions, that may impact the ability of the ICT third-party service provider to provide the ICT services or the financial entity to receive those ICT services;
- (e) consents to contractual arrangements that ensure that it is effectively possible to conduct audits at the ICT third-party service provider, including onsite, by the financial entity itself, appointed third parties, and competent authorities;
- (f) acts in an ethical and socially responsible manner, respects human rights and children's rights, including the prohibition of child labour, respects applicable principles on environmental protection, and ensures appropriate working conditions.

2. The policy shall specify the required level of assurance concerning the effectiveness of ICT third-party service providers' risk management framework for the ICT services supporting critical or important functions to be provided by an ICT third-party service provider. The policy shall require that the due diligence process includes an assessment of the existence of risk mitigation and business continuity measures and of how their functioning within the ICT third-party service provider is ensured.

3. The policy shall determine the due diligence process for selecting and assessing the prospective ICT third-party service providers and shall indicate which of the following elements are to be used for the required level of assurance on the ICT third-party service provider's performance:

- (a) audits or independent assessments performed by the financial entity itself or on its behalf;
- (b) the use of independent audit reports made on request by the ICT third-party service provider;
- (c) the use of audit reports made by the internal audit function of the ICT third-party service provider;
- (d) the use of appropriate third-party certifications;
- (e) the use of other relevant information available to the financial entity or other information provided by the ICT third-party service provider.

4. Financial entities shall ensure an appropriate level of assurance on the ICT third-party service provider's performance, taking into account the elements listed in paragraph 3, points (a) to (e). Where appropriate, more than one element listed in those points shall be used.

#### *Article 7*

##### **Conflicts of interest**

1. The policy shall specify the appropriate measures to identify, prevent and manage actual or potential conflicts of interest arising from the use of ICT third-party service providers that are to be taken before entering relevant contractual arrangements and shall provide for an ongoing monitoring of such conflicts of interest.

2. Where ICT services supporting critical or important functions are provided by ICT intra-group service providers, the policy shall specify that decisions on the conditions, including the financial conditions, for the ICT services are to be taken objectively.

#### *Article 8*

##### **Contractual clauses**

1. The policy shall specify that the relevant contractual arrangements are to be in written form and are to include all the elements referred to in Article 30(2) and (3) of Regulation (EU) 2022/2554. The policy shall also include elements regarding requirements referred to in Article 1(1), point (a), of Regulation (EU) 2022/2554, as well as other relevant Union and national law as appropriate.

2. The policy shall specify that the relevant contractual arrangements are to include the right for the financial entity to access information, to carry out inspections and audits, and to perform tests on ICT. For that purpose, the policy shall require that the financial entity uses the following methods, without prejudice to the ultimate responsibility of the financial entity:

- (a) its own internal audit or an audit by an appointed third party;
- (b) where appropriate, pooled audits and pooled ICT testing, including threat-led penetration testing, that are organised jointly with other contracting financial entities or firms that use ICT services of the same ICT third-party service provider and that are performed by those contracting financial entities or firms or by a third party appointed by them;

- (c) where appropriate, third-party certifications;
  - (d) where appropriate, internal or third-party audit reports made available by the ICT third-party service provider.
3. The financial entity shall not over time rely solely on certifications referred to in paragraph 2, point (c), or audit reports referred to in point (d) of that paragraph. The policy shall only permit the use of the methods referred to in paragraph 2, points (c) and (d), where the financial entity:
- (a) is satisfied with the audit plan of the ICT third-party service provider for the relevant contractual arrangements;
  - (b) ensures that the scope of the certifications or audit reports cover the systems and key controls identified by it and ensures compliance with relevant regulatory requirements;
  - (c) thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verifies that the reports or certifications are not obsolete;
  - (d) ensures that key systems and controls are covered in future versions of the certification or audit report;
  - (e) is satisfied with the aptitude of the certifying or auditing party;
  - (f) is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;
  - (g) has the contractual right to request, with a frequency that is reasonable and legitimate from a risk management perspective, modifications of the scope of the certifications or audit reports to other relevant systems and controls;
  - (h) has the contractual right to perform individual and pooled audits at its discretion with regard to the contractual arrangements and execute those rights in line with the agreed frequency.
4. The policy shall ensure that material changes to the contractual agreement are to be formalised in a written document which is dated and signed by all parties and shall specify the renewal process for the contractual arrangements.

#### *Article 9*

#### **Monitoring of the contractual arrangements**

1. The policy shall require that the contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures. The policy shall also specify measures that apply when service level agreements are not met, including contractual penalties where appropriate.
2. The policy shall specify how the financial entity is to assess whether the ICT third-party service providers used for the ICT services supporting critical or important functions meet appropriate performance and quality standards in line with the contractual arrangement and the financial entity's own policies. The policy shall, in particular, ensure the following:
  - (a) that the ICT third-party service providers provide appropriate reports on their activities and services to the financial entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and reports on business continuity measures and testing;



- (b) that the performance of ICT third-party service providers is assessed with key performance indicators, key control indicators, audits, self-certifications and independent reviews in line with the financial entity's ICT risk management framework;
  - (c) that the financial entity receives other relevant information from the ICT third-party service providers;
  - (d) that the financial entity is notified, where appropriate, of ICT-related incidents and operational or security payment-related incidents;
  - (e) that an independent review and audits verifying compliance with legal and regulatory requirements and policies are performed.
3. The policy shall specify that the assessment referred to in paragraph 2 is to be documented and its results to be used to update the financial entity's risk assessment referred to in Article 6.
4. The policy shall establish the appropriate measures that the financial entity is to adopt if it identifies shortcomings of the ICT third-party service providers, including ICT-related incidents and operational or security payment related incidents, in the provision of the ICT services supporting critical or important functions or in the compliance with contractual arrangements or legal requirements. It shall also specify how the implementation of such measures is to be monitored in order to ensure that they are effectively complied with within a defined timeframe, taking into account the materiality of the shortcomings.

#### *Article 10*

##### **Exit from and termination of the contractual arrangements**

The policy shall contain requirements for a documented exit plan for each contractual arrangement and for the periodic review and testing of the documented exit plan. When establishing the exit plan, the following shall be taken into account:

- (a) unforeseen and persistent service interruptions;
- (b) inappropriate or failed service delivery;
- (c) the unexpected termination of the contractual arrangement.

The exit plan shall be realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the contractual arrangements.

#### *Article 11*

##### **Entry into force**

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

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

Done at Brussels, 13 March 2024.

## **APPENDIX V: Commission Delegated Regulation (EU) 2024/1774**

**of 13 March 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**

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<sup>56</sup>, 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 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

---

<sup>56</sup> OJ L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

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<sup>57</sup>. 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.
- (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 data 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.

---

<sup>57</sup> 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>).

- (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<sup>58</sup>, (EU) No 600/2014<sup>59</sup> and (EU) No 909/2014<sup>60</sup> 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 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<sup>61</sup>, in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>62</sup> and in Article 54 of Regulation (EU)

---

<sup>58</sup> 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>).

<sup>59</sup> 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>).

<sup>60</sup> 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>).

<sup>61</sup> 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>).

<sup>62</sup> 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>).

No 1095/2010 of the European Parliament and of the Council<sup>63</sup> 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, Regulations (EU) 2016/679<sup>64</sup> and (EU) 2018/1725<sup>65</sup> of the European Parliament and of the Council should fully apply. For instance, the data minimisation principle should be complied with where personal data are collected 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**

<sup>63</sup> 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>).

<sup>64</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

<sup>65</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

***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:
- (iv) vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions;
  - (v) 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 prompt 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, first subparagraph, 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, first subparagraph, 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**

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) (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 in 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, first paragraph, 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<sup>66</sup>;
- (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.

#### *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, first paragraph, 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;

---

<sup>66</sup> 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>).



- (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) (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) 2024/1772<sup>67</sup> 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**

---

<sup>67</sup> Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents (OJ L, 2024/1772, 25.6.2024, ELI: [http://data.europa.eu/eli/reg\\_del/2024/1772/oj](http://data.europa.eu/eli/reg_del/2024/1772/oj)).

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:
  - (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**

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, first paragraph, 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, assess 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;
  - (i) 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 March 2024.

## APPENDIX VI: Draft Implementing Technical Standards

### on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

[\(JC 2023 85 – 10 01 2024\)](#)

[Art. 28(9)]

COMMISSION IMPLEMENTING REGULATION (EU) .../...

of **XX Month YYYY**

laying down implementing technical standards with regard to standard templates for the register of information according to Regulation (EU) 2022/2554 of the European Parliament and of the Council

(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<sup>68</sup> and in particular the second subparagraph of Article 28(9) thereof,

Whereas:

- (1) This Regulation establishes standard templates for the purposes of the register of information, including information that is common to all contractual arrangements on the use of information and communication technology (ICT) services. Information gathered from the register of information is essential for (i) the financial entities' internal ICT risk management, (ii) the effective supervision of the financial entities by their competent authorities and (iii) the establishment and conduct of oversight of the critical ICT third-party providers by the Lead Overseer as well as the annual process to designate critical ICT third-party service providers by the European Supervisory Authorities (ESAs).
- (2) To ensure supervisory outcomes which are consistent with the existing supervisory frameworks, the parent undertaking of financial entities that are part of a group as defined in the applicable financial services regulations should define the scope of entities to be included in the register of information at sub-consolidated and consolidated level by applying these financial services regulations. To reduce their administrative costs, groups may develop a single register of information at entity, subconsolidated and consolidated levels in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers to all the financial entities, which are part of the group. In such cases, the single register of information should allow each financial entity to fulfil its obligation to maintain and update the register of information at entity and sub-consolidated level, when applicable, including its reporting to its competent authority.

---

<sup>68</sup> OJ L 333, 27.12.2022, p. 1.

- (3) Pursuant to Article 28(1), point (b) of Regulation (EU) 2022/2554, the financial entities' management of ICT third-party risks takes into account the nature, scale, complexity and importance of ICT-related dependencies, as well as the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers. This should take into account the criticality or importance of the service, process or function and the potential impact on the continuity and availability of financial services and activities, at entity and at group level.
- (4) Union financial services sectoral specific laws contain certain rules on outsourcing, which have been further detailed by the ESAs through the development of guidelines containing the expectation for some financial entities to record specific information on their outsourcing arrangements, in some cases also in the form of registers, as part of their outsourcing risk management. In recent years, several National and European Competent Authorities performed data collection of information included in such registers as part of their supervision of financial entity compliance to the outsourcing requirements. Leveraging on the lessons learned from the different data collection exercises of outsourcing registers performed in the recent years by competent authorities and the ESAs, the templates established by this Regulation are designed in a technologyneutral manner building up on open tables, which have a predefined number of columns but an indefinite number of rows. In addition, the templates are linked to one another by using different specific keys to form a relational structure between them.
- (5) In order to receive ICT services from an ICT third-party service provider, including ICT intra-group service providers, financial entities conclude a written contract with the ICT third-party service provider. In case of groups, ICT intra-group service providers may conclude a contract with ICT third-party providers external to the group to provide ICT services to one or more financial entities of the group. In order to capture the full ICT service supply chain, financial entities maintaining the register of information should report information on both the contractual arrangement with their ICT intra-group service provider as well as information on the arrangement stipulated by the ICT intragroup service provider and the ICT third-party providers external to the group as subcontractors. To reflect this practice, the register of information includes a specific template allowing the reconciliation between the intra-group contracts and the contracts with ICT third-party service providers external to the group.
- (6) The provision of ICT services to financial entities may rely on potentially long or complex chains of subcontracting which should be monitored by the financial entities. Financial entities should assess the associated risks, including ICT third-party concentration risk with regard to the ICT third-party service providers supporting a critical or important function or material part thereof, considering a risk-based approach and the principle of proportionality. To enable this assessment, financial entities should be required to document within the register of information only those subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof, including all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision. In identifying those subcontractors, financial entities should consider business and ICT service continuity and ICT security aspects.
- (7) In case a financial entity outsources a function or activity to a service provider, and this service provider makes use of ICT services to support this function or activity, the responsibility for ensuring the operational resilience of that function or activity remains with the financial entity. Therefore, for the purpose of the register of information, the service provider should be treated as a direct ICT third-party service provider. In the case where a financial entity or a management entity acting on behalf of the financial entity, outsources all its activity to a service provider, the ICT third-party service providers to that service provider should be treated as a direct ICT third-party service provider of the financial entity or of the management entity, respectively.
- (8) To allow transparency and comparability of contractual arrangements and their ongoing monitoring, the register of information focuses on the operational links between the financial entities and the ICT third-party service providers. This is enabled by using four keys, which, among others, serve to link relevant data to each other across the templates of the register of information: (i) the contractual arrangement reference number between the financial entity signing the contractual arrangement and the direct ICT third-party provider, (ii) the legal entity identifier (LEI) of financial entities and the ICT third-party service providers, (iii) the function identifier and (iv) the type of ICT services.

- (9) The templates of the register of information use a valid LEI to identify financial entities and the ICT third-party service providers who provide ICT services to financial entities either directly or through subcontracting. To enable the competent authorities, the Oversight Forum and the ESAs to carry out their duties as stipulated in Regulation (EU) 2022/2554, it is necessary to use a unique international identifier for an unambiguous and consistent identification of financial entities and ICT third-party service providers at a global level. In contrast to national codes or names of legal entities, LEI is a widely recognised and financially accessible international identifier suited for overseeing complex subcontracting chains where providers from multiple jurisdictions provide ICT services. Only an international identifier allows for aggregation of information at the European level, improving the quality and timeliness of aggregated data and reducing the reporting burden for reporting entities. The template ensures that individuals acting in a business capacity as ICT third-party service providers have an alternative to LEI.
- (10) As each financial entity, including financial entities from the same group, have their own internal taxonomy of functions depending on their specific business models and internal organisations, financial entities should themselves identify relevant functions by the function identifier at individual and group level to allow for a clear monitoring between the functions of the financial entities and the ICT services.
- (11) To enable the operability of the register of information at entity, sub-consolidated and consolidated level across all the financial entities that are part of the same group, financial entities should ensure the uniformity, correctness and consistency of all the data in the register of information. In particular, ensuring the unicity and consistency across the scope of consolidation of the different keys e.g. the contractual arrangement reference numbers, the function identifier and the unique identifiers of the financial entities and ICT third-party service providers (i.e. 'LEI') is crucial to ensure such operability.
- (12) The structure of the templates and the requirements of the data points are designed considering data management and reporting perspectives to ensure consistency and harmonisation by design and avoid burdensome reprocessing of data for reporting purposes. When maintaining and updating the register of information, financial entities should adhere to data quality principles and ensuring therefore full comparability of the information reported in the register of information with the one provided in other regulatory or statistical reporting.
- (13) This Regulation is based on the draft implementing technical standards submitted to the European Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority (the ESAs).
- (14) The ESAs have conducted open public consultations on the draft implementing technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the ESAs' Stakeholder Groups established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council<sup>69</sup>, Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>70</sup> and Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>71</sup>.

HAS ADOPTED THIS REGULATION:

---

<sup>69</sup> 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).

<sup>70</sup> Regulation (EU) No 1094/2010 of the European Parliament and of the Council 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).

<sup>71</sup> 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).

CHAPTER I

**SUBJECT MATTER AND DEFINITIONS**

*Article 1*

**Subject matter**

This Regulation lays down implementing technical standards to establish the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of information and communication technology (ICT) services provided by ICT third-party service providers referred to in Article 28(3) of Regulation (EU) 2022/2554.

*Article 2*

**Definitions**

1. For the purposes of this Regulation, the following definitions shall apply:

- (a) ‘direct ICT third-party service provider’ means an ICT third-party service provider or ICT intra-group service provider that signed a contractual arrangement with:
- a. a financial entity to provide its ICT services directly to that financial entity;
  - b. a financial or a non-financial entity to provide its services to other financial entities within the same group.

The rank of the direct ICT third-party service provider in the ICT service supply chain is always ‘1’.

(b) ‘subcontractor’ means an ICT third-party service provider or ICT intra-group service provider that provides ICT services to another ICT third-party service provider in the same ICT service supply chain. The rank of the subcontractor in the ICT service supply chain is always higher than ‘1’;

(c) ‘ICT service supply chain’ means a sequence of contractual arrangements connected with the ICT service being provided by the direct ICT third-party service provider to the financial entity, starting with the direct ICT third-party service provider which has one or multiple other ICT third-party service providers as counterparties (subcontractors);

(d) ‘rank’ means the position of an ICT third-party service provider in the ICT service supply chain. The rank assigned to each ICT third-party service provider is any natural number higher or equal to ‘1’. The lower the natural number assigned to the rank, the closer the arrangement is to the financial entity.

CHAPTER II

**CONTENT OF THE REGISTER OF INFORMATION**

*Article 3*

**General requirements for maintaining and updating the register of information**

1. Financial entities that maintain and update the register of information shall ensure that:
  - a. the register of information includes the required information in relation to all the ICT services provided by direct ICT third-party providers; and

- b. the register of information includes information on all subcontractors that effectively underpin ICT services supporting critical or important functions or material part thereof.
2. Financial entities shall ensure that the information contained in the register of information is accurate and consistent. To this end, financial entities shall review the information contained in the register of information on a regular basis. Financial entities shall promptly correct any errors or discrepancies detected. In case of groups, financial entities responsible for maintaining and updating the register of information at subconsolidated and consolidated level shall ensure that information in relation to entity level within the scope of consolidation is correct and consistent with the information at the sub-consolidated and consolidated level.
  3. Financial entities shall maintain the information in the register of information in relation to contractual arrangements that are terminated for at least 5 years after the termination of the provision of the ICT services. This requirement shall apply to the contractual arrangements in force from the date of application of Regulation (EU) 2022/2554.
  4. Financial entities shall ensure that the information contained in the register adhere to the principles of data quality, i.e., accuracy, completeness, consistency, integrity, uniqueness, and validity.
  5. Financial entities shall use a valid and active legal entity identifier (LEI) to identify all of their ICT third-party service providers that are legal persons, except for individuals acting in a business capacity who chose not to obtain an LEI.
  6. When an ICT service provided by a direct ICT third-party service provider is supporting a critical or important function of the financial entities, financial entities shall ensure through the direct ICT third-party service provider, that all the subcontractors included in the register of information according to paragraph (1) point b. of this Article, obtain and maintain a valid and active LEI except if these are individuals acting in a business capacity who chose not to obtain an LEI.

#### *Article 4*

##### **Data format requirement**

Financial entities maintaining and updating the register of information at entity level, or at sub-consolidated and consolidated level shall complete the templates of the register of information using the formats set out in the instructions in Annex I, in accordance with the following requirements:

1. each template composing the register of information shall be a table with a predefined number of columns but an indefinite number of rows;
2. financial entities shall complete each data point with a single value. If more than one value is valid for a specific data point, the financial entities shall add an additional row in the corresponding template for each valid value;
3. financial entities shall report all data points in the register of information at entity level, sub-consolidated and consolidated level, as applicable. If the data is not applicable, financial entities shall record the string 'not applicable';
4. financial entities shall express all amounts in the same currency used by the financial entity for the preparation of the financial statements at entity, subconsolidated or consolidated level, as applicable;
5. when amounts are in a currency other than the currency used for the purposes of maintaining the register of information, financial entities shall convert the amounts into the reporting currency using the same basis of conversion as they use for accounting purposes.

#### *Article 5*

##### **Content of the register of information**

1. Financial entities shall include in the register of information at least the following information:

- (a) general information on the financial entity maintaining and updating the register of information at entity, sub-consolidate and consolidated level, respectively as specified in template RT.01.01 and in accordance with the instructions set out in Annex I of this Regulation;
- (b) general information on the entities in the scope of consolidation as specified in template RT.01.02 and in accordance with the instructions set out in Annex I of this Regulation;
- (c) identification of the branches of financial entities located outside the home country listed in template RT.01.02, where applicable, as specified in template RT.01.03 and in accordance with the instructions set out in Annex I of this Regulation;
- (d) general information on the contractual arrangements as specified in template RT.02.01 and in accordance with the instructions set out in Annex I of this Regulation;
- (e) specific information on the contractual arrangements as specified in template RT.02.02, and in accordance with the instructions set out in Annex I of this Regulation;
- (f) information on the links between intra-group contractual arrangements and contractual arrangements with ICT third-party service provider which are not part of the group using the contractual reference numbers when part of the ICT service supply chain is intra-group as specified in template RT.02.03, and in accordance with the instructions set out in Annex I of this Regulation;
- (g) information on the links between intra-group contractual arrangements and contractual arrangements with ICT third-party service provider which are not part of the group using the contractual reference numbers when part of the ICT service supply chain is intra-group as specified in template RT.02.03, and in accordance with the instructions set out in Annex I of this Regulation;
- (h) information on the entities signing the contractual arrangements with the direct ICT third-party service providers for receiving ICT services or on behalf of the entities making use of the ICT services as specified in template RT.03.01 and in accordance with the instructions set out in Annex I of this Regulation;
- (i) identification of the ICT third-party service providers signing the contractual arrangements for providing ICT service(s) as specified in template RT.03.02 and in accordance with the instructions set out in Annex I of this Regulation;
- (j) identification of the entities signing the contractual arrangements for providing ICT service(s) to other entities within the scope of consolidation as specified in template RT.03.03 and in accordance with the instructions set out in Annex I of this Regulation;
- (k) information on the entities making use of the ICT services provided by the ICT third-party service providers as specified in template RT.04.01 and in accordance with the instructions set out in Annex I of this Regulation;
- (l) information on the direct ICT third-party service providers and subcontractors, as specified in template RT.05.01 and in accordance with the instructions set out in Annex I of this Regulation;
- (m) information on the ICT service supply chain, as specified in template RT.05.02 and in accordance with the instructions set out in Annex I of this Regulation;
- (n) information on the identification of functions as specified in template RT.06.01, and in accordance with the instructions set out in Annex I of this Regulation;

(o) information on the assessment of the ICT services provided by ICT third-party service providers supporting a critical or important function or material part thereof provided as specified in template RT.07.01 and in accordance with the instructions set out in Annex I of this Regulation;

(p) information on the internal definitions used by financial entities and the terms included in close lists and taxonomies used when filling in the templates as specified in template RT.99.01 and in accordance with the instructions set out in Annex I of this Regulation.

2. Where relevant for their risk management or contract management purposes, financial entities may include into the register of information additional information not specified in this Regulation in the format that is most appropriate for the purposes of such additional information.

## CHAPTER III

### SCOPE OF CONSOLIDATION

#### *Article 6*

#### **Scope of the register of information at sub-consolidated and consolidated level**

1. In the case of groups, the parent undertakings shall take into account the relevant financial services regulations when identifying the scope of entities to be included in the register of information.

2. Register of information maintained and updated at sub-consolidated and consolidated levels shall encompass all financial entities and ICT intra-group service providers, which are part of the sub-group and group.

## CHAPTER IV

### FINAL PROVISIONS

#### *Article 7*

#### **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,



**ANNEX I****Instructions for completing the register of information****Part 1****General instructions**

Financial entities while maintaining and updating the register of information at entity, subconsolidated and consolidated level, shall fill-in the templates of the register of information with data using the formats set out in the instructions in Part 2 of this annex.

Part 2 of this annex lays down instructions to be followed by financial entities to complete each column of each template. In order to complete the information of certain columns, financial entities shall refer to other annexes of this Regulation or other external sources to complete the templates. In such cases, the reference to the relevant annexes or external sources is indicated in the instructions.

**List of the templates**

Template Code	Template Name	Short Description
RT.01.01	Entity maintaining the register of information	This template identifies the entity maintaining and updating the register of information at entity, subconsolidated and consolidated level, respectively.
RT.01.02	List of entities within the scope of consolidation	This template identifies all the entities belonging to the group. In case the financial entity responsible for maintaining and updating the register of information does not belong to a group, only this financial entity shall be reported in this template.
RT.01.03	List of branches	Objective of this template is to identify the branches of the financial entities referred to in template RT.01.02.
RT.02.01	Contractual arrangements – general information	Objective of this template is to list all contractual arrangements with direct ICT third-party service providers.  For each contractual arrangement with direct ICT third-party service provider, the financial entity maintaining the register of information shall assign a unique ‘contractual arrangement reference number’ to identify unambiguously the contractual arrangement itself.
RT.02.02	Contractual arrangements – specific information	Objective of this template is to provide details in relation to each contractual arrangement listed in template RT.02.01 with regard to:  (i) the ICT services included in the scope of the contractual arrangement;  (ii) the functions of the financial entities supported by those ICT services;  (iii) other important information in relation to the specific ICT services provided (e.g. notice period, law governing the arrangement, etc.).

Template Code	Template Name	Short Description
RT.02.03	List of intra-group contractual arrangements	Objective of this template is to identify the links between intra-group contractual arrangements and contractual arrangements with ICT third-party service provider which are not part of the group using the contractual reference numbers when part of the ICT service supply chain.
RT.03.01	Entities signing the contractual arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)	<p>Objective of this template is to provide information on the entity signing the contractual arrangements with the direct ICT third-party service provider for the entity making use of the ICT services.</p> <p>In case the register of information is maintained and updated at entity level, the entity signing the contractual arrangement and the entity making use of the ICT services is the financial entity maintaining and updating the register of information.</p> <p>Within the scope of sub-consolidation and consolidation, the financial entity making use of the ICT services provided is not necessarily the entity signing the contractual arrangement with the ICT third-party service providers.</p>
RT.03.02	ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)	Objective of this template is to identify all the ICT third-party service providers referred to in template RT.05.01 signing the contractual arrangements referred to in template RT.02.01 for providing the ICT services.
RT.03.03	Entities signing the Contractual arrangements for providing ICT service(s) to other entities within the scope of consolidation	Objective of this template is to identify all the entities referred to in template RT.01.02 signing the contractual arrangements referred to in template RT.02.01 for providing the ICT services to other entities in the scope of consolidation.
RT.04.01	Entities making use of the ICT services	<p>Objective of this template is to ensure that all entities making uses of the ICT services provided by ICT thirdparty service providers are registered in the register of information.</p> <p>The entities making use of the ICT services shall be either the financial entities in scope, either the ICT intra-group service providers.</p> <p>In case the register of information is maintained and updated at entity level, the entity signing the contractual arrangement and the entity making use of the ICT services are the financial entity maintaining the register.</p>

Template Code	Template Name	Short Description
RT.05.01	ICT third-party service providers	<p>Objective of this template is to list and provide general information to enable the identification of:</p> <ul style="list-style-type: none"> <li>(i) the direct ICT third-party service providers;</li> <li>(ii) the ICT intra-group service providers;</li> <li>(iii) all subcontractors included in template RT.05.02 on ICT service supply chain;</li> <li>(iv) and identify the ultimate parent undertaking of the ICT third-party service providers listed in points (i) to (iii) above.</li> </ul>
RT.05.02	ICT service supply chain	<p>Objective of this template is to identify and link one to another the ICT third-party service providers that are part of the same ICT service supply chain.</p> <p>Financial entities shall identify and rank the ICT thirdparty service providers for each ICT service included in the scope of each contractual arrangement.</p> <p>Example: a financial entity has a contractual arrangement with an ICT third-party service provider (say, ICT third-party service provider X) to receive 2 specific ICT services (say ICT service A and ICT service B) and the service provider makes use of a subcontractor (say, ICT third-party service provider Y) to provide one of these services (say ICT service B).</p> <ul style="list-style-type: none"> <li>▪ In relation to ICT service A, the ICT service supply chain is composed by one ICT third-party service provider, ICT third-party service provider X, which will be given 'rank' 1 in the template. ICT thirdparty service provider X is the direct ICT thirdparty service provider.</li> <li>▪ In relation to ICT service B, the ICT service supply chain is composed by two ICT third-party service providers: <ul style="list-style-type: none"> <li>(i) ICT third-party service provider X, which will be given 'rank' 1 in the template. ICT third-party service provider X is the direct ICT third-party service provider.</li> <li>(ii) ICT third-party service provider Y, which will be given 'rank' 2 in the template. ICT third-party service provider Y is a subcontractor.</li> </ul> </li> </ul> <p>All ICT third-party service providers belonging to the same ICT service supply chain share the same 'contractual arrangement reference number' as referred to in template RT.02.01 and the same type of ICT services</p>
RT.06.01	Functions identification	<p>Objective of this template is to identify and provide information on the functions of the financial entity making use of the ICT services.</p> <p>Within the information to be provided within this template, financial entities shall include a unique identifier, the 'function</p>

Template Code	Template Name	Short Description
		<p>identifier’ for each combination of a financial entity’s LEI, licenced activity and function.</p> <p>Example: a financial entity (LEI: 21USLEIC20231109J3Z8) which operates under two licensed activities (say, activity A and activity B) will identify two unique ‘function identifiers’ for the same function X (e.g. Sales) performed for activity A and activity B. The function identifier will be:</p> <p>F1 for the combination of “21USLEIC20231109J3Z8” “Activity A” and ‘Function X”</p> <p>F2 for the combination of “21USLEIC20231109J3Z8” “Activity B” and ‘Function X”</p>
RT.07.01	Assessments of the ICT services	Objective of this template is to capture information in relation to the risk assessment on the ICT services (e.g. substitutability, date of last audit, etc.) when the latter are supporting a critical or important function or material part thereof
RT.99.01	Definitions from Entities making use of the ICT Services	<p>Objective of this template is to capture entity-internal explanations, meanings and definitions of the closed set of indicators used in the register of information.</p> <p>For example, in template RT.07.01 financial entity shall provide an indication of the impact of discontinuation of the ICT services by using a closed set of options (low medium, high). In template RT99.01 the financial entity needs to specify the meaning of those options.</p>

**Part 2****Template-specific instructions****1. Instructions to complete template RT.01.01 — Entity maintaining the register of information**

Identify the entity maintaining and updating the register of information.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.01.01.0010	LEI of the entity maintaining the register of information	Alphanumerical	Identify the entity maintaining and updating the register of information using the LEI, 20-character, alpha-numeric code based on the ISO 17442 standard	Mandatory
RT.01.01.0020	Name of the entity	Alphanumerical	Legal name of the entity maintaining and updating the register of information	Mandatory
RT.01.01.0030	Country of the entity	Country	Identify the ISO 3166–1 alpha–2 code of the country where the license or the registration of the entity reported in the Register on Information has been issued.	Mandatory
RT.01.01.0040	Type of entity	Closed set of options	Identify the type of entity using one of the options in the following closed list: <ul style="list-style-type: none"> <li>1. credit institutions;</li> <li>2. payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;</li> <li>3. account information service providers;</li> <li>4. electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;</li> <li>5. investment firms;</li> <li>6. crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in cryptoassets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of assetreferenced tokens;</li> </ul>	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			7. central securities depositories; 8. central counterparties; 9. trading venues; 10. trade repositories; 11. managers of alternative investment funds; 12. management companies; 13. data reporting service providers; 14. insurance and reinsurance undertakings; 15. insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; 16. institutions for occupational retirement provision; 17. credit rating agencies; 18. administrators of critical benchmarks; 19. crowdfunding service providers; 20. securitisation repositories. 21. Other financial entity 22. Non-financial entity: ICT intra-group service provider 23. Non-financial entity: Other	
<b>RT.01.01.0050</b>	<b>Competent Authority</b>	Alphanumerical	Identify the competent authority according to Article 46 of Regulation (EU) 2022/2554 to which the register of information is reported.	Mandatory in case of reporting
<b>RT.01.01.0060</b>	<b>Date of the reporting</b>	Date	Identify the ISO 8601 (yyyy-mm-dd) code of the date of reporting	Mandatory in case of reporting

## 2. Instructions to complete template RT.01.02 —List of entities within the scope of the register of information

In case the register of information is maintained and updated at sub-consolidated and consolidated level, this template identifies all the entities belonging to the sub-group and group. In case the financial entity responsible for maintaining and updating the register of information does not belong to a group, only this financial entity shall be reported in this template and the entry of this template shall be the same as template RT.01.01.

In case a financial entity or a management entity acting on behalf of the financial entity outsources all its operational activities to a service provider, the ICT third-party service providers of the financial entity or of the management entity shall be recorded as the ICT third-party service providers of the financial entity. In this case, both, the financial entity or the management entity and the service provider shall be reported in this template.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.01.02.0010	LEI of the entity	Alphanumerical	Identify the entity reported in the Register on Information using the LEI, 20-character, alpha-numeric code based on the ISO 17442 standard	Mandatory
RT.01.02.0020	Name of the entity	Alphanumerical	Legal name of the entity reported in the register of information.	Mandatory
RT.01.02.0030	Country of the entity	Country	Identify the ISO 3166–1 alpha–2 code of the country where the license or the registration of the entity reported in the Register on Information has been issued.	Mandatory
RT.01.02.0040	Type of entity	Closed set of options	Identify the type of entity using one of the options in the following closed list: <ol style="list-style-type: none"> <li>1. credit institutions;</li> <li>2. payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;</li> <li>3. account information service providers;</li> <li>4. electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;</li> <li>5. investment firms;</li> <li>6. crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in cryptoassets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of assetreferenced tokens;</li> </ol>	Mandatory

APPENDIX VI: DRAFT IMPLEMENTING TECHNICAL STANDARDS

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			7. central securities depositories; 8. central counterparties; 9. trading venues; 10. trade repositories; 11. managers of alternative investment funds; 12. management companies; 13. data reporting service providers; 14. insurance and reinsurance undertakings; 15. insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; 16. institutions for occupational retirement provision; 17. credit rating agencies; 18. administrators of critical benchmarks; 19. crowdfunding service providers; 20. securitisation repositories. 21. Other financial entity 22. Non-financial entity: ICT intra-group service provider 23. Non-financial entity: Other	
<b>RT.01.02.0050</b>	<b>Hierarchy of the entity within the group (where applicable)</b>	Closed set of options	Identify the hierarchy of the entity within the scope of consolidation using one of the options in the following closed list:  1. The entity is the ultimate parent undertaking of the scope of consolidation; 2. The entity is the parent undertaking of a sub-consolidated part of the scope of consolidation; 3. The entity is a subsidiary within the scope of consolidation and is not a parent undertaking of a sub-consolidated part; 4. The entity is not part of a group; 5. The entity is a service provider to which the financial entity (or the management entity acting on its behalf) is outsourcing all its operational activities.	Mandatory



Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.01.02.0060	LEI of the direct parent undertaking of the entity	Alphanumerical	Identify the direct parent undertaking of the entity reported in the Register on Information using the LEI, 20-character, alpha-numeric code based on the ISO 17442 standard	Mandatory
RT.01.02.0070	Date of last update	Date	Identify the ISO 8601 (yyyy-mm-dd) code of the date of the last update made on the Register of information in relation to the entity.	Mandatory
RT.01.02.0080	Date of integration in the Register of information	Date	Identify the ISO 8601 (yyyy-mm-dd) code of the date of integration in the Register of information	Mandatory
RT.01.02.0090	Date of deletion in the Register of information	Date	Identify the ISO 8601 (yyyy-mm-dd) code of the date of deletion in the Register of information. If the entity has not been deleted, '9999-12-31' shall be reported	Mandatory
RT.01.02.0100	Currency	Currency	Identify the ISO 4217 alphabetic code of the currency used for the preparation of the financial entity's financial statements	Mandatory
RT.01.02.0110	Value of total assets - of the financial entity	Monetary	Monetary value of total assets of the entity making use of the ICT services as reported in the entity's annual financial statement of the year before the date of the last update of the register of information.  Refer to Annex IV for the approach to be followed when filling in this column.	Mandatory if the entity is a financial entity

**3. Instructions to complete template RT.01.03 — List of branches**

In case a financial entity has branches located outside its home country, identify those branches through this template.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.01.03.0010	Identification code of the branch	Alphanumerical	<p>Identify a branch of a financial entity located outside its home country using a unique code for each branch. One of the options in the following closed list shall be used:</p> <ul style="list-style-type: none"> <li>- LEI of the branch if unique for this branch and different from RT.01.03.0020;</li> <li>- Other identification code used by the financial entity to identify the branch (if the LEI of the branch is equivalent to the one in RT.01.03.0020 or equivalent to the LEI of another branch).</li> </ul>	Mandatory
RT.01.03.0020	LEI of the financial entity head office of the branch	Alphanumerical	<p><b>As referred to in RT.01.02.0010</b></p> <p>Identify the financial entity head office of the branch, using the LEI, 20-character, alphanumeric code based on the ISO 17442 standard</p>	Mandatory
RT.01.03.0030	Name of the branch	Alphanumerical	Identify the name of the branch	Mandatory
RT.01.03.0040	Country of the branch	Country	Identify the ISO 3166–1 alpha–2 code of the country where the branch is located.	Mandatory

#### 4. Instructions to complete template RT.02.01 — Contractual arrangements – General Information

Financial entities shall identify a ‘contractual arrangement reference number’ in relation to each contractual arrangement in scope of the register of information. In case the ICT third-party service provider is making use of subcontractors, financial entities shall not include in the register of information a ‘contractual arrangement reference number’ for the arrangements between the ICT third-party service providers and their subcontractors.

The ‘contractual arrangement reference number’ shall refer to the following type of contractual arrangements:

- i. any kind of standalone arrangements.
- ii. any kind of ‘overarching or framework arrangements’ such as master and framework arrangements;
- iii. any kind of ‘subsequent or associated arrangements’ such as implementing arrangements, subservice arrangements, amendments, order forms;

The contract reference number does not refer to any kind of service level agreement subordinated to any of the above-mentioned types of contractual arrangements.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.02.01.0010	<b>Contractual arrangement reference number</b>	Alphanumerical	<p>Identify the contractual arrangement between the financial entity or, in case of a group, the group subsidiary and the direct ICT third-party service provider.</p> <p>The contractual arrangement reference number is the internal reference number of the contractual arrangement assigned by the financial entity.</p> <p>The contractual arrangement reference number shall be unique and consistent over time at entity, sub-consolidated and consolidated level, where applicable.</p> <p>The contractual arrangement reference number shall be used consistently across all templates of the register of information when referring to the same contractual arrangement.</p>	Mandatory
RT.02.01.0020	<b>Type of contractual arrangement</b>	Closed set of options	<p>Identify the type of contractual arrangement by using one of the options in the following closed list:</p> <ol style="list-style-type: none"> <li>1. Standalone arrangement</li> <li>2. Overarching arrangement</li> <li>3. Subsequent or associated arrangement</li> </ol>	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.02.01.0030	<b>Overarching contractual arrangement reference number</b>	Alphanumerical	Not applicable if the contractual arrangement is the 'overarching contractual arrangement' or a 'standalone arrangement'. In the other cases, report the contractual arrangement reference number of the overarching arrangement, which shall be equal to value as reported in the column RT.02.01.0010 when reporting the overarching contractual arrangement.	Mandatory
RT.02.01.0040	<b>Currency of the amount reported in RT.02.01.0050</b>	Currency	Identify the ISO 4217 alphabetic code of the currency used to express the amount in RT.02.01.0050	Mandatory
RT.02.01.0050	<b>Annual expense or estimated cost of the contractual arrangement for the past year</b>	Monetary	<p>Annual expense or estimated cost (or intragroup transfer) of the ICT service arrangement for the past year.</p> <p>The annual expense or estimated cost shall be expressed in the currency reported in RT.01.02.0040.</p> <p>In case of an overarching arrangement with subsequent or associated arrangements, the sum of the annual expenses or estimated costs reported for the overarching arrangement and the subsequent or associated arrangements shall be equal to the total expenses or estimated costs for the overall contractual arrangement. This means, there should be no repetition or duplication of annual expenses or estimated costs. The following cases should be reflected:</p> <p>(a) if the annual expenses or estimate costs are not determined at the level of the overarching arrangement (i.e. they are 0), the annual expenses or estimated costs should be reported at the level of each subsequent or associated arrangements.</p> <p>(b) if the annual expenses or estimated costs cannot be reported for each of the subsequent or associated arrangements, the total annual expense or estimated cost should be reported at the level of the overarching arrangement.</p> <p>(c) if there are annual expenses or estimated costs related to each level of the arrangement, i.e. overarching and subsequent or associated, and this information is available, the annual expenses or estimated costs shall be reported without duplication at each level of the contractual arrangement</p>	Mandatory

### 5. Instructions to complete template RT.02.02 — Contractual arrangements – Specific information

Financial entities shall maintain this template at the maximum level of granularity possible. In order to do so, in case the contractual arrangement includes multiple ICT services supporting multiple functions, use as many rows as the elements in the matrix resulting combining the ICT services covered in the contractual arrangement and the financial entity's functions.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.02.02.0010	Contractual arrangement reference number	Alphanumerical	As reported in RT.02.01.0010	Mandatory
RT.02.02.0020	LEI of the entity making use of the ICT service(s)	Alphanumerical	As reported in RT.04.01.0020 Identify the entity making use of the ICT service(s) using the LEI, 20- character, alphanumeric code based on the ISO 17442 standard	Mandatory
RT.02.02.0030	Identification code of the ICT thirdparty service provider	Alphanumerical	As reported in RT.05.01.0010 Code to identify the ICT third-party service provider	Mandatory
RT.02.02.0040	Type of code to identify the ICT third-party service provider	Pattern	As reported in RT.05.01.0020 Identify the type of code to identify the ICT third-party service provider in RT.02.02.0030  1. 'LEI' for LEI 2. 'Country Code'+Underscore+'Type of Code' for non LEI code  Country Code: Identify the ISO 3166-1 alpha-2 code of the country of issuance of the other code to identify the ICT third-party service provider Type of Code:  1. CRN for Corporate registration number 2. VAT for VAT number 3. PNR for Passport Number	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			4. NIN for National Identity Number	
RT.02.02.0050	Function identifier	Pattern	As defined by the financial entity in RT.06.01.0010	Mandatory
RT.02.02.0060	Type of ICT services	Closed set of options	One of the types of ICT services referred to in Annex III	Mandatory
RT.02.02.0070	Start date of the contractual arrangement	Date	Identify the date of entry into force of the contractual arrangement as stipulated in the contractual arrangement using the ISO 8601 (yyyy–mm–dd) code	Mandatory
RT.02.02.0080	End date of the contractual arrangement	Date	Identify the end date as stipulated in the contractual arrangement using the ISO 8601 (yyyy–mm–dd) code. If the contractual arrangement is indefinite, it shall be filled in with '9999-12-31'. If the contractual arrangement has been terminated on a date different than the end date, this shall be filled in with the termination date. In case the contractual arrangement foresees a renewal, this shall be filled in with the date of the contract renewal as stipulated in the contractual arrangement.	Mandatory
RT.02.02.0090	Reason of the termination or ending of the contractual arrangement	Closed set of options	<p>In case the contractual arrangement has been terminated or it is ended, identify the reason of the termination or ending of the contractual arrangements using one of the options in the following closed list:</p> <ol style="list-style-type: none"> <li>1. Termination not for cause. The contractual arrangement has expired/ended and has not been renewed by any of the party;</li> <li>2. Termination for cause. The contractual arrangement has been terminated, being the ICT third-party service provider in a breach of applicable law, regulations or contractual provisions</li> <li>3. Termination for cause. The contractual arrangement has been terminated, due to impediments of the ICT third-party service provider capable of altering the supported function are identified;</li> </ol>	Mandatory if the contractual arrangement is terminated

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			<p>4. Termination for cause: The contractual arrangement has been terminated due to weaknesses of the ICT third-party provider regarding the management and security of sensitive data or information of any of the counterparty;</p> <p>5. Termination following a request by any Authority. The contractual arrangement has been terminated following a request by a Competent Authority.</p> <p>6. Other. The contractual arrangement has been terminated by any of the party for any reason different from the above.</p>	
<b>RT.02.02.0100</b>	<b>Notice period for the financial entity making use of the ICT service(s)</b>	Natural number	Identify the notice period for terminating the contractual arrangement by the financial entity in a business-as-usual case. The notice period shall be expressed as number of calendar days from the receipt of the counterparty of the request to terminate the ICT service.	Mandatory if the ICT service is supporting a critical or important function
<b>RT.02.02.0110</b>	<b>Notice period for the ICT third-party service provider</b>	Natural number	Identify the notice period for terminating contractual arrangement by the direct ICT third-party service provider in a business-as-usual case. The notice period shall be expressed as number of calendar days from the receipt of the counterparty of the request to terminate the ICT service.	Mandatory if the ICT service is supporting a critical or important function
<b>RT.02.02.0120</b>	<b>Country of the governing law of the contractual arrangement</b>	Country	Identify the country of the governing law of the contractual arrangement using the ISO 3166-1 alpha-2 code.	Mandatory if the ICT service is supporting a critical or important function

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.02.02.0130	Country of provision of the ICT services	Country	Identify the country of provision of the ICT services using the ISO 3166– 1 alpha–2 code.	Mandatory if the ICT service is supporting a critical or important function
RT.02.02.0140	Storage of data	[Yes/No]	Is the ICT service related to (or foresees) storage of data?  One of the options provided in the following closed list:  1. Yes 2. No	Mandatory if the ICT service is supporting a critical or important function
RT.02.02.0150	Location of the data at rest (storage)	Country	Identify the country of location of the data at rest (storage) using the ISO 3166–1 alpha–2 code.	Mandatory if 'Yes' is reported in RT.02.02.0140
RT.02.02.0160	Location of management of the data (processing)	Country	Identify the country of location of management of the data (processing) using the ISO 3166–1 alpha–2 code.	Mandatory if the ICT service is based on or foresees data processing
RT.02.02.0170	Sensitiveness of the data stored by the ICT third-party service provider	Closed set of options	Identify the level of sensitiveness of the data stored or processed by the ICT third-party service provider using one of the options provided in the following closed list:  1. Low or Medium 2. High	Mandatory if the ICT thirdparty service provider stores data and if the ICT service is



Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			The most sensitive data take precedence: e.g. if both 'Medium' and 'High' apply, then 'High' shall be selected.	supporting a critical or important function or material part thereof
<b>RT.02.02.0180</b>	<b>Level of reliance on the ICT service supporting the critical or important function.</b>	Closed set of options	<p>One of the options in the following closed list shall be used:</p> <ol style="list-style-type: none"> <li>1. Not significant</li> <li>2. Low reliance: in case of disruption of the services, the supported functions would not be significantly impacted (no interruption, no important damage) or disruption can be resolved quickly and with minimal impact on the function/s supported</li> <li>3. Material reliance: in case of disruption of the services, the supported functions would be significantly impacted if the disruption lasts more than few minutes/few hours, and the disruption may engender damages, but still manageable</li> <li>4. Full reliance: in case of disruption of the services, the supported functions would be immediately and severely interrupted/damaged, for a long period</li> </ol>	Mandatory if the ICT service is supporting a critical or important function or material part thereof

**6. Instructions to complete template RT.02.03 — List of intra-group contractual arrangements**

Template RT.02.03 aims at identifying contractual arrangements from the same ICT service supply chain using the intra-group contractual reference numbers in cases where the ICT service supply chain contains ICT intra-group service providers, i.e. when in case at least one of the ICT third-party service provider in the ICT service supply chain is an entity belonging to the same group of the entity making use of the ICT services.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.02.03.0010	<b>Contractual arrangement reference number</b>	Alphanumerical	Contractual arrangement reference number between the entity making use of the ICT service(s) provided and the ICT intra-group service provider.  The contractual arrangement reference number shall be unique and consistent over time and across all the group.	Mandatory
RT.02.03.0020	<b>Contractual arrangement linked to the contractual arrangement referred in RT.02.03.0010</b>	Alphanumerical	Contractual arrangement reference number of the contractual arrangement between the ICT intra-group service provider of the contractual arrangement in RT.02.03.0010 and its direct ICT third-party service provider	Mandatory

### 7. Instructions to complete template RT.03.01 — Entities signing the Contractual arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)

Identify all the entities referred to in template RT.01.02 signing the contractual arrangements referred to in template RT.02.01 for receiving the ICT services. In case the register of information is maintained and updated at entity level the entity signing the contractual arrangements is the financial entity maintaining and updating the register of information itself.

The entity signing the contractual arrangement is not necessarily a financial entity nor the entity making use of the ICT services provided by the ICT third-party service provider.

For example, the entity signing the contractual arrangement referred above could be an ICT intra-group service provider, a financial and/or non-financial entity belonging to the same group of the financial entities making use of the ICT services provided by the ICT third-party service provider.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.03.01.0010	Contractual arrangement reference number	Alphanumerical	<p><b>As reported in RT.02.02.0010</b></p> <p>Identify the contractual reference number signed by the entity</p>	Mandatory
RT.03.01.0020	LEI of the entity signing the contractual arrangement	Alphanumerical	Identify the entity signing the contractual arrangement using the LEI, 20-character, alpha-numeric code based on the ISO 17442 standard	Mandatory

**8. Instructions to complete template RT.03.02 — ICT third-party service providers signing the Contractual arrangements for providing ICT service(s)**

Identify all the ICT third-party service providers referred to in template RT.05.01 signing the contractual arrangements referred to in template RT.02.01 for providing the ICT services.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.03.02.0010	Contractual arrangement reference number	Alphanumerical	<p><b>As reported in RT.02.02.0010</b></p> <p>Identify the contractual arrangement reference number signed by the ICT third-party service provider</p>	Mandatory
RT.03.02.0020	Identification code of ICT third-party service provider	Alphanumerical	<p><b>As reported in RT.05.01.0010</b></p> <p>Code to identify the ICT third-party service provider</p>	Mandatory
RT.03.02.0030	Type of code to identify the ICT third-party service provider	Pattern	<p><b>As reported in RT.05.01.0020</b></p> <p>Identify the type of code to identify the ICT third-party service provider in RT.03.02.0020</p> <p>1. 'LEI' for LEI 2. 'Country Code'+Underscore+'Type of Code' for non LEI code</p> <p>Country Code: Identify the ISO 3166–1 alpha–2 code of the country of issuance of the other code to identify the ICT third-party service provider</p> <p>Type of Code:</p> <p>1. CRN for Corporate registration number 2. VAT for VAT number 3. PNR for Passport Number 4. NIN for National Identity Number</p>	Mandatory

**9. Instructions to complete template RT.03.03 — Entities signing the Contractual arrangements for providing ICT service(s) to other entity within the scope of consolidation.**

Identify all the entities referred to in template RT.01.02 signing the contractual arrangements referred to in template RT.02.01 for providing the ICT services to other entities in the scope of consolidation referred to in template RT.01.02.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.03.03.0010	Contractual arrangement reference number	Alphanumerical	<p><b>As reported in RT.02.02.0010</b></p> <p>Identify the contractual reference number signed by the entity for providing ICT service(s)</p>	Mandatory
RT.03.03.0020	LEI of the entity providing ICT services	Alphanumerical	<p><b>As reported in RT.01.02.0010</b></p> <p>Identify the entity providing ICT services using LEI, 20-character, alpha-numeric code based on the ISO 17442 standard</p>	Mandatory

**10. Instructions to complete template RT.04.01 —Entities making use of the ICT services**

All the entities referred to in template RT.01.02 and branches of financial entity referred in template RT.01.03 making use of the ICT services provided by ICT third-party shall be reported in this template.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.04.01.0010	<b>Contractual arrangement reference number</b>	Alphanumerical	<b>As reported in RT.02.01.0010</b>  Identify the contractual reference number in relation to the entity making use of the ICT services provided	Mandatory
RT.04.01.0020	<b>LEI of the entity making use of the ICT service(s)</b>	Alphanumerical	Identify the entity making use of the ICT service(s) using the LEI, 20-character,	Mandatory
RT.04.01.0030	<b>Nature of the entity making use of the ICT service(s)</b>	Closed set of options	One of the options in the following closed list shall be used:  1. The entity making use of the ICT service(s) is a branch of a financial entity 2. The entity making use of the ICT service(s) is not a branch	Mandatory
RT.04.01.0040	<b>Identification code of the branch</b>	Alphanumerical	Identification code of the branch as reported in RT.01.03.0010	Mandatory if the entity making use of the ICT service(s) is a branch of a financial entity (RT.04.01.0030)

**11. Instructions to complete template RT.05.01 — ICT third-party service provider**

This template aims at identifying all the relevant ICT third-party service providers:

- all the direct ICT third-party providers;
- the ICT intra-group service provider;
- the subcontractors reported in template RT.05.02 on the ICT service supply chain (in line with Article 3);
- and identify the ultimate parent undertaking of the ICT third-party service providers listed in the three points above.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.05.01.0010	Identification code of ICT third-party service provider	Alphanumerical	Code to identify the ICT third-party service provider	Mandatory
RT.05.01.0020	Type of code to identify the ICT thirdparty service provider	Pattern	<p>Identify the type of code to identify the ICT third-party service provider in RT.05.01.0010</p> <p>1. 'LEI' for LEI 2. 'Country Code'+Underscore+'Type of Code' for non LEI code</p> <p>Country Code: Identify the ISO 3166–1 alpha–2 code of the country of issuance of the other code to identify the ICT thirdparty service provider</p> <p>Type of Code: 1. CRN for Corporate registration number 2. VAT for VAT number 3. PNR for Passport Number 4. NIN for National Identity Number</p>	Mandatory
RT.05.01.0030	Name of the ICT third-party service provider	Alphanumerical	Legal name of the ICT third-party service provider	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.05.01.0040	Type of person of the ICT thirdparty service provider	Closed set of options	One of the options in the following closed list shall be used:  1. Legal person 2. Individual acting in a business capacity  Providing the LEI is mandatory for legal person including natural persons acting in a business capacity	Mandatory
RT.05.01.0050	Country of the ICT thirdparty service provider's headquarters	Country	Identify the ISO 3166–1 alpha–2 code of the country in which the global operating headquarters of ICT third-party service provider are located.	Mandatory
RT.05.01.0060	Currency of the amount reported in RT.05.01.0070	Currency	Identify the ISO 4217 alphabetic code of the currency used to express the amount in RT.05.01.0070	Mandatory if RT.05.01.0070 is reported
RT.05.01.0070	Total annual expense or estimated cost of the ICT third-party service provider	Monetary	Annual expense or estimated cost for using the ICT services provided by the ICT third-party service provider to the entities making use of the ICT services	Mandatory if the ICT third-party service provider is a direct ICT third-party service provider
RT.05.01.0080	Identification code of the ICT thirdparty service provider's ultimate parent undertaking	Alphanumerical	Code to identify the ICT third-party service provider's ultimate parent undertaking	Mandatory if the ICT third-party service provider is not the ultimate



Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
				parent undertaking
RT.05.01.0090	Type of code to identify the ICT thirdparty service provider's ultimate parent undertaking	Pattern	<p>Identify the type of code to identify the ICT third-party service provider's ultimate parent undertaking in RT.05.01.0080</p> <ol style="list-style-type: none"> <li>'LEI' for LEI</li> <li>'Country Code'+Underscore+'Type of Code' for non LEI code</li> </ol> <p>Country Code: Identify the ISO 3166–1 alpha–2 code of the country of issuance of the other code to identify the ICT thirdparty service provider</p> <p>Type of Code:</p> <ol style="list-style-type: none"> <li>CRN for Corporate registration number</li> <li>VAT for VAT number</li> <li>PNR for Passport Number</li> <li>NIN for National Identity Number</li> </ol>	Mandatory if the ICT third-party service provider is not the ultimate parent undertaking

## 12. Instructions to complete template RT.05.02 — ICT service supply chains

This template aims at identifying and linking one to each other the ICT third-party service providers part of the same ICT service supply chain.

In line with Article 3, the ICT service supply chain shall include, where applicable:

- (i) all ICT direct ICT third-party service providers;
- (ii) all ICT intragroup service providers;
- (iii) in relation to the ICT services supporting a critical or important function or material part thereof, the register of information includes all subcontractors that effectively underpin the provision of these ICT services (i.e. all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision);
- (iv) in case an ICT intragroup service provider makes use of subcontractors to provide their ICT services to the financial entity, at least the first extra-group subcontractor even if the ICT services provided do not support a critical or important function or material part thereof.

All ICT third-party service providers belonging to the same ICT service supply chain share:

- (i) the same 'contractual arrangement reference number' as referred to in template RT.02.01;
- (ii) the same 'type of ICT services' as referred to in Annex III;

Each ICT third-party service providers belonging to the same ICT service supply is assigned with a 'rank' (RT.05.02.0050) to identify its position within the ICT service supply chain. In case multiple ICT third-party service providers have the same position within the same ICT service supply chain, they will be assigned with the same 'rank'. The direct ICT third-party service providers are therefore at rank 1. If the rank is higher than 1, the ICT third-party service providers are subcontractors.

In order to link one to each other the ICT third-party service providers belonging to the same ICT service supply chain, for each ICT subcontractor (i.e. where the 'rank' is higher than 1) it is needed to identify the ICT third-party service provider recipient of its subcontracted services. The identification of the ICT third-party service provider recipient of subcontracted services shall be carried out by using the columns RT.05.02.0060 and RT.05.02.0070.

For each ICT service supply chain (i.e., a combination of a "contractual arrangement reference number" and a "type of ICT services"), if there are multiple ICT third-party service providers receiving subcontracted services, all of these service providers shall be reported in separate rows in the template. The same logic applies at each rank of the ICT service supply chain.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.05.02.0010	Contractual arrangement reference number	Alphanumerical	As reported in RT.02.01.0010	Mandatory
RT.05.02.0020	Type of ICT services	Closed set of options	One of the types of ICT services referred to in Annex III	Mandatory
RT.05.02.0030	Identification code of the ICT third-party service provider	Alphanumerical	As reported in RT.05.01.0010	Mandatory
RT.05.02.0040	Type of code to identify the ICT third-party service provider	Pattern	As reported in RT.05.01.0020	Mandatory
RT.05.02.0050	Rank	Natural number	<p>If the ICT third-party service provider is signing the contractual arrangement with the financial entity, it is considered as a direct ICT third-party service provider and the 'rank' to be reported shall be 1;</p> <p>If the ICT third-party service provider is signing the contract with the direct ICT third-party service provider, it is considered as a subcontractor and the 'rank' to be reported shall be 2;</p> <p>The same logic apply to all the following subcontractors by incrementing the 'rank'.</p> <p>In case multiple ICT third-party service providers have the same 'rank' in the ICT service supply chain, financial entities shall report the same 'rank' for all those ICT third-party service providers.</p>	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.05.02.0060	Identification code of the recipient of sub-contracted ICT services	Alphanumerical	<p>‘Not applicable’ if the ICT third-party service provider RT.05.02.0030) is a direct ICT third-party service provider i.e. at ‘rank’ r = 1 (RT.05.02.0050);</p> <p>If the ICT third-party service provider is at ‘rank’ r = n where n&gt;1, indicate the ‘Identification code of the recipient of sub-contracted services’ at ‘rank’ r=n-1 that subcontracted the ICT service (even partially) to the ICT third-party service provider at ‘rank’ r=n</p>	Mandatory Not applicable for rank 1
RT.05.02.0070	Type of code to identify the recipient of subcontracted ICT services	Pattern	<p>‘Not applicable’ if the ICT third-party service provider RT.05.02.0030) is at contracting rank r = 1 (RT.05.02.0050);</p> <p>If the ICT third-party service provider is at ‘rank’ r = n where n&gt;1, indicate the ‘Type of code to identify the recipient of sub-contracted service’ at ‘rank’ r=n-1 that subcontracted the ICT service (even partially) to the ICT third-party service provider at ‘rank’ r=n.</p> <p>1. ‘LEI’ for LEI 2. ‘Country Code’+Underscore+‘Type of Code’ for non LEI code</p> <p>Country Code: Identify the ISO 3166–1 alpha–2 code of the country of issuance of the other code to identify the ICT third-party service provider</p> <p>Type of Code: 1. CRN for Corporate registration number 2. VAT for VAT number 3. PNR for Passport Number 4. NIN for National Identity Number</p>	Mandatory Not applicable for rank 1

**13. Instructions to complete template RT.06.01 — Functions identification**

This template aims at identifying and providing information on the functions of the financial entity according to the financial entity's internal organisation. Only functions supported by an ICT service provided by ICT third-party providers shall be reported.

Each combination of the three following items shall have a unique function identifier assigned:

- i. 'LEI of the financial entity making use of the ICT service(s)' column RT.06.01.0040
- ii. 'Licenced activity' column RT.06.01.0020
- iii. 'Function name' column RT.06.01.0030

Financial entities shall use as many rows as the elements in the matrix resulting combining the two items above to fill-in this template.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.06.01.0010	Function Identifier	Pattern	<p>The function identifier shall be composed by the letter F (capital letter) followed by an natural number (e.g. "F1" for the 1st function identifier and "Fn" for the nth function identifier with "n" being an natural number).</p> <p>Each combination between 'LEI of the financial entity making use of the ICT service(s)' (RT.06.01.0040), 'Function name' (RT.06.01.0030) and 'Licenced activity' (RT.06.01.0020) shall have a unique function identifier</p> <p>Example: a financial entity which operates under two licensed activities (say, activity A and activity B) will identify two unique 'function identifiers' for the same function X (e.g. Sales) performed for activity A and activity B.</p>	Mandatory
RT.06.01.0020	Licenced activity	Closed set of options	One of the licenced activities referred to in Annex II for the different type of financial entities. In case the function is not linked to a registered or licenced activity, 'support functions' shall be reported.	Mandatory
RT.06.01.0030	Function name	Alphanumerical	Function name according to the financial entity's internal organisation	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.06.01.0040	LEI of the financial entity	Alphanumerical	<p><b>As reported in RT.04.01.0020</b></p> <p>Identify the financial entity using the LEI, 20-character, alphanumeric code based on the ISO 17442 standard</p>	Mandatory
RT.06.01.0060	Criticality or importance assessment	Closed set of options	<p>Use this column to indicate whether the function is critical or important according to the financial entity's assessment. One of the options in the following closed list shall be used:</p> <ol style="list-style-type: none"> <li>1. Yes</li> <li>2. No</li> <li>3. Assessment not performed</li> </ol>	Mandatory
RT.06.01.0070	Reasons for criticality or importance	Alphanumerical	Brief explanation on the reasons to classify the function as critical or important (300 characters maximum)	Optional
RT.06.01.0080	Date of the last assessment of criticality or importance	Date	<p>Identify the ISO 8601 (yyyy-mm-dd) code of the date of the last assessment of criticality or importance in case the function is supported by ICT services provided by ICT third-party service providers.</p> <p>In case the function's assessment of criticality or importance is not performed, it shall be filled in with '9999-12-31'</p>	Mandatory
RT.06.01.0090	Recovery time objective of the function	Natural number	In number of hours. If the recovery time objective is less than 1 hour, '1' shall be reported. In case the recovery time objective of the function is not defined '0' shall be reported	Mandatory
RT.06.01.0100	Recovery point objective of the function	Natural number	In number of hours. If the recovery point objective is less than 1 hour, '1' shall be reported. In case the recovery time objective of the function is not defined '0' shall be reported.	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.06.01.0110	Impact of discontinuing the function	Closed set of options	Use this column to indicate the impact of discontinuing the function according to the financial entity's assessment. One of the options in the following closed list shall be used  <ol style="list-style-type: none"><li>1. Low or Medium</li><li>2. High</li><li>3. Assessment not performed</li></ol>	Mandatory

**14. Instructions to complete template RT.07.01 — Assessment of the ICT services**

When supporting a critical or important function or material part thereof, this template aims at further assessing the ICT services provided by ICT thirdparty service providers, including the first extra-group subcontractor in the ICT service supply chain when the prior ICT third-party service providers are intra-group, to the financial entity.

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.07.01.0010	Contractual arrangement reference number	Alphanumerical	As reported in RT.02.01.0010	Mandatory
RT.07.01.0020	Identification code of the ICT thirdparty service provider	Alphanumerical	As reported in RT.05.01.0010	Mandatory
RT.07.01.0030	Type of code to identify the ICT thirdparty service provider	Pattern	As reported in RT.05.01.0020	Mandatory
RT.07.01.0040	Type of ICT services	Closed set of options	One of the types of ICT services referred to in Annex III	Mandatory
RT.07.01.0050	Substitutability of the ICT third-party service provider	Closed set of options	<p>Use this column to provide the results of the financial entity’s assessment in relation to the degree of substitutability of the ICT third-party service provider to perform the specific ICT services supporting a critical or important function.</p> <p>One of the options in the following closed list shall be used:</p> <ol style="list-style-type: none"> <li>1. Not substitutable</li> <li>2. Highly complex substitutability</li> <li>3. Medium complexity in terms of substitutability</li> <li>4. Easily substitutable</li> </ol>	Mandatory



Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
RT.07.01.0060	<b>Reason if the ICT thirdparty service provider is considered not substitutable or difficult to be substitutable</b>	Closed set of options	<p>One of the options in the following closed list shall be used:</p> <ol style="list-style-type: none"> <li>1. The lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider’s organisation or activity.</li> <li>2. Difficulties in relation to partially or fully migrating the relevant data and workloads from the relevant ICT third- party service provider to another ICT third-party service provider or to reintegrate them in the financial entity’s operations, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk or other operational risks to which the financial entity.</li> <li>3. Both abovementioned reasons</li> </ol>	Mandatory in case “not substitutable” or “highly complex substitutability” is selected in RT.07.01.0050
RT.07.01.0070	<b>Date of the last audit on the ICT thirdparty service provider</b>	Date	<p>Use this column to provide the date of the last audit on the specific ICT services provided by the ICT third-party service provider.</p> <p>This column relates to audits conducted by:</p> <ol style="list-style-type: none"> <li>(i) the internal audit department or any other additional qualified personnel of the financial entity,</li> <li>(ii) a joint team together with other clients of the same ICT third-party service provider (“pooled audit”) or</li> <li>(iii) a third party appointed by the supervised entity to audit the service provider.</li> </ol> <p>This column does not relate to the reception or reference date of third-party certifications or internal audit reports of the ICT thirdparty service provider, the annual monitoring date of the arrangement by the financial entity or the date of review of the risk assessment by the financial entity.</p> <p>This column shall be used to report all types of audits performed by any of the subjects listed above concerning fully or partially the ICT services provided by the ICT third-party service provider.</p>	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
			To report the date, the ISO 8601 (yyyy-mm-dd) code shall be used.  If no audit has been performed, it shall be filled in with '9999-12- 31'.	
RT.07.01.0080	Existence of an exit plan	[Yes/No]	Use this column to report the existence of an exit plan from the ICT third-party service provider in relation to the specific ICT service provided.  One of the options in the following closed list shall be used:  1. Yes 2. No	Mandatory
RT.07.01.0090	Possibility of reintegration of the contracted ICT service	Closed set of options	One of the options in the following closed list shall be used:  1. Easy 2. Difficult 3. Highly complex  In case the ICT service is provided by an ICT third-party service provider that is not an ICT intra-group service provider	Mandatory
RT.07.01.0100	Impact of discontinuing the ICT services	Closed set of options	Use this column to provide the impact for the financial entity of discontinuing the ICT services provided by the ICT third-party service provider according to the financial entity's assessment.  One of the options in the following closed list shall be used:  1. Low or medium 2. High 3. Assessment not performed	Mandatory
RT.07.01.0110	Are there alternative ICT thirdparty	Closed set of options	One of the options in the following closed list shall be used:  1. Yes	Mandatory

Column Code	Column Name	Type	Fill-in Instruction	Fill-in Option
	<b>service providers identified?</b>		2. No 3. Assessment not performed  In principle, for each ICT third-party service provider supporting a critical or important function, the assessment to identify an alternative service provider shall be performed.	
<b>RT.07.01.0120</b>	<b>Identification of alternative ICT TPP</b>	Alphanumerical	If 'Yes' is reported in <b>RT.07.01.0110</b> , <b>additional information could be provided in this column</b>	Optional

15. Instructions to complete template RT.99.01 — Definitions from Entities making use of the ICT Services

	RT.99.01.C0010	RT.99.01.C0020	RT.99.01.C0030	RT.99.01.C0040
	Column Code	Column Name	Option	Description/Internal definition of the option
RT.99.01.R0010	RT.02.01.0020	Type of contractual arrangement	1. Standalone arrangement	
RT.99.01.R0020			2. Overarching arrangement	
RT.99.01.R0030			3. Subsequent or associated arrangement	
RT.99.01.R0040	RT.02.02.0170	Sensitiveness of the data stored by the ICT third-party service provider	1. Low	
RT.99.01.R0050			2. Medium	
RT.99.01.R0060			3. High	
RT.99.01.R0070	RT.06.01.0110	Impact of discontinuing the function	1. Low	
RT.99.01.R0080			2. Medium	
RT.99.01.R0090			3. High	
RT.99.01.R0100	RT.07.01.0050	Substitutability of the ICT third-party service provider	1. Not substitutable	
RT.99.01.R0110			2. Highly complex substitutability	
RT.99.01.R0120			3. Medium complexity in terms of substitutability	
RT.99.01.R0130			4. Easily substitutable	
RT.99.01.R0140	RT.07.01.0090	Possibility of reintegration of the contracted ICT service	1. Easy	
RT.99.01.R0150			2. Difficult	
RT.99.01.R0160			3. Highly complex	
RT.99.01.R0170	RT.07.01.0100	Impact of discontinuing the ICT services	1. Low	
RT.99.01.R0180			2. Medium	
RT.99.01.R0190			3. High	

## Annex II

**List of activities by type of entity**

Type of entity	List of activities and services
(a) credit institutions	Activities listed in Annex I of Directive 2013/36/EU and activities listed in Section A and B of Annex I of Directive 2014/65/EU
(b) payment institutions, including exempted payment institutions pursuant to Directive (EU) 2015/2366	Activities listed in Annex I of Directive (EU) 2015/2366 of PSD2
(c) account information service providers	Account information services as referred to in point (8) of Annex I of PSD2
(d) electronic money institutions, including exempted electronic money institutions pursuant to Directive 2009/110/EC	Issuing electronic money in accordance with 2009/110/EC (EMD) and the activities listed in Annex I of PSD2
(e) investment firms	Investment services and activities listed in Section A and B of Annex I of Directive 2014/65/EU
(f)* crypto-asset service providers pursuant to Regulation (EU) 2023/1114	Services and activities listed in Article 3(16) of Regulation (EU) 2023/1114 (MiCAR)
(f)** issuers of asset-referenced tokens pursuant to Regulation (EU) 2023/1114	Activities mentioned in Article 16(1) of Regulation (EU) 2023/1114 (MiCAR)
(g) central securities depositories	Activities listed in Annex of Regulation (EU) No 909/2014 (CSDR)
(h) central counterparties	Activity of CCPs as described in Article 2(1) of Regulation (EU) No 648/2012 (EMIR)
(i) trading venues	Activity of trading venues as described in Article 2(4) of Regulation (EU) No 648/2012 (EMIR)
(j) trade repositories	Activities of trade repositories as described in Article 2(2) of Regulation EU No 648/2012 and in Article 3(1) of Regulation EU No 2015/2365
(k) managers of alternative investment funds	Activities listed in Article 6(4) + Annex I of Directive 2011/61/EU (AIFMD)
(l) management companies	Activities listed in Article 6(3) + Annex II of Directive 2009/65/EC (UCITD)
(m) data reporting service providers	Services referred to in Article 3(1)(34), (35) and (36) of Regulation (EU) 600/2014

Type of entity	List of activities and services
(n) insurance and reinsurance undertakings	Activities authorised for the classes of nonlife insurance as described in Annex I Section B of Directive 2009/138/EC and classes of life insurance as described in Annex II of Directive 2009/138/EC (Solvency II)
(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries	Activities of insurance and reinsurance distribution as described in Articles 2(1)(1) and 2(1)(2) of Directive (EU) 2016/97 (IDD)
(p) institutions for occupational retirement provision	Activities of IORPs as described in Article 7 of Directive (EU) 2016/2341 (IORP II)
(q) credit rating agencies	Activities of CRAs as described in Articles 2(1) and 3.1(a) and (b) of Regulation (EC) No 1060/2009
(r) administrators of critical benchmarks	Activity of administrators of benchmarks as defined in Article 3(1), (5) and (6) of Regulation (EU) 2016/1011, referred to the benchmarks defined in Article 3(1)(25) of the same Regulation
(s) crowdfunding service providers	Provision of crowdfunding services in accordance with Article 3 of Regulation (EU) 2020/1503
(t) securitisation repositories	Activity of SRs as described in Article 2(23) of Regulation (EU) 2017/2402
Non-financial entity: ICT intra-group service provider	Not applicable
Non-financial entity: Other intra-group entity	Not applicable
Non-financial entity: ICT third-party service provider	Not applicable

**Annex III****Type of ICT services**

When referring to a type of ICT services in the templates of the register of information, only the identifier (from S01 to S19) of the relevant type of ICT services shall be reported.

Identifier	Type of ICT services	Description
S01	1. ICT project management	Provision of services related to Project Management Officer (PMO).
S02	2. ICT Development	Provision of services related to: business analysis, software design and development, testing.
S03	3. ICT help desk and first level support	Provision of services related to: helpdesk support and first level support on ICT incident
S04	4. ICT security management services	Provision of services related to: ICT security (protection, detection, response and recovering), including security incident handling and forensics.
S05	5. Provision of data	Subscription to the services of data providers. (digital data service)
S06	6. Data analysis	Provision of services related to the support for data analysis. (digital data service)
S07	7. ICT, facilities and hosting services (excluding Cloud services)	Provision of ICT infrastructure, facilities and hosting services. This includes the provision of utilities (energy, heat management...), telecom access and physical security. (excluding Cloud services)
S08	8. Computation	Provision of digital processing capabilities (including data computation). This excludes the computation services performed in the context of a cloud environment.
S09	9. Non-Cloud Data storage	Provision of data storage platform (excluding Cloud services).
S10	10. Telecom carrier	Operations for telecommunication systems and flow management. Traditional analogue telephone services are explicitly excluded as per Article 3(21) of Regulation (EU) 2022/2554
S11	11. Network infrastructure	Provision of network infrastructure
S12	12. Hardware and physical devices	Provision of workstations, phones, servers, data storage devices, appliances, etc. in a form of a service

Identifier	Type of ICT services	Description
S13	13. Software licencing (excluding SaaS)	Provision of software run on premises.
S14	14. ICT operation management (including maintenance)	Provision of services related to: infrastructure (systems and hardware except network) configuration, maintenance, installing, capacity management, business continuity management, etc. Including Managed Service Providers (MSP)
S15	15. ICT Consulting	Provision of intellectual / ICT expertise services.
S16	16. ICT Risk management	Verification of compliance with ICT risk management requirements in accordance with Article 6(10) of Regulation (EU) 2022/2554
S17	17. Cloud services: IaaS	Infrastructure-as-a-Service
S18	18. Cloud services: PaaS	Platform-as-a-Service
S19	19. Cloud services: SaaS	Software-as-a-Service



**Annex IV****Instruction to report the “total value of assets”****Value of total assets**

Type of entity	Instruction to report value of total assets in column RT.01.02.0110
(a) credit institutions	Information as specified in Annex X, Template C40.00 Row 0410, Column 0010 of Commission Implementing Regulation (EU) 2021/451
(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366	Value of the total assets in the statutory accounts
(c) account information service providers	Value of the total assets in the statutory accounts
(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC	Value of the total assets in the statutory accounts
(e) investment firms	Information as specified in Annex I, template Z01.00, column 0090 of Commission Implementing Regulation (EU) 2018/1624
(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of assetreferenced tokens	Value of the total assets in the statutory accounts
(g) central securities depositories	Value of the total assets in the audited financial statements reported to CAs pursuant to article 41(a) Regulation (EU) 2017/392
(h) central counterparties	Information as reported in "Public quantitative disclosure standards for central counterparties" of BIS/IOSCO <sup>72</sup> , field 15.2
(i) trading venues	Value of the total assets in the statutory accounts
(j) trade repositories	Value of the total assets in the statutory accounts
(k) managers of alternative investment funds	Value of the total assets in the statutory accounts
(l) management companies	Value of the total assets in the statutory accounts

<sup>72</sup> <https://www.bis.org/cpmi/publ/d125.pdf>

Type of entity	Instruction to report value of total assets in column RT.01.02.0110
(m) data reporting service providers	Value of the total assets in the statutory accounts
(n) insurance and reinsurance undertakings	Information as specified in Annex II and Annex III, Template S02.01 Row 0500, Column 0010 of Commission Implementing Regulation (EU) 2015/2450
(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries	Value of the total assets in the statutory accounts
(p) institutions for occupational retirement provision	Information as specified in ECB guideline 2021/831 Annex 1 Part 4 Section 2
(q) credit rating agencies	Value of the total assets in the statutory accounts
(r) administrators of critical benchmarks	Value of the total assets in the statutory accounts
(s) crowdfunding service providers	Value of the total assets in the statutory accounts
(t) securitisation repositories	Value of the total assets in the statutory accounts
Non-financial entity: ICT intra-group service provider	Not applicable
Non-financial entity: Other intra-group entity	Not applicable
Non-financial entity: ICT third-party service provider	Not applicable

## APPENDIX VII: RTS and ITS on the content, format, templates and timelines for reporting major ICT-related incidents and significant cyber threats

[\(JC 2024 33 – 17 July 2024\)](#)

[Art. 20(a) and (b)]

**COMMISSION DELEGATED REGULATION (EU) .../...**

**of XXX**

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content of the reports and notifications for major ICT-related incidents and significant cyber threats and the time limits for reporting of these incidents

**(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, and in particular Article 20(a) third subparagraph thereof,

Whereas:

- (1) Given that Regulation (EU) 2022/2554 aims to harmonise and streamline incident reporting requirements, and to ensure that competent and other relevant authorities receive all necessary information about the major incident in order to take supervisory actions and to prevent potential spill-over effects, the reports for major incidents submitted from financial entities to competent authorities should provide essential and exhaustive information about the incident, in a consistent and standardised manner for all financial entities within the scope of Regulation (EU) 2022/2554.
- (2) With a view to ensure the harmonisation of the reporting requirements for major incidents and to maintain a consistent approach with Directive (EU) 2022/2555, the time limits for reporting major incidents should be consistent for all types of financial entities. The time limits should also be consistent with, to the greatest extent possible, and at least equivalent in effect to the requirements set out in Directive (EU) 2022/2555.
- (3) In order to take proper action, competent authorities need to receive information about the major incident at the very early stages after the incident has been classified as major. Consequently, the timeline for submitting the initial notification should be as short as possible after classification of the incident but also providing flexibility for financial entities, especially for non-time critical service business models, with a longer timeline after financial entities become aware of the incident in case financial entities require more time to handle the incident. To avoid imposing an undue reporting burden to the financial entity at a time when it will be handling with the incident, the content of such initial notification should be limited to the most significant information.
- (4) Given that, after having received the initial notification, competent authorities will need more detailed information about the incident with the intermediate report and the full set of relevant information with the final report to further assess the situation and evaluate supervisory actions they may want to take, the

reporting timelines should be such to allow competent authorities to receive the information timely, while ensuring financial entities have sufficient time to obtain complete and accurate information.

- (5) In accordance with the proportionality requirement set out in Article 20(a), second sub-paragraph of Regulation (EU) 2022/2554, the reporting timelines should not pose burden to microenterprises and other financial entities that are not significant. Therefore, the reporting timelines should take into account, in particular weekends and bank holidays.
- (6) Since significant cyber threats are to be reported on a voluntary basis, the requested information should not pose burden to financial entities to obtain and should be more limited than the information requested for major incidents.
- (7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities.
- (8) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the [...] Stakeholder Group established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010 and 1095/2010 of the European Parliament and of the Council<sup>73</sup>

HAS ADOPTED THIS REGULATION:

*Article 1*

**General provisions**

Financial entities shall provide the initial notification, the intermediate report or the final report with the content as set out in this Regulation following the description and instructions as set out in the Implementing Regulation [insert reference once published in OJ].

*Article 2*

**General information to be provided in the major incident initial notification, intermediate and final reports**

When submitting the initial notification, the intermediate report and the final report, financial entities shall provide the following general information:

- (a) the type of report as referred to in Article 19(4) of Regulation (EU)2022/2554;
- (b) name, LEI code of the financial entity and specify, which of the type of entities referred to in Article 2(1) of Regulation (EU)2022/2554 it is authorised or registered as;
- (c) name and identification code of the entity submitting the report for the financial entity;
- (d) names and LEI codes of all financial entities covered in the aggregated report, where applicable.
- (e) contact details of the contact persons responsible for communicating with the competent authority;
- (f) identification of the parent undertaking of the group, where applicable; and
- (g) reporting currency.

---

<sup>73</sup> Regulation (EU) No 109x/2010 of the European Parliament and of the Council ...[+full title] (OJ L [number], [date dd.mm.yyyy], [p. ]).

*Article 3*

**Content of initial notifications**

Financial entities shall provide at least the following information about the incident in the initial notification:

- (a) incident reference code
- (b) date and time of detection and classification of the incident;
- (c) description of the incident;
- (d) classification criteria that triggered the incident report as set out in [Articles 1 to 8 of Delegated Regulation [insert number once published in official journal]];
- (e) members States impacted by the incident, where applicable;
- (f) information on how the incident has been discovered;
- (g) information about the origin of the incident, where available;
- (h) indication whether a business continuity plan has been activated;
- (i) information about the reclassification of the incident from major to non-major, where applicable; and
- (j) other information, where available.

*Article 4*

**Content of intermediate reports**

Financial entities shall provide at least the following information about the incident in the intermediate report:

- (a) incident reference code provided by the competent authority, where applicable;
- (b) date and time of occurrence of the incident;
- (c) date and time when regular activities have been restored, where applicable;
- (d) information about the classification criteria that triggered the incident report;
- (e) type of the incident;
- (f) threats and techniques used by the threat actor, where applicable;
- (g) affected functional areas and business processes;
- (h) affected infrastructure components supporting business processes;
- (i) impact on the financial interest of clients;
- (j) information about reporting to other authorities;
- (k) temporary actions/measures taken or planned to be taken to recover from the incident; and
- (l) information on indicators of compromise, where applicable.

*Article 5*

**Content of final reports**

Financial entities shall provide the following information about the incident in the final re-port:

- (a) information about the root causes of the incident
- (b) dates and times when the incident was resolved and the root cause addressed;
- (c) information on the incident resolution;
- (d) information relevant for resolution authorities, where applicable;
- (e) information about direct and indirect costs and losses stemming from the incident and information about financial recoveries; and
- (f) information about recurring incidents, where applicable

*Article 6*

**Time limits for the initial notification and intermediate report and final reports referred to in Article 19(4) of Regulation (EU)2022/2554**

1. The time limits for the submission of the initial notification and the intermediate and final reports as referred to in Article 19(4)(a) to (c) of Regulation (EU)2022/2554 shall be as follows:

- (a) the initial report shall be submitted as early as possible within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the moment the financial entity has become aware of the incident;
- (b) An intermediate report shall be submitted the latest within 72 hours from the submission of the initial notification even where the status or the handling of the incident have not changed as referred to in Article 19(4)(b) of Regulation (EU) 2022/2554. Financial entities shall submit without undue delay an updated intermediate report, in any case, when regular activities have been recovered.
- (c) the final report shall be submitted no later than one month from the submission of the latest updated intermediate report.

2. Where an incident that has not been classified as major within the 24 hours is classified as major at a later stage, the financial entity shall submit the initial notification within the four-hours after the classification of the incident.

3. Where financial entities are unable to submit the initial notification, intermediate report or final report within the timelines as set out in paragraph 1, financial entities shall in-form the competent authority without undue delay, but no later than the respective time limit for submission of the notification/report, and shall explain the reasons for the de-lay.

4. Where the time limit for submission of an initial notification, intermediate report or a final report falls on a weekend day or a bank holiday in the Member State of the report-ing financial entity, the financial entity may submit the initial notification, intermediate or final reports by noon of the next working day.

5. Paragraph 4 shall not apply for the submission of an initial notification and an interme-diate report by credit institutions, central counterparties, operators of trading venues, and other financial entities identified as essential or important entities pursuant to na-tional rules transposing Article 3 of Directive (EU) 2022/2555, or financial entities de-clared as significant or systemic by the competent authority. In this case, the financial entities shall apply the time limits set out in paragraph 1.

*Article 7*

**Content of the voluntary notification of significant cyber threat**

The content of the notification in relation to significant cyber threats in accordance with Article 19(2) of Regulation (EU) 2022/2554 shall cover:

- (a) general information about the reporting entity as set out in Article 4;
- (b) date and time of detection of the significant cyber threat and any other relevant timestamps related to the threat;
- (c) description of the significant cyber threat;
- (d) information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts;
- (e) the classification criteria that would have triggered a major incident report, if the cyber threat had materialised;
- (f) information about the status of the cyber threat and any changes in the threat activity;
- (g) description of the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, where applicable; and
- (h) information about notification of the cyber threat to other financial entities or authorities;
- (i) information on indicators of compromise, where applicable; and
- (j) other relevant information, where available.

*Article 8*

**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,

**COMMISSION IMPLEMENTING REGULATION (EU) .../...**

**of XXX**

**laying down implementing technical standards for the application of [Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.**

**(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 and in particular Article 20 (b) thereof,

Whereas:

- (1) In order to ensure consistent reporting of major incidents and submission of good quality data, it should be specified which data fields need to be provided by financial entities at various stages of the reporting, when providing initial notification, inter-mediate and final reports as referred to in Article 19(4) of Regulation (EU) 2024/25542. It is important that information provided over the different reporting stages until the final report is presented in a way that allows for a single overview. Therefore, there should be a single template which covers all necessary information throughout the reporting stages that should be used for the submission of the initial notification, the intermediate and final report.
- (2) Financial entities should complete those data fields of the template, which correspond to the information requirements of the respective notification or report. However, where financial entities have information which they are required to provide at a later reporting stage, i.e. the intermediate or final report as relevant, they should be allowed to anticipate that data and complete those data fields and provide to the competent authorities.
- (3) The design of the template and data fields should also enable the reporting of multiple or recurring incidents, since those incidents may constitute a major incident in accordance with Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.
- (4) In order to ensure accurate and up to date information, financial entities should update the previously submitted information when submitting the intermediate and final report, respectively, and should reclassify major incidents as non-major, where necessary.
- (5) The legal identification of entities within the scope of this Implementing Regulation should be aligned with the identifiers specified in the Commission Implementing Regulation specifying Art. 28(9) of Regulation (EU) 2022/2554.
- (6) To identify more easily the impact of an incident having occurred at or being caused by a third-party provider affecting multiple financial entities within a single Member State, and to reduce the reporting effort for financial entities, the reporting template should allow for the submission of an aggregated report covering aggregated information about the impact of the incident on all impacted financial entities that have classified the incident as major.
- (7) The design of the template should be technology and reporting format neutral to allow for its integration into various incident reporting solutions that already exist or may be developed for the implementation of the requirements of the Regulation (EU) 2022/2554.



- (8) The design of the reporting templates and data fields should facilitate the reporting of major ICT-related incidents by third parties to whom financial entities outsourced their reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554.
- (9) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Supervisory Authorities (ESAs).
- (10) The ESAs have conducted open public consultations on the draft implementing technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010, 1095/2010 of the European Parliament and of the Council,

HAS ADOPTED THIS REGULATION:

*Article 1*

**Standard form for reporting of ICT-related major incidents**

1. Financial entities shall use the template in Annex I to submit the initial notification, intermediate and final report as follows:
  - (a) Where an initial notification is submitted, financial entities shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 3 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554. Financial entities may complete data fields, the completion of which is not required for an initial notification, but for an intermediate or final report, where they have the relevant information.
  - (b) Where an intermediate report is submitted, financial entities shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 4 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554. Financial entities may complete data fields, the completion of which is not required for the intermediate report, but for the final report, where they have the relevant information.
  - (c) Where a final report is submitted, financial entities shall complete the data fields of the template to be completed which correspond to the information to be provided in accordance with Article 5 of Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554.
2. Financial entities shall ensure that the information contained in the initial notification, intermediate and final report is complete and accurate.
3. Where accurate data is not available at the time of reporting for the initial notification or the intermediate report, the financial entity shall provide estimated values based on other available data and information to the extent possible.
4. When submitting an intermediate or final report, financial entities shall update, where applicable, the information that was previously provided with the initial notification or the intermediate report.
5. Financial entities shall follow the data glossary and instructions set out in Annex II when completing the template in Annex I.

*Article 2*

**Submission of initial notification, intermediate and final reports together**

Financial entities may combine the submission of the initial notification, intermediate report and/or final report to provide two or all of those at the same time, where regular activities have been recovered and/or the root cause analysis has been completed, provided that the timelines set out in Article 6 of the Commission Delegated Regulation specifying Article 20a of Regulation (EU) 2022/2554 are met.

*Article 3*

**Recurring incidents**

Where the information is provided for recurring incidents, which do not individually meet the criteria for a major ICT related incident but do so cumulatively in accordance with Article 8(2) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, financial entities shall provide aggregated information regarding such incidents.

*Article 4*

**Use of secure channels in case of deviation from established channels or time limits**

1. Financial entities shall use secure electronic channels set out by their competent authority to submit the initial notification and intermediate and final reports .
2. Where financial entities are unable to use established channels to submit incident notifications or reports to their competent authority, financial entities shall inform the competent authority about the major incident through other secure means, after consulting with or as previously agreed with the competent authority. If required by the competent authority, financial entities shall resubmit the initial notification, intermediate or final report through the established channels under paragraph 1 once they are able to do so.

*Article 5*

**Reclassification of major incidents**

Where after further assessment of the incident, the financial entity reaches the conclusion that the incident previously reported as major at no time fulfilled the classification criteria and thresholds in accordance with Article 18(4) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, the financial entity shall indicate it has reclassified the incident from major to non-major and shall submit the information related to the reclassification of the major incident as non-major by completing the template in Annex II in relation to the fields 'type of report' and 'other information'.

*Article 6*

**Notification of outsourcing of the reporting obligation**

Where financial entities intend to outsource the incident reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554, including where such outsourcing will be part of a general and/or long-term outsourcing arrangement, they shall inform their competent authority prior to the first notification or reporting under such an arrangement and the latest as soon as the outsourcing arrangement has been concluded. Financial entities shall provide to the competent authority the name, contact details, and an identification code of the third-party that will submit the incident notifications or reports for them. Financial entities shall also inform their competent authority, where such outsourcing no longer takes place or has been cancelled.

*Article 7*

**Aggregated reporting**

1. A third-party provider, to whom reporting obligations have been outsourced, may aggregate the information about a major ICT-related incident impacting multiple financial entities in one single notification or report, and submit it to the competent authority for all impacted financial entities, provided that all of the following conditions are met:
  - a) the major incidents to be reported originate from or is being caused by a third-party provider;
  - b) this third-party provider provides the relevant ICT service to more than one financial entity, or to a group, in the Member State;

- c) the incident is classified as major individually by each financial entity covered in the aggregated report,
  - d) the incident affects financial entities within a single Member State and the aggregated report relates to financial entities which are supervised by the same competent authority;
  - e) the financial entities affected by the incident have outsourced reporting obligations to a third-party provider in accordance with Art. 19(5) of Regulation (EU) 2022/2554 and Article 6 of this Regulation, and
  - f) competent authorities have explicitly permitted aggregated reporting to those financial entities.
2. Significant credit institutions in accordance with Article 6(4) of Regulation (EU) No 1024/2013, operators of trading venues and central counterparties shall be required to submit an incident notification or report at solo level to their competent authority.
3. Upon request by the competent authority, financial entities shall submit a separate individual incident notification or report.

*Article 8*

**Standard form for voluntary reporting of notification of significant cyber threats**

1. When notifying the competent authorities of significant cyber threats in accordance with Article 19(2) of Regulation (EU) 2022/2554, financial entities shall use the template in Annex III and follow the data glossary and instructions set out Annex IV.
2. Financial entities shall ensure that the information contained in the cyber threat notification is complete and accurate.

*Article 9*

**Entry into force and application**

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,

**ANNEX I**

**Templates for the reporting of major incidents**

Number of field	Data field	
<b>General information about the financial entity</b>		
1.1	Type of report	
1.2	Name of the entity submitting the report	
1.3	Identification code of the entity submitting the report	
1.4	Type of the affected financial entity	
1.5	Name of the financial entity affected	
1.6	LEI code of the financial entity affected	
1.7	Primary contact person name	
1.8	Primary contact person email	
1.9	Primary contact person telephone	
1.10	Second contact person name	
1.11	Second contact person email	
1.12	Second contact person telephone	
1.13	Name of the ultimate parent undertaking	
1.14	LEI code of the ultimate parent undertaking	
1.15	Reporting currency	
<b>Content of the initial notification</b>		
2.1	Incident reference code provided by the financial entity	
2.2	Date and time of detection of the incident	

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Number of field	Data field	
2.3	Date and time of classification of the incident as major	
2.4	Description of the incident	
2.5	Classification criteria that triggered the incident report	
2.6	Materiality thresholds for the classification criterion 'Geographical spread'	
2.7	Discovery of the incident	
2.8	Indication whether the incident originates from a third-party provider or another financial entity	
2.9	Activation of business continuity plan, if activated	
2.10	Other information	
<b>Content of the intermediate report</b>		
3.1	Incident reference code provided by the competent authority	
3.2	Date and time of occurrence of the incident	
3.3	Date and time when services, activities and/or operations have been restored	
3.4	Number of clients affected	
3.5	Percentage of clients affected	
3.6	Number of financial counterparts affected	
3.7	Percentage of financial counterparts affected	
3.8	Impact on relevant clients or financial counterparts	
3.9	Number of affected transactions	
3.10	Percentage of affected transactions	
3.11	Value of affected transactions	
3.12	Information whether the numbers are actual or estimates, or whether there has not been any impact	
3.13	Reputational impact	
3.14	Contextual information about the reputational impact	

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Number of field	Data field	
3.15	Duration of the incident	
3.16	Service downtime	
3.17	Information whether the numbers for duration and service downtime are actual or estimates.	
3.18	Types of impact in the Member States	
3.19	Description of how the incident has an impact in other Member States	
3.20	Materiality thresholds for the classification criterion 'Data losses'	
3.21	Description of the data losses	
3.22	Classification criterion 'Critical services affected'	
3.23	Type of the incident	
3.24	Other types of incidents	
3.25	Threats and techniques used by the threat actor	
3.26	Other types of techniques	
3.27	Information about affected functional areas and business processes	
3.28	Affected infrastructure components supporting business processes	
3.29	Information about affected infrastructure components supporting business processes	
3.30	Impact on the financial interest of clients	
3.31	Reporting to other authorities	
3.32	Specification of 'other' authorities	
3.33	Temporary actions/measures taken or planned to be taken to recover from the incident	
3.34	Description of any temporary actions and measures taken or planned to be taken to recover from the incident	
3.35	Indicators of compromise	
<b>Content of the final report</b>		
4.1	High-level classification of root causes of the incident	

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Number of field	Data field	
4.2	Detailed classification of root causes of the incident	
4.3	Additional classification of root causes of the incident	
4.4	Other types of root cause types	
4.5	Information about the root causes of the incident	
4.6	Incident resolution summary	
4.7	Date and time when the incident root cause was addressed	
4.8	Date and time when the incident was resolved	
4.9	Information if the permanent resolution date of the incident differs from the initially planned implementation date	
4.10	Assessment of risk to critical functions for resolution purposes	
4.11	Information relevant for resolution authorities	
4.12	Materiality threshold for the classification criterion 'Economic impact'	
4.13	Amount of gross direct and indirect costs and losses	
4.14	Amount of financial recoveries	
4.15	Information whether the non-major incidents have been recurring	
4.16	Date and time of occurrence of recurring incidents	

**ANNEX II**

**Data glossary and instructions for the reporting of major incidents**

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
<b>General information about the financial entity</b>					
1.1. Type of report	Indicate the type of incident notification or report being submitted to the competent authority.	Yes	Yes	Yes	Choice: - initial notification - intermediate report - final report - major incident reclassified as non-major
1.2. Name of the entity submitting the report	Full legal name of the entity submitting the report.	Yes	Yes	Yes	Alphanumeric
1.3. Identification code of the entity submitting the report	<p>Identification code of the entity submitting the report.</p> <p>Where financial entities submit the notification/report, the identification code is to be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.</p> <p>Where a third-party provider submits a report for a financial entity, they can use an identification code as specified in the Commission Implementing Regulation specifying Art. 28(9) from Regulation (EU) 2022/2554.</p>	Yes	Yes	Yes	Alphanumeric
1.4. Type of the affected financial entity	Type of the entity under Article 2.1(a)-(t) of DORA for whom the report is submitted.	Yes	Yes	Yes	Choice (multiselect): - credit institution - payment institution - exempted payment institution - account information service provider - electronic money institution - exempted electronic money institution - investment firm



APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					<ul style="list-style-type: none"> <li>- crypto-asset service provider</li> <li>- issuer of asset- referenced tokens</li> <li>- central securities depository</li> <li>- central counterparty</li> <li>- trading venue</li> <li>- trade repository</li> <li>- manager of alternative investment fund</li> <li>- management company</li> <li>- data reporting service provider</li> <li>- insurance and reinsurance undertaking</li> <li>- insurance intermediary, reinsurance intermediary and ancillary insurance intermediary</li> <li>- institution for occupational retirement provision</li> <li>- credit rating agency</li> <li>- administrator of critical benchmarks</li> <li>- crowdfunding service provider</li> <li>- securitisation repository</li> </ul>
1.5. Name of the financial entity affected	<p>Full legal name of the financial entity affected by the major ICT-related incident and required to report the major incident to their competent authority under Article 19 of Regulation (EU) 2022/2554.</p> <p>In case of aggregated reporting:</p> <p>(a) list of all names of the financial entities affected by the major ICT- related incident, separated by a semicolon.</p> <p>(b) the third-party provider submitting a major incident notification or in an aggregated manner in accordance with Article 7, to list the names of all financial entities impacted by the incident, separated by a semicolon.</p>	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
		reporting.	reporting	reporting	
1.6. LEI code of the financial entity affected	<p>Legal Entity Identifier (LEI) of the financial entity affected by the major ICT-related incident assigned in accordance with the International Organisation for Standardisation.</p> <p>In case of aggregated reporting</p> <p>(a) a list of all LEI codes of the financial entities affected by the major ICT-related incident, separated by a semicolon.</p> <p>(b) the third-party provider submitting a major incident notification or report in an aggregated manner in accordance with Article 7 to list the LEI codes of all financial entities impacted by the incident, separated by a semicolon.</p> <p>The order of appearance of LEI codes and FE names has to be the same so that it is possible to match name and LEI.</p>	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Yes, if the financial entity affected by the incident is different from the entity submitting the report and in case of aggregated reporting.	Unique 20 alphanumeric character code, based on ISO 17442-1:2020
1.7. Primary contact person name	<p>Name and surname of the primary contact person of the financial entity</p> <p>In case of aggregated reporting in accordance with Article 7, the name of the primary contact person in the entity submitting the aggregated report.</p>	Yes	Yes	Yes	Alphanumeric
1.8. Primary contact person email	<p>Email address of the primary contact person that can be used by the competent authority for follow-up communication</p> <p>In case of aggregated reporting in accordance with Article 7, the email of the primary contact person in the entity submitting the aggregated report.</p>	Yes	Yes	Yes	Alphanumeric
1.9. Primary contact person telephone	<p>Telephone number of the primary contact person that can be used by the competent authority for follow-up communication</p> <p>In case of aggregated reporting in accordance with Article 7, the telephone number of the primary contact person in the entity submitting the aggregated report.</p> <p>Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXXX)</p>	Yes	Yes	Yes	Alphanumeric
1.10. Second contact person name	<p>Name and surname of the second contact person or the name of the responsible team of the financial entity or an entity submitting the report on behalf of the financial entity</p>	Yes	Yes	Yes	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
1.11. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication	Yes	Yes	Yes	Alphanumeric
1.12. Second contact person telephone	Telephone number of the second contact person or a team that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Yes	Yes	Alphanumeric
1.13. Name of the ultimate parent undertaking	Name of the ultimate parent undertaking of the group in which the affected financial entity belongs to, where applicable	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Alphanumeric
1.14. LEI code of the ultimate parent undertaking	LEI of the ultimate parent undertaking of the group in which the affected financial entity belongs to, where applicable. Assigned in accordance with the International Organisation for Standardisation.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Yes, if the FE belongs to a group.	Unique 20 alphanumeric character code, based on ISO 17442-1:2020.
1.15. Reporting currency	Currency used for the incident reporting	Yes	Yes	Yes	Choice populated by using ISO 4217 currency codes
<b>Content of the initial notification</b>					
2.1. Incident reference code provided by the financial entity	Unique reference code issued by the financial entity unequivocally identifying the major incident. In case of aggregated reporting in accordance with Article 7, the incident reference code assigned by the third-party provider.	Yes	Yes	Yes	Alphanumeric
2.2. Date and time of detection of the incident	Date and time at which the financial entity has become aware of the ICT-related incident. For recurring incidents, the data and time at which the last ICT-related incident was detected.	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
2.3. Date and time of classification of the incident as major	Date and time when the ICT-related incident was classified as major according to the classification criteria established in Regulation (EU) 2023/XXXX	Yes	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
2.4. Description of the incident	Description of the most relevant aspects of the major ICT-related incident. Financial entities shall provide a high-level overview of the following information	Yes	Yes	Yes	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>such as possible causes, immediate impacts, systems affected, and others.</p> <p>Financial entities, shall include, where known or reasonably expected, whether the incident impacts third-party providers or other financial entities, the type of provider or financial entity, their name and their respective identification codes.</p> <p>In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the ICT-related incident and include also a description of any other relevant information about the incident not captured by the data fields, including the internal severity assessment by the financial entity (e.g. very low, low, medium, high, very high) and an indication of the level and name of most senior decision structures that has been involved in response to the incident.</p>				
2.5. Classification criteria that triggered the incident report	<p>Classification criteria under Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 that have triggered determination of the ICT-related incident as major and subsequent notification and reporting.</p> <p>In the case of aggregated reporting in accordance with Article 7, the classification criteria that have triggered determination of the ICT-related incident as major for at least one or more financial entities.</p>	Yes	Yes	Yes	Choice (multiple): - Clients, financial counterparts and transactions affected - Reputational impact - Duration and service downtime - Geographical spread - Data losses - Critical services affected Economic impact
2.6. Materiality thresholds for the classification criterion 'Geographical spread'	<p>EEA Member States impacted by the ICT-related incident</p> <p>Financial entities shall have regard to Articles 4 and 12 of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details.</p>	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.	Yes, if 'Geographical spread' threshold is met.	Choice (multiple) populated by using ISO 3166 ALPHA-2 of the affected countries
2.7. Discovery of the incident	Indication of how the incident has been discovered.	Yes	Yes	Yes	Choice: - IT Security - Staff - Internal audit

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					<ul style="list-style-type: none"> <li>- External audit</li> <li>- Clients</li> <li>- Financial counterparts</li> <li>- Third-party provider</li> <li>- Attacker</li> <li>- Monitoring systems</li> <li>- Authority/agency/law enforcement body</li> <li>- Other</li> </ul>
2.8. Indication whether the incident originates from a third-party provider or another financial entity	Indication whether the incident originates from a third-party provider or another financial entity (including financial entities belonging to the same group as the reporting entity) and the name and identification code of the third-party provider or financial entity.	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Yes, if the incident originates from a third-party provider or another financial entity	Alphanumeric
2.9. Activation of business continuity plan, if activated	Indication of whether there has been a formal activation of their business continuity response measures.	Yes	Yes	Yes	Boolean (Yes or No)
2.10. Other information	Any further information not covered in the template.  Where the incident has been reclassified as non-major, financial entities shall provide a description of the reasons why the incident does not fulfil the criteria to be considered as major and is not expected to fulfil them any longer before it is resolved.	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major.	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major	Yes, if there is other information not covered in the template or if the incident has been reclassified as non-major	Alphanumeric
<b>Content of the intermediate report</b>					
3.1. Incident reference code provided by the	Unique reference code assigned by the competent authority at the time of receipt of the initial notification to unequivocally identify the major incident.	No	Yes, if applicable	Yes, if applicable	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
competent authority					
3.2. Date and time of occurrence of the incident	Date and time at which the ICT-related incident has occurred, if different from the time of the financial entity has become aware of the incident For recurring incidents, the date and time at which the last ICT-related incident has occurred	No	Yes	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
3.3. Date and time when services, activities and/or operations have been restored	Information on the date and time of the restoration of the services, activities and/or operations affected by the incident	No	Yes, if data field 3.16. 'Service downtime' has been populated	Yes, if data field 3.16. 'Service downtime' has been populated	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
3.4. Number of clients affected	Number of clients affected by the ICT-related incident, which may be natural or legal persons, that make use of the service provided by the financial entity  Financial entities shall have regard of Articles 1.1 and 9.1(b) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual number of clients impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.  In the case of aggregated reporting in accordance with Article 7, the total number of clients affected across all financial entities.	No	Yes	Yes	Numerical integer
3.5. Percentage of clients affected	Percentage of clients affected by the ICT-related incident in relation to the total number of clients that make use of the affected service provided by the financial entity. In case of more than one service affected, these shall be provided in an aggregated manner.  Financial entities shall have regard of Articles 1.1 and 9.1(a) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual percentage of clients impacted cannot be determined, the financial entity shall use estimates based on available data from comparable	No	Yes	Yes	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	reference periods.  In the case of aggregated reporting in accordance with Article 7, the sum of all affected clients divided by the total number of clients of all impacted financial entities.				
3.6. Number of financial counterparts affected	Number of financial counterparts affected by the ICT-related incident, that have concluded a contractual arrangement with the financial entity  Financial entities shall have regard to Article 1.2 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual number of financial counterparts impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.  In the case of aggregated reporting in accordance with Article 7, the total number of financial counterparts affected across all financial entities.	No	Yes	Yes	Numerical integer
3.7. Percentage of financial counterparts affected	Percentage of financial counterparts affected by the ICT-related incident, in relation to the total number of financial counterparts that have concluded a contractual arrangement with the financial entity  Financial entities shall have regard to see Articles 1.1 and 9.1(c) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554 for more details. Where the actual percentage of financial counterparts impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.  In the case of aggregated reporting in accordance with Article 7, indicate the sum of all affected financial counterparts divided by the total number of financial counterparts of all impacted financial entities.	No	Yes	Yes	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.8. Impact on relevant clients or financial	Any identified impact on relevant clients or financial counterpart in accordance with Articles 1.3 and 9.1(f) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.	No	Yes, if 'Relevance of clients and	Yes, if 'Relevance of clients and	Boolean (Yes or No)

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
counterpart			financial counterparts' threshold is met	financial counterparts' threshold is met	
3.9. Number of affected transactions	<p>Number of transactions affected by the ICT-related incidents.</p> <p>In accordance with article 1.4 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, the financial entity shall take into account all affected domestic and cross-border transactions containing a monetary amount that have at least one part of the transaction carried out in the EU.</p> <p>Where the actual number of transactions impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.</p> <p>In the case of aggregated reporting in accordance with Article 7, indicate the total number of transactions affected across all financial entities.</p>	No	Yes, if any transaction has been affected by the incident	Yes, if any transaction has been affected by the incident	Numerical integer
3.10. Percentage of affected transactions	<p>Percentage of affected transactions in relation to the daily average number of domestic and cross-border transactions carried out by the financial entity related to the affected service</p> <p>Financial entities shall have regard of Article 1.4 and article 9.1(d) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.</p> <p>Where the actual percentage of transactions impacted cannot be determined, the financial entity shall use estimates.</p> <p>In the case of aggregated reporting in accordance with Article 7, the sum of the number of all affected transactions divided by the total number of transactions of all impacted financial entities.</p>	No	Yes, if any transaction has been affected by the incident	Yes, if any transaction has been affected by the incident	Expressed as percentage - any value up to 5 numeric characters including up to 1 decimal place expressed as percentage (e.g. 2.4 instead of 2.4%). If the value has more than 1 digit after the decimal, reporting counterparties shall round half-up
3.11. Value of affected transactions	<p>Total value of the transactions affected by the ICT-related incident in accordance with Article 1.4 and article 9.1e of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.</p>	No	Yes, if any transactions have been	Yes, if any transaction has been affected	Monetary The data point shall be



APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>Where the actual value of transactions impacted cannot be determined, the financial entity shall use estimates based on available data from comparable reference periods.</p> <p>The monetary amount is to be reported as a positive value.</p> <p>In the case of aggregated reporting in accordance with Article 7, the total value of the transactions affected across all financial entities.</p>		affected by the incident	by the incident	reported in units using a minimum precision equivalent to thousands of units (e.g. 2.5 instead of EUR 2500).
3.12. Information whether the numbers are actual or estimates, or whether there has not been any impact	Information whether the values reported in the data fields 3.4. to 3.11. are actual or estimates, or whether there has not been any impact.	No	Yes	Yes	Choice (multiple): <ul style="list-style-type: none"> <li>- Actual figures for clients affected</li> <li>- Actual figures for financial counterparts affected</li> <li>- Actual figures for transactions affected</li> <li>- Estimates for clients affected</li> <li>- Estimates for financial counterparts affected</li> <li>- Estimates for transactions affected</li> <li>- No impact on clients</li> <li>- No impact on financial counterparts</li> <li>- No impact on transactions</li> </ul>
3.13. Reputational impact	<p>Information about the reputational impact resulting from the incident in accordance with Article 2 and Article 10 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.</p> <p>In the case of aggregated reporting in accordance with Article 7, the reputational impact categories that apply to at least one financial entity.</p>	No	Yes, if 'Reputational impact' criterion met	Yes, if 'Reputational impact' criterion met	Choice (multiple): <ul style="list-style-type: none"> <li>- the incident has been reflected in the media;</li> <li>- the incident has resulted in repetitive complaints from different clients or financial counterparts on client-facing services or critical business</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
					relation-ships  - the financial entity will not be able to or is likely not to be able to meet regulatory requirements as a result of the incident  - the financial entity will or is likely to lose clients or financial counterparts with a material impact on its business as a result of the incident
3.14. Contextual information about the reputational impact	<p>Information describing how the ICT-related incident has affected or could affect the reputation of the financial entity, such as infringements of law, regulatory requirements not met, number of client complaints and others.</p> <p>The contextual information Include additional information, such as type of media (e.g. traditional, social media, blogs, social networks, streaming platforms) and media coverage, including reach of the media (local, national, international). It should be noted that media coverage in this context does not mean only a few negative comments by followers or users of social networks.</p> <p>The financial entity shall also indicate whether the media coverage highlighted significant risks for its clients in relation to the incident, such as the risk of the financial entity’s insolvency or the risk of losing funds. Financial entities shall also indicate whether it has provided information to the media that served to reliably inform the public about the incident and its consequences.</p> <p>Financial entities may also indicate whether there was false information in the media in relation to the incident, including information based on deliberate misinformation spread by threat actors, or information relating to or illustrating defacement of the financial entity's website.</p>	No	Yes, if 'Reputational impact' criterion met.	Yes, if 'Reputational impact' criterion met.	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.15. Duration of the incident	<p>The duration of the ICT-related incident shall be measured from the moment the incident occurs until the moment when the incident is resolved</p> <p>Where financial entities are unable to determine the moment when the incident has occurred, they shall measure the duration of the incident from the earlier between the moment it was detected and the moment when it has been recorded in network or system logs or other data sources. Where financial entities do not yet know the moment when the incident will be resolved, they shall apply estimates. The value shall be expressed in days, hours and minutes.</p> <p>In the case of aggregated reporting in accordance with Article 7, the longest duration of the incident in case of differences between financial entities.</p>	No	Yes	Yes	DD:HH:MM
3.16. Service downtime	<p>Service downtime measured from the moment the service is fully or partially unavailable to clients, financial counterparts or other internal or external users to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident.</p> <p>Where the service downtime causes a delay in the provision of service after regular activities/operations have been restored, the downtime shall be measured from the start of the incident to the moment when that delayed service is provided. Where financial entities are unable to determine the moment when the service downtime has started, they shall measure the service downtime from the earlier between the moment it was detected and the moment when it has been recorded. In the case of aggregated reporting in accordance with Article 7, the longest duration of the service downtime in case of differences between financial entities.</p>	No	Yes, if the incident has caused a service downtime	Yes, if the incident has caused a service downtime	DD:HH:MM
3.17. Information whether the numbers for duration and service downtime are actual or	Information whether the values reported in data fields 3.15 and 3.16. are actual or estimates.	No	Yes, if 'Duration and service downtime' criterion met	Yes, if 'Duration and service downtime' criterion met	Choice: <ul style="list-style-type: none"> <li>- Actual figures</li> <li>- Estimates Actual figures and estimates</li> <li>- No information available</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
estimates.					
3.18. Types of impact in the Member States	Type of impact in the respective EEA Member States.  Indication of whether the major ICT-related incident has had an impact in other EEA Member States (other than the Member State of the competent authority to which the incident is directly reported), in accordance with Article 4 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, and in particular with regard to the significance of the impact in relation to: a) clients and financial counterparts affected in other Member States; or b) Branches or other financial entities within the group carrying out activities in other Member States; or c) Financial market infrastructures or third-party providers, which may affect financial entities in other Member States to which they provide services.	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Choice (multiple): - clients - financial counterparts - branch of the financial entity - financial entities within the group carrying out activities in the respective Member State - financial market infrastructure - third-party providers that may be common with other financial entities
3.19. Description of how the incident has an impact in other Member States	Description of the impact and severity of the incident in each affected Member State  Information should include the assessment of impact and severity on: a) clients; or b) financial counterparts; or c) Branches of the financial entity; or d) Other financial entities within the group carrying out activities in the respective Member State; or e) Financial market infrastructures; or f) Third-party providers that may be common with other financial entities as applicable in other member state(s).	No	Yes, if 'Geographical spread' threshold is met	Yes, if 'Geographical spread' threshold is met	Alphanumeric
3.20. Materiality thresholds for the classification criterion 'Data losses'	Type of data losses that the ICT-related incident entails in relation to availability, authenticity, integrity and confidentiality of data.  In accordance with Articles 5 and 13 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.  In case of aggregated reporting in accordance with Article 7, the data losses	No	Yes, if 'Data losses' criterion is met	Yes, if 'Data losses' criterion is met	Choice (multiple): - availability - authenticity - integrity - confidentiality

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	affecting at least one financial entity.				
3.21. Description of the data losses	<p>Description of the impact of the incident on availability, authenticity, integrity and confidentiality of critical data</p> <p>In accordance with Articles 5 and 13 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554. Information about the impact on the implementation of the business objectives of the financial entity and/or on meeting regulatory requirements.</p> <p>As part of the information provided, financial entities shall indicate whether the data affected is client data, other entities’ data (e.g. financial counterparts) or data of the financial entity itself.</p> <p>The financial entity may also indicate the type of data involved in the incident - in particular, whether the data is confidential and what type of confidentiality was involved (e.g. commercial/business confidentiality, personal data, professional secrecy: banking secrecy, insurance secrecy, payment services secrecy, etc.).</p> <p>The information may also include possible risks associated with the data losses, such as whether the data affected by the incident can be used to identify individuals and could be used by the threat actor to obtain credit or loans without their consent, to conduct spear phishing attacks, to disclose information publicly.</p> <p>In the case of aggregated reporting in accordance with Article 7, a general description of the impact of the incident on the affected financial entities. Where there are differences of the impact, the description of the impact should clearly indicate the specific impact on the different financial entities.</p>	No	Yes, if ‘Data losses’ criterion is met	Yes, if ‘Data losses’ criterion is met	Alphanumeric
3.22. Classification criterion ‘Critical services affected’	<p>Information related to the criterion ‘Critical services affected’.</p> <p>In accordance with Articles 6 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, including information about:</p> <ul style="list-style-type: none"> <li>- the affected services or activities that require authorisation, registration or that are supervised by competent authorities; and/or</li> <li>- the ICT services or network and information systems that support critical or important functions of the financial entity; and</li> </ul>	No	Yes	Yes	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>- the nature of the malicious and unauthorised access to the network and information systems of the financial entity.</p> <p>In the case of aggregated reporting in accordance with Article 7, the impact on critical services that apply to at least one financial entity.</p>				
3.23. Type of the incident	Classification of incidents by type.	No	Yes	Yes	Choice (multiple): <ul style="list-style-type: none"> <li>- Cybersecurity-related</li> <li>- Process failure</li> <li>- System failure</li> <li>- External event</li> <li>- Payment-related</li> <li>- Other (please specify)</li> </ul>
3.24. Other types of incidents	Other types of incidents, where financial entities have selected 'other' type of incidents in the data field 3.23, financial entities shall specify the type of incident.	No	Yes, if 'other' type of incidents is selected in data field 3.23	Yes, if 'other' type of incidents is selected in data field 3.23	Alphanumeric
3.25. Threats and techniques used by the threat actor	Indicate the threats and techniques used by the threat actor. The following threats and techniques shall be considered: <ol style="list-style-type: none"> <li>1. Social engineering, including phishing</li> <li>2. (D)DoS</li> <li>3. Identity theft</li> <li>4. Data encryption for impact, including ransomware</li> <li>5. Resource hijacking</li> <li>6. Data exfiltration and manipulation, excluding identity theft</li> <li>7. Data destruction</li> <li>8. Defacement</li> <li>9. Supply-chain attack</li> <li>10. Other (please specify)</li> </ol>	No	Yes, if the type of the incident is 'cybersecurity-related' in field 3.23	Yes, if the type of the incident is 'cybersecurity-related' in field 3.23	Choice (multiple): <ul style="list-style-type: none"> <li>- Social engineering (including phishing)</li> <li>- (D)DoS</li> <li>- Identity theft</li> <li>- Data encryption for impact, including ransomware</li> <li>- Resource hijacking</li> <li>- Data exfiltration and manipulation, including identity theft</li> <li>- Data destruction</li> <li>- Defacement</li> <li>- Supply-chain attack</li> <li>- Other (please specify)</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
3.26. Other types of techniques	<p>Other types of techniques</p> <p>Where financial entities have selected ‘other’ type of techniques in data field 3.25, financial entities shall specify the type of technique.</p>	No	Yes, if other’ type of techniques is selected in data 3.25	Yes, if other’ type of techniques is selected in data 3.25	Alphanumeric
3.27. Information about affected functional areas and business processes	<p>Indication of the functional areas and business processes that are affected by the incident, including products and services.</p> <p>The functional areas may include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Marketing and business development</li> <li>• Customer service</li> <li>• Product management</li> <li>• Regulatory compliance</li> <li>• Risk management</li> <li>• Finance and accounting</li> <li>• HR and general services</li> <li>• Information Technology</li> </ul> <p>Business processes</p> <p>The business processes may include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Account information</li> <li>• Actuarial services</li> <li>• Acquiring of payment transactions</li> <li>• Authentication/authorization</li> <li>• Authority/client on-boarding</li> <li>• Benefit administration</li> <li>• Benefit payment management</li> <li>• Buying and selling packages insurances policies between insurances</li> <li>• Card payments</li> <li>• Cash management</li> </ul>	No	Yes	Yes	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<ul style="list-style-type: none"> <li>• Cash placement and/or withdrawals</li> <li>• Claim management</li> <li>• Claim process insurance</li> <li>• Clearing</li> <li>• Corporate loans conglomerates</li> <li>• Collective insurances</li> <li>• Credit transfers</li> <li>• Custody and asset safekeeping</li> <li>• Customer onboarding</li> <li>• Data ingestion</li> <li>• Data processing</li> <li>• Direct debits</li> <li>• Export insurances</li> <li>• Finalizing trades/deals trade floors</li> <li>• Financial instruments placing</li> <li>• Fund accounting</li> <li>• FX money</li> <li>• Investment advice</li> <li>• Investment management</li> <li>• Issuing of payment instruments</li> <li>• Lending management</li> <li>• Life insurance payments process</li> <li>• Money remittance</li> <li>• Net asset calculation</li> <li>• Order</li> <li>• Payment initiation</li> <li>• Policy underwriting issuance</li> <li>• Portfolio management</li> <li>• Premium collection</li> </ul>				



APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<ul style="list-style-type: none"> <li>• Reception/transmission/execution</li> <li>• Reinsurance</li> <li>• Settlement</li> <li>• Transaction monitoring</li> </ul> <p>In the case of aggregated reporting in accordance with Article 7, the affected functional areas and business processes that have been impacted in at least one financial entity.</p>				
3.28. Affected infrastructure components supporting business processes	Information on whether infrastructure components (servers, operating systems, software, application servers, middleware, network components, others) supporting business processes have been affected by the incident.	No	Yes	Yes	Choice: - Yes - No - Information not available
3.29. Information about affected infrastructure components supporting business processes	<p>Description on the impact of the incident on infrastructure components supporting business processes including hardware and software.</p> <p>Hardware includes servers, computers, data centres, switches, routers, hubs. Software includes operating systems, applications, databases, security tools, network components, others please specify. The descriptions should include the description or name of affected infrastructure components or systems, which may be complemented with the following information, where available:</p> <ul style="list-style-type: none"> <li>• Version information</li> <li>• Internal infrastructure/partially outsourced/fully outsourced – third-party provider name</li> <li>• Whether the infrastructure is shared/dedicated across multiple business functions</li> <li>• Relevant resilience/continuity/recovery/ substitutability arrangements in place</li> </ul>	No	Yes, if the incident has affected infrastructure components supporting business processes	Yes, if the incident has affected infrastructure components supporting business processes	Alphanumeric
3.30. Impact on the financial interest of	Information on whether the incident has impacted financial interest of clients	No	Yes	Yes	Choice: - Yes - No

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
clients					- Information not available
3.31. Reporting to other authorities	Specification of what authorities were informed about the incident.  Taking into account the differences resulting from the national legislation of the Member States, the concept of law enforcement authorities should be understood broadly to include public authorities empowered to prosecute cybercrime, including but not limited to police, law enforcement agencies or public prosecutors	No	Yes	Yes	Choice (multiple): - Police/Law Enforcement - CSIRT - Data Protection Authority - National Cybersecurity Agency - None - Other (please specify)
3.32. Specification of 'other' authorities	Specification of 'other' types of authorities informed about the incident  If selected in Data field 3.31. 'Other' the description shall include more detailed information about the authority to which the information about the incident was submitted.	No	Yes, if 'other' type of authorities have been informed by the financial entity about the incident	Yes, if 'other' type of authorities have been informed by the financial entity about the incident	Alphanumeric
3.33. Temporary actions/measures taken or planned to be taken to recover from the incident	Indication of whether financial entity has implemented (or plan to implement) any temporary actions that have been taken (or planned to be taken) to recover from the incident.	No	Yes	Yes	Boolean (Yes or No)
3.34. Description of any temporary actions and measures taken or planned to be taken to recover from the	The information shall include description of the immediate actions taken such as isolation of the incident at the network level, workaround procedures activated, USB ports blocked, Disaster Recovery site activated, any other additional security controls temporarily put in place.  Financial entities shall also indicate the date and the time of the implementation of the temporary actions and the expected date of return to the primary site. For any temporary actions that have not been implemented but are still planned,	No	Yes, if temporary actions/measures have been taken or are planned to be taken (data field 3.33)	Yes, if temporary actions/measures have been taken or are planned to be taken (data	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
incident	<p>indication of the date by when their implementation is foreseen.</p> <p>If no temporary actions/measures have been taken, please indicate the reason.</p>			field 3.33)	
3.35. Indicators of compromise	<p>Information related to the incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.</p> <p>The field applies only to the financial entities within the scope of Directive (EU) 2022/2555 and those financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, where relevant.</p> <p>The IoC provided by the financial entity may include, but not be limited to, the following categories of data:</p> <ul style="list-style-type: none"> <li>• IP addresses;</li> <li>• URL addresses;</li> <li>• Domains;</li> <li>• File hashes;</li> <li>• Malware data (malware name, file names and their locations, specific registry keys associated with malware activity);</li> <li>• Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic);</li> <li>• E-mail message data (sender, recipient, subject, header, content);</li> <li>• DNS requests and registry configurations;</li> <li>• User account activities (logins, privileged user account activity, privilege escalation);</li> <li>• Database traffic (read/write), requests to the same file.</li> </ul> <p>In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to “command and control” servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or</p>	No	Yes, if cybersecurity - related is selected as a type of incident in data field 3.23s	Yes, if cybersecurity- related is selected as a type of incident in data field 3.23	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	websites observed hosting malware or exploit kits, etc				
<b>Content of the final report</b>					
4.1. High- level classification of root causes of the incident	<p>High-level classification of root cause of the incident under the incident types.</p> <p>The following high-level categories shall be considered:</p> <ol style="list-style-type: none"> <li>1. Malicious actions</li> <li>2. Process failure</li> <li>3. System failure/malfunction</li> <li>4. Human error</li> <li>5. External event</li> </ol>	No	No	Yes	Choice (multiple): <ul style="list-style-type: none"> <li>- Malicious actions</li> <li>- Process failure</li> <li>- System failure/malfunction</li> <li>- Human error</li> <li>- External event</li> </ul>
4.2. Detailed classification of root causes of the incident	<p>Detailed classification of root causes of the incident under the incident types.</p> <p>The following detailed categories shall be considered linked to the high- level categories that are reported in data field 4.1:</p> <p><b>1. Malicious actions</b> (if selected, choose one or more the following)</p> <ol style="list-style-type: none"> <li>a. Deliberate internal actions</li> <li>b. Deliberate physical damage/manipulation/theft</li> <li>c. Fraudulent actions</li> </ol> <p><b>2. Process failure</b> (if selected, choose one or more the following):</p> <ol style="list-style-type: none"> <li>a. Insufficient and/or failure of monitoring and control</li> <li>b. Insufficient/unclear roles and responsibilities</li> <li>c. ICT risk management process failure:</li> <li>d. Insufficient and/or failure of ICT operations and ICT security operations</li> <li>e. Insufficient and/or failure of ICT project management</li> <li>f. Inadequate of internal policies, procedures and documentation</li> <li>g. Inadequate ICT Systems Acquisition, Development, and Maintenance</li> <li>h. Other (please specify)</li> </ol> <p><b>3. System failure/malfunction</b> (if selected, choose one or more the following)</p> <ol style="list-style-type: none"> <li>a. Hardware capacity and performance: incidents caused by hardware resources which prove inadequate in terms of capacity or performance to fulfil</li> </ol>	No	No	Yes	Choice (multiple): <ul style="list-style-type: none"> <li>- Malicious actions: deliberate internal actions</li> <li>- Malicious actions deliberate physical damage/manipulation /theft</li> <li>- Malicious actions: fraudulent actions</li> <li>- Process failure: insufficient and/or failure of monitoring and control</li> <li>- Process failure: insufficient/unclear roles and responsibilities</li> <li>- Process failure: ICT risk management process failure:</li> <li>- Process failure: insufficient and/or failure of ICT operations and ICT security</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>the applicable legislative requirements.</p> <p>b. Hardware maintenance: incidents resulting from inadequate or insufficient maintenance of hardware components, other than “Hardware obsolescence/ageing” as defined below.</p> <p>c. Hardware obsolescence/ageing: This root cause type involves incidents resulting from outdated or aging hardware components.</p> <p>d. Software compatibility/configuration: incidents caused by software components that are incompatible with other software or system configurations. It includes, but it is not limited to, incidents resulting from software conflicts, incorrect settings, or misconfigured parameters that impact the overall system functionality.</p> <p>e. Software performance: incidents resulting from software components that exhibit poor performance or inefficiencies, for reasons other than those defined under “Software compatibility/configuration” above. It includes incidents caused by slow response times, excessive resource consumption, or inefficient query execution impacting the performance of the software or system.</p> <p>f. Network configuration: incidents resulting from incorrect or misconfigured network settings or infrastructure. It includes but it is not limited to incidents caused by network configuration errors, routing issues, firewall misconfigurations, or other network-related problems affecting connectivity or communication.</p> <p>g. Physical damage: incidents caused by physical damage to ICT infrastructure which lead to system failures.</p> <p>h. Other (please specify)</p> <p><b>4. Human error</b> (if selected, choose one or more the following)</p> <p>a. Omission (unintentional)</p> <p>b. Mistake</p> <p>c. Skills &amp; knowledge: incidents resulting from a lack of expertise or proficiency in handling ICT systems or processes, that may be caused by inadequate training, insufficient knowledge, or gaps in skills required to perform specific tasks or address technical challenges</p> <p>d. Inadequate human resources: incidents caused by a lack of necessary resources, such as hardware, software, infrastructure, or personnel. It includes</p>				<p>operations</p> <ul style="list-style-type: none"> <li>- Process failure: insufficient and/or failure of ICT project management</li> <li>- Process failure: inadequate of internal policies, procedures and documentation</li> <li>- Process failure: inadequate ICT Systems Acquisition, Development, and Maintenance</li> <li>- Process failure: other (please specify)</li> <li>- System failure: hardware capacity and performance                             <ul style="list-style-type: none"> <li>- System failure: hardware maintenance</li> </ul> </li> <li>- System failure: hardware obsolescence/ageing</li> <li>- System failure: software compatibility/configuration</li> <li>- System failure: software performance</li> <li>- System failure: network configuration</li> <li>- System failure: physical damage</li> <li>- System failure: other (please specify)</li> <li>- Human error: omission</li> <li>- Human error: mistake</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>but it is not limited to situations where insufficient resources lead to operational inefficiencies, system failures, or an inability to meet business demands</p> <p>e. Miscommunication</p> <p>f. Other (please specify)</p> <p><b>5. External event</b> (if selected, choose one or more the following)</p> <p>a. Natural disasters/force majeure</p> <p>b. Third-party failures</p> <p>c. Other (please specify)</p> <p>Financial entities shall take into account that for recurring incidents, the specific apparent root cause of the incident.</p>				<ul style="list-style-type: none"> <li>- Human error: skills &amp; knowledge</li> <li>- Human error: inadequate human resources</li> <li>- Human error miscommunication                             <ul style="list-style-type: none"> <li>- Human error: other (please specify)</li> </ul> </li> <li>- External event: natural disasters/force majeure</li> <li>- External event: third-party failures                             <ul style="list-style-type: none"> <li>- External event: other (please specify)</li> </ul> </li> </ul>
<p>4.3. Additional classification of root causes of the incident</p>	<p>Additional classification of root causes of the incident under the incident types.</p> <p>The following additional classification categories shall be considered linked to the detailed categories that reported in data field 4.2.</p> <p>The field is mandatory for the final report if specific values required additional classification listed below are reported in data field 4.2.</p> <p>2(a) Insufficient and/or failure of monitoring and control:</p> <ul style="list-style-type: none"> <li>- Monitoring of policy adherence</li> <li>- Monitoring of third-party service providers</li> <li>- Monitoring and verification of remediation of vulnerabilities</li> <li>- Identity and access management</li> <li>- Encryption and cryptography</li> <li>- Logging</li> </ul> <p>2(c) ICT risk management process failure:</p> <ul style="list-style-type: none"> <li>- Failure in defining accurate risk tolerance levels</li> </ul>	No	No	Yes	<p>Choice (multiple):</p> <ul style="list-style-type: none"> <li>- Monitoring of policy adherence</li> <li>- Monitoring of third-party service providers</li> <li>- Monitoring and verification of remediation of vulnerabilities                             <ul style="list-style-type: none"> <li>- Identity and access management</li> </ul> </li> <li>- Inadequate ICT Systems Acquisition, Development, and Maintenance                             <ul style="list-style-type: none"> <li>- Insufficient and /or failure of software testing</li> </ul> </li> <li>- Encryption and cryptography</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<ul style="list-style-type: none"> <li>- Insufficient vulnerability and threat assessments</li> <li>- Inadequate risk treatment measures</li> <li>- Poor management of residual ICT risks</li> </ul> <p>2(d) Insufficient and/or failure of ICT operations and ICT security operations:</p> <ul style="list-style-type: none"> <li>- Vulnerability and patch management</li> <li>- Change management</li> <li>- Capacity and performance management</li> <li>- ICT asset management and information classification</li> <li>- Backup and restore</li> <li>- Error Handling</li> </ul> <p>2(g) Inadequate ICT Systems Acquisition, Development, and Maintenance:</p> <ul style="list-style-type: none"> <li>- Inadequate ICT Systems Acquisition, Development, and Maintenance</li> </ul> <p>Insufficient and /or failure of software testing</p>				<ul style="list-style-type: none"> <li>- Logging</li> <li>- Failure in defining accurate risk tolerance levels</li> <li>- Insufficient vulnerability and threat assessments</li> <li>- Inadequate risk treatment measures</li> <li>- Poor management of residual ICT risks</li> <li>- Vulnerability and patch management</li> <li>- Change management</li> <li>- Capacity and performance management</li> <li>- ICT asset management and information classification</li> <li>- Backup and restore</li> <li>- Error Handling</li> </ul>
4.4. Other types of root cause types	Financial entities shall specify other types of root cause types where they have selected 'other' type of root cause in data field 4.2.	No	No	Yes, if 'other' type of root causes is selected in data field 4.2.	Alphanumeric
4.5. Information about the root causes of the incident	Description of the sequence of events that led to the incident and description of how the incident has a similar apparent root cause if the incident is classified as a recurring incident. This includes a concise description of all underlying reasons and primary factors that contributed to the occurrence of the incident. Where there were malicious actions, description of the modus operandi of the malicious action, including the tactics, techniques and procedures used, as well as	No	No	Yes	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<p>the entry vector of the incident.</p> <p>Includes description of the investigations and analysis that led to the identification of the root causes, if applicable.</p>				
4.6. Incident resolution	<p>Additional information regarding the actions/measures taken/planned to permanently resolve the incident and to prevent that incident from happening again in the future.</p> <p>Lessons learnt from the incident.</p> <p>The description shall include the following points in your answer (non- exhaustive list):</p> <p>A) Resolution actions description</p> <ul style="list-style-type: none"> <li>• Actions taken to permanently resolve the incident (excluding any temporary actions);</li> <li>• For each action taken, indicate the potential involvement of a third-party provider and of the financial entity;</li> <li>• Indicate if procedures have been adapted, following the incident;</li> <li>• Indicate any additional controls that were put in place or that are planned with related implementation timeline.</li> </ul> <p>Potential issues identified regarding the robustness of the IT systems impacted and/or in terms of the procedures and/or controls in place, if applicable.</p> <p>Financial entities shall clearly indicate how the envisaged remediation actions will address the identified root causes and when the incident is expected to be resolved permanently.</p> <p>B) Lessons learnt</p> <p>Financial entities shall describe findings from the post-incident review.</p>	No	No	Yes	Alphanumeric
4.7. Date and time when the incident root cause was	Date and time when the incident root cause was addressed.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)



APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
addressed					
4.8. Date and time when the incident was resolved	Date and time when the incident was resolved.	No	No	Yes	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)
4.9. Information if the permanent resolution date of the incidents differs from the initially planned implementation date	Descriptions of the reason for the permanent resolution date of the incidents being different from the initially planned implementation date, if applicable.	No	No	Yes	Alphanumeric
4.10. Assessment of risk to critical functions for resolution purposes	<p>Assessment on whether the incident poses a risk to critical functions within the meaning of Article 2(1), point (35) of Directive 2014/59/EU.</p> <p>Entities referred to in Art. 1(1) of the Directive 2014/59/EU shall indicate whether the incident poses a risk to critical functions within the meaning of Article 2(1), point (35) of the BRRD, and reported in Template Z07.01 of Commission Implementing Regulation (EU) 2018/1624 and mapped to the specific entity in Template Z07.02.</p>	No	No	Yes, if the incident poses a risk to critical functions of financial entities under Art. 2(1), point 35 of Directive 2014/59/E U	Alphanumeric
4.11. Information relevant for resolution authorities	<p>Description of whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>Entities referred to in Art. 1(1) of the Directive 2014/59/EU shall provide information on whether and, if so, how the major ICT-related incident has affected the resolvability of the entity or the group.</p> <p>The entities shall also indicate whether the incident affects the solvency or liquidity of the financial entity and the potential quantification of the impact.</p> <p>The entities shall also provide information on the impact on operational continuity, impact on resolvability of the entity, any additional impact on the costs and losses from the incident, including on the financial entity's capital</p>	No	No	Yes, if the incident has affected the resolvability of the entity or the group.	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	position, and whether the contractual arrangements on the use of ICT services are still robust and fully enforceable in the event of resolution of the institution.				
4.12. Materiality threshold for the classification criterion 'Economic impact'	Detailed information about thresholds eventually reached by the incident in relation to the criterion 'Economic impact' in accordance with articles 7 and 14 of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.	No	No	Yes	Alphanumeric
4.13. Amount of gross direct and indirect costs and losses	<p>Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major incident, including: Amount of expropriated funds or financial assets for which the financial entity is liable</p> <p>Amount of replacement or relocation costs of software, hardware or infrastructure.</p> <p>Amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff.</p> <p>Amount of fees due to non-compliance with contractual obligations.</p> <p>Amount of customer redress and compensation costs.</p> <p>Amount of losses due to forgone revenues.</p> <p>Amount of costs associated with internal and external communication.</p> <p>Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services.</p> <p>Amount other costs and losses, including:</p> <ul style="list-style-type: none"> <li>• direct charges, including impairments and settlement charges, to the Profit and Loss account and write-downs due to the major ICT- related incident;</li> </ul>	No	No	Yes	Monetary

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	<ul style="list-style-type: none"> <li>• provisions or reserves accounted for in the Profit and Loss account against probable losses related to the major ICT-related incident;</li> <li>• pending losses, in the form of losses stemming from the major ICT-related incident, which are temporarily booked in transitory or suspense accounts and are not yet reflected in the Profit and Loss which are planned to be included within a time period commensurate to the size and age of the pending item;</li> <li>• material uncollected revenues, related to contractual obligations with third parties, including the decision to compensate a client following the major ICT-related incident, rather than by a reimbursement or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific future period of time;</li> <li>• timing losses, where they span more than one financial accounting year and give rise to legal risk.</li> </ul> <p>In accordance with article 7(1) and (2) of the Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554, before taking into account financial recoveries of any type.</p> <p>The monetary amount is to be reported as a positive value.</p> <p>In the case of aggregated reporting in accordance with Article 7, the total amount of costs and losses across all financial entities.</p> <p>The data point shall be reported in units using a minimum precision equivalent to thousands of units.</p>				
4.14. Amount of financial recoveries	<p>Total amount of financial recoveries.</p> <p>Financial recoveries cover the occurrence related to the original loss that is independent of that loss and that is separate in time, in which funds or inflows of economic benefits are received from first or third parties.</p> <p>The monetary amount is to be reported as a positive value.</p>	No	No	Yes	<p>Monetary</p> <p>The data point shall be reported in units using a minimum precision equivalent to thousands of units</p>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory for initial notification	Mandatory for intermediate report	Mandatory for final report	Field type
	In the case of aggregated reporting in accordance with Article 7, the total amount of financial recoveries across all financial entities.				
4.15. Information whether the non-major incidents have been recurring	<p>Information on whether more than one non-major incident have been recurring and are considered a major incident within the meaning of Article 8(2) of Commission Delegated Regulation specifying Article 18(3) of Regulation (EU) 2022/2554.</p> <p>Financial entities shall indicate whether the non-major incidents have been recurring and are considered as one major incident.</p> <p>Financial entities shall also indicate the number of occurrences of these non-major incidents.</p>	No	No	Yes, if the major incident comprises more than one nonmajor recurring incidents.	Alphanumeric
4.16. Date and time of occurrence of recurring incidents	Where recurring incidents are being reported, date and time at which the first ICT-related incident has occurred.	No	No	Yes, for recurring incidents	ISO 8601 standard UTC (YYYY-MM-DD Thh: mm:ss)

**ANNEX III**

**Templates for notification of significant cyber threats**

Number of field	Data field	
1	Name of the entity submitting the notification	
2	Identification code of the entity submitting the notification	
3	Type of the financial entity submitting the notification	
4	Name of the financial entity	
5	LEI code of the financial entity	
6	Primary contact person name	
7	Primary contact person email	
8	Primary contact person telephone	
9	Second contact person name	
10	Second contact person email	
11	Second contact person telephone	
12	Date and time of detection of the cyber threat	
13	Description of the significant cyber threat	
14	Information about potential impact	
15	Potential incident classification criteria	
16	Status of the cyber threat	
17	Actions taken to prevent materialisation	
18	Notification to other stakeholders	
29	Indicators of compromise	
20	Other relevant information	

ANNEX IV

Data glossary and instructions for notification of significant cyber threats

Data field	Description	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification.	Yes	Alphanumeric
2. Identification code of the entity submitting the notification	<p>Identification code of the entity submitting the notification.</p> <p>Where financial entities submit the notification/report, the identification code is to be a Legal Entity Identifier (LEI), which is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.</p> <p>Where a third-party provider submits a report for a financial entity, they can use an identification code as specified in the Commission Implementing Regulation specifying Art. 28(9) from Regulation (EU) 2022/2554.</p>	Yes	Alphanumeric
3. Type of financial entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report.	Yes, if the report is not provided by the affected financial entity directly.	Choice (multiselect): <ul style="list-style-type: none"> <li>- credit institution</li> <li>- payment institution</li> <li>- exempted payment institution</li> <li>- account information service provider</li> <li>- electronic money institution</li> <li>- exempted electronic money institution</li> <li>- investment firm</li> <li>- crypto-asset service provider</li> <li>- issuer of asset-referenced tokens</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
			<ul style="list-style-type: none"> <li>- central securities depository</li> <li>- central counterparty</li> <li>- trading venue</li> <li>- trade repository</li> <li>- manager of alternative investment fund</li> <li>- management company</li> <li>- data reporting service provider</li> <li>- insurance and reinsurance undertaking</li> <li>- insurance intermediary, reinsurance intermediary and ancillary insurance intermediary</li> <li>- institution for occupational retirement provision</li> <li>- credit rating agency</li> <li>- administrator of critical benchmarks</li> <li>- crowdfunding service provider</li> <li>- securitisation repository</li> </ul>
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Yes, if the financial entity is different from the entity submitting the notification.	Alphanumeric
5. LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation.	Yes, if the financial entity notifying the significant cyber threat is different from the entity submitting the report	Unique alphanumeric 20 character code, based on ISO 17442-1:2020

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
6. Primary contact person name	Name and surname of the primary contact person of the financial entity.	Yes	Alphanumeric
7. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Yes	Alphanumeric (
8. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX)	Yes	Alphanumeric
9. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity, where available.	Yes, if name and surname of the second contact person of the financial entity or an entity submitting the notification for the financial entity is available.	Alphanumeric
10. Second contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication, where available.	Yes, if email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication is available.	Alphanumeric
11. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication, where available. Telephone number shall be reported with all international prefixes (e.g. +33XXXXXXXXX).	Yes, if telephone number of the second contact person that can be used by the competent authority for follow-up communication is available.	Alphanumeric



APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
12. Date and time of detection of the cyber threat	Date and time at which the financial entity has become aware of the significant cyber threat.	Yes	ISO 8601 standard UTC (YYYY- MM-DD Thh: mm:ss)
13. Description of the significant cyber threat	<p>Description of the most relevant aspects of the significant cyber threat.</p> <p>Financial entities shall provide:</p> <ul style="list-style-type: none"> <li>- a high-level overview of the most relevant aspects of the significant cyber threat;</li> <li>- the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited;</li> <li>- information about the probability of materialisation of the significant cyber threat;</li> </ul> <p>and</p> <ul style="list-style-type: none"> <li>- Information about the source of information about the cyber threat.</li> </ul>	Yes	Alphanumeric
14. Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts if the cyber threat has materialised	Yes	Alphanumeric
15. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materialised.	Yes	<p>Choice (multiple):</p> <ul style="list-style-type: none"> <li>- Clients, financial counterparts and transactions affected</li> <li>- Reputational impact</li> <li>- Duration and service downtime</li> <li>- Geographical spread</li> <li>- Data losses</li> <li>- Critical services affected</li> <li>- Economic impact</li> </ul>
16. Status of the cyber threat	<p>Information about the status of the cyber threat for the financial entity and whether there have been any changes in the threat activity.</p> <p>Where the cyber threat has stopped communicating with the financial entity's information systems, the status can be marked as inactive. If the financial entity</p>	Yes	<p>Choice:</p> <ul style="list-style-type: none"> <li>- active</li> <li>- inactive</li> </ul>

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
	has information that the threat remains active against other parties or the financial system as a whole, the status should be marked as active.		
17. Actions taken to prevent materialisation	High-level information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.	Yes	a) Alphanumeric
18. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities.	Yes, if other financial entities or authorities have been informed about the cyber threat).	Alphanumeric
19. Indicators of compromise	<p>Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.</p> <p>The IoC provided by the financial entity may include, but not be limited to, the following categories of data:</p> <ul style="list-style-type: none"> <li>• IP addresses;</li> <li>• URL addresses;</li> <li>• Domains;</li> <li>• File hashes;</li> <li>• Malware data (malware name, file names and their locations, specific registry keys associated with malware activity);</li> <li>• Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic);</li> <li>• E-mail message data (sender, recipient, subject, header, content);</li> <li>• DNS requests and registry configurations;</li> <li>• User account activities (logins, privileged user account activity, privilege escalation);</li> <li>• • Database traffic (read/write), requests to the same file.</li> </ul> <p>In practice, this type of information may include data relating to, for example,</p>	Yes, if information about indicators of compromise connected with the cyber threat are available.)	Alphanumeric

APPENDIX VII: RTS AND ITS ON THE CONTENT, FORMAT, TEMPLATES AND TIMELINES FOR REPORTING MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS

Data field	Description	Mandatory field	Field type
	indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to “command and control” servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc.		
20. Other relevant information	Any other relevant information about the significant cyber threat	Yes, if applicable and if there is other information available, not covered in the template.	Alphanumeric

## **APPENDIX VIII: RTS on subcontracting of critical or important functions**

[Art. 30(5)]

The ESAs indicated in their press release of 17 July 2024 that these RTS will be published in due course.

## APPENDIX IX: RTS on harmonisation of conditions enabling the conduct of the oversight activities

[\(JC 2024 35 – 17 July 2024\)](#)

[Art. 41]

COMMISSION DELEGATED REGULATION (EU) .../...

of **DD Month YYYY**

**supplementing Regulation 2022/2554 of the European Parliament and of the Council with regard to  
regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight  
activities**

(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) 2016/10111<sup>74</sup>, and in particular Article 41(2), second subparagraph, thereof,

Whereas:

- (1) The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 introduces a Union oversight framework for the information and communication technology (ICT) third-party service providers to the financial sector designated as critical in accordance with Article 31 of that Regulation.
- (2) Considering that Article 31(11) of Regulation (EU) 2022/2554 grants a limited time period of 6 months from the receipt of the application, it is crucial that the European Banking Authority, European Insurance and Occupational Pensions Authority, and European Securities and Markets Authority (collectively European Supervisory Authorities or ESAs), receive a voluntary request to be designated as critical from a ICT third-party service provider, that is complete. In case the application submitted is not complete, the relevant ESA should reject the application and request the missing information.
- (3) Regulation (EU) 2022/2554 mandates the Lead Overseer to carry out a comprehensive assessment of the ICT risks that ICT third party service providers pose to financial entities. In order to carry out this assessment, Regulation (EU) 2022/2554 equips the Lead Overseer with power to request information covering areas directly or indirectly related to the ICT services the critical ICT third-party service providers provide to the financial entities.

---

<sup>74</sup> OJ L 333, 27.12.2022, p. 1.

## APPENDIX IX: RTS ON HARMONISATION OF CONDITIONS ENABLING THE CONDUCT OF THE OVERSIGHT ACTIVITIES

---

- (4) The request to critical ICT third-party service providers to transmit to the Lead Overseer information that is necessary to carry out its duties, including the one on subcontracting arrangements, should be done considering the second subparagraph of Article 33(2) of Regulation (EU) 2022/2554.
- (5) The legal identification of ICT third-party service providers within the scope of this Regulatory Technical Standards should be aligned with the identification code set out in Commission Implementing Regulation adopted in accordance with Article 28(9) from Regulation (EU) 2022/2554.
- (6) As a follow-up to the recommendations issued by the Lead Overseer to critical ICT third-party providers, the Lead Overseer should monitor critical ICT third party service providers' compliance with the recommendations. With a view to ensure a level playing field and an efficient and effective monitoring of the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to these recommendations, the Lead Overseer should be able to require the reports referred to in Article 35(1), point (c), of Regulation (EU) 2022/2554, which should be intended as interim progress reports and final reports.
- (7) Also for the purpose of assessment specified in Article 42(2) of Regulation (EU) 2022/2554, according to which Lead Overseer is obliged to evaluate whether explanation provided by critical ICT third-party provider is sufficient, the notification to the Lead Overseer by the critical ICT third-party service provider of its intention to follow the recommendations received should be complemented by such explanation in the form of a remediation plan. In such remediation plan the critical ICT third-party service provider describes the actions and the measures planned to mitigate the risks of the recommendations, along with their respective timelines.
- (8) As the information submitted to the Lead Overseer by critical ICT third-party service providers may be of confidential nature, the Lead Overseer should provide the critical ICT third-party service provider with secure electronic channels for information submission.
- (9) The critical ICT third-party service provider should always provide information in a clear, concise and complete manner. Considering the unified nature of the European oversight framework, information should be submitted, disclosed or reported by the ICT third-party service providers pursuant to Article 35(1) in English.
- (10) As the Lead Overseer is expected to assess the subcontracting arrangements of the critical ICT third-party service provider, a template needs to be developed for providing information on those arrangements. The template should take into account the fact that the critical ICT third-party service providers have different structures than financial entities. The templates should therefore not fully mirror the templates of the register of information referred to in Article 28(3) of Regulation (EU) 2022/2554.
- (11) Once the recommendations to a critical ICT third-party service provider are issued by the Lead Overseer, and competent authorities have informed the relevant financial entities of the risks identified in that recommendations, the Lead Overseer should monitor and assess the implementation by the critical ICT third-party service provider of the actions and remedies to comply with the recommendations. Competent authorities should monitor and assess the extent to which the financial entities are exposed to the risks identified in these recommendations. With a view to maintain a level playing field while carrying out their respective tasks, particularly when the risks identified in the recommendations are severe and shared among a large number of financial entities in multiple Member States, both the competent authorities and the Lead Overseer should share among each other relevant findings which are necessary for them to carry out their respective tasks. The objective of the information sharing is to ensure that the feedback of the Lead Overseer to the critical ICT third-party provider in relation to the actions and remedies the latter is implementing takes into account the impact on the risks of the financial entities, and that the supervisory

---

activities performed by the competent authorities are informed by the assessment carried out by the Lead Overseer.

- (12) To allow for an efficient and effective sharing of information, the competent authorities should assess, as part of their supervisory activities, the extent to which the financial entities supervised by them are exposed to the risks identified in the recommendations. This assessment should be carried out in a proportionate and risk-based manner. Lead Overseer should request the competent authorities to share the results of this assessment in the specific cases when the risks associated with the recommendations are severe and shared among a large number of financial entities in multiple Member States. To make the best use of the resources of the competent authorities, when asking to provide the results of this assessment, the Lead Overseer should always take into account that the objective of these requests is to evaluate the actions and remedies of the critical ICT third-party providers.
- (13) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities.
- (14) The Joint Committee of the European Supervisory Authorities has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council<sup>75</sup>, the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>76</sup>, and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>77</sup>.

HAS ADOPTED THIS REGULATION:

#### CHAPTER I

### **INFORMATION TO BE PROVIDED BY ICT THIRD-PARTY SERVICE PROVIDERS IN THE APPLICATION FOR A VOLUNTARY REQUEST TO BE DESIGNATED AS CRITICAL**

#### *Article 1*

#### **Information to be provided by ICT third-party service provider in the application for a voluntary request to be designated as critical**

1. For the purpose of Article 31(11) of Regulation (EU) 2022/2554, the information to be provided by an ICT third-party service provider in the reasoned application for a voluntary request to be designated as critical in accordance with Article 31(1), point (a), of Regulation (EU) 2022/2554 shall include all of the following
- (a) name of the legal entity;
  - (b) legal entity identification code;

---

<sup>75</sup> 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).

<sup>76</sup> 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).

<sup>77</sup> 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).

## APPENDIX IX: RTS ON HARMONISATION OF CONDITIONS ENABLING THE CONDUCT OF THE OVERSIGHT ACTIVITIES

---

- (c) country where the legal entity has registered office
- (d) description of the corporate structure including at least the following information on its parent company and other related undertakings to the applicant ICT third-party service providers providing ICT services to Union financial entities, where applicable;
  - (i) name of the legal entities;
  - (ii) legal entity identification code,;
  - (iii) country where the legal entity has registered office
- (e) an estimation of the market share of the ICT third-party service provider in the Union financial sector and estimation of market share per type of financial entity as referred to in Article 2(1) of Regulation (EU) 2022/2554 as of the year of application and the year before application;
- (f) a clear description of each ICT service provided by the ICT third-party service provider to Union financial entities including:
  - (i) a description of the nature of business and the type of ICT services provided to financial entities;
  - (ii) a list of the functions of financial entities supported by the ICT services provided, where available;
  - (iii) information whether the ICT services provided to financial entities support critical or important functions, where available;
- (g) a list of financial entities that make use of the ICT services provided by the ICT third-party service provider, including the following information for each of the financial entity serviced, where available:
  - (i) name of the legal entity;
  - (ii) legal entity identification code, where known to the ICT third-party service provider;
  - (iii) type of financial entity as specified in Article 2(1) of Regulation 2022/2554;
  - (iv) the geographic location of the legal entity, from which ICT services are provided, where available;
- (h) a list of the critical ICT third-party service providers included in the latest available list of such providers published by the ESAs pursuant to Article 31(9) of Regulation (EU) 2022/2554 that rely on the services provided by the applicant ICT third-party service provider, where available;
- (i) a self-assessment by the ICT third-party service provider including the following:
  - (i) the degree of substitutability for each ICT service provided by the ICT third-party service provider considering:
    1. the market share of the ICT third-party service provider in the EU financial sector;
    2. the number of known relevant competitors per type of ICT services, or group of ICT services;
    3. description of specificities relating to the ICT services offered, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;
  - (ii) knowledge about the availability of the alternative ICT third-party service providers to provide the same ICT services as the ICT third-party service provider submitting the application;



- (j) information on future strategy and investment plans in relation to the provision of ICT services and infrastructure to financial entities in the Union, including any planned changes in the group or management structure, entry into new markets or activities;
  - (k) information on subcontractors which have been designated as critical ICT third-party service providers pursuant to Article 31(1), point (a), of Regulation (EU) 2022/2554
  - (l) other reasons relevant for the ICT third-party service provider's application to be designated as critical
2. Where the ICT third-party service provider belongs to a group, the information referred to in paragraph 1 shall be provided in relation to the ICT services provided by the group as a whole.
3. As part of their review of the application received from the ICT third-party service provider, the ESAs may request clarifications of the information submitted.

*Article 2*

**Assessment of completeness of application**

1. The ICT third-party service provider shall submit its complete reasoned application, which contains all information necessary for the purpose of designation as critical in Article 1 of this Regulation, to the relevant ESA, via means determined by the ESAs.
2. Where the relevant ESA considers that information provided in the application is incomplete, it shall reject the application and request the missing information.

CHAPTER II

**INFORMATION FROM CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS TO THE LEAD OVERSEER**

*Article 3*

**Content of information provided by critical ICT third-party service providers**

1. Critical ICT third-party service providers shall provide to the Lead Overseer, upon its request, any information deemed necessary by the Lead Overseer to carry out its oversight duties in accordance with the requirements of Regulation (EU) 2022/2554. Critical ICT third-party service providers shall transmit this information according to the structure and format described in Article 5 of this Regulation, within the time limits and with the frequency set by the Lead Overseer.
2. Without prejudice to paragraph 1, upon Lead Overseer request, the critical ICT third-party service provider shall submit all of the following information:
- (a) information about the arrangements, and copies of contractual documents, between:
    - (i) the critical ICT third-party service provider and the financial entities as defined in Article 2(2) of Regulation (EU) 2022/2554;
    - (ii) the critical ICT third-party service provider and its subcontractors with a view to capture the entire technological value chain that effectively underpins the ICT services provided to the financial entities in the Union;
  - (b) information about the organisational and group structure of the critical ICT third-party service provider, including identification of all entities belonging to the same group that directly or indirectly provide ICT services to financial entities in the Union;

## APPENDIX IX: RTS ON HARMONISATION OF CONDITIONS ENABLING THE CONDUCT OF THE OVERSIGHT ACTIVITIES

---

- (c) information about the major shareholders, including their structure and geographical spread, of the entities that:
  - (i) without prejudice to Article 3(2), point (b), of this Regulation, hold, solely or jointly with their linked entities, 25% or more of the capital or voting rights of the critical ICT third-party service provider;
  - (ii) hold the right to appoint or remove a majority of the members of the administrative, management, or supervisory body of the critical ICT third-party service provider; or
  - (iii) control, pursuant to an agreement, a majority of shareholders' or members' voting rights in the critical ICT third-party service provider;
- (d) information about the critical ICT third-party service provider's own estimation of its market share, per type of services, in the relevant markets where it operates;
- (e) information about the internal governance arrangements of the critical ICT third-party service provider, including the structure with lines of governance responsibility and accountability rules;
- (f) the meeting minutes of the critical ICT third-party service provider's management body and any other internal relevant committees, which relate in any way to activities and risks concerning ICT third-party services supporting functions of financial entities within the Union;
- (g) information about the ICT security and data protection frameworks, including personal and non-personal data, of the critical ICT third party service provider, including relevant strategies, objectives, policies, procedures, protocols, processes, control measures to protect sensitive data, access controls, encryption practices, incident response plans, and compliance with all relevant regulations and national and international standards where applicable;
- (h) information about the mechanisms the critical ICT third-party service provider offers to the Union financial entities for data portability, application portability and interoperability;
- (i) information about the exact location of the data centres and ICT production centres used in any way for the purposes of providing services to the financial entities, including a list of all relevant premises and facilities of the critical ICT third-party service provider, including outside the Union;
- (j) information about provision of services by the critical ICT third-party service provider from third countries, including information on relevant legal provisions applicable to personal and non-personal data processed by the ICT third-party provider in different jurisdictions;
- (k) information about measures taken to address risks arising from the provision of ICT services by the critical ICT third-party service provider and their subcontractors from third-countries;
- (l) information about the risk management framework and the incident management framework, including policies, procedures, tools, mechanisms, and governance arrangements of the critical ICT third-party service provider and of its subcontractors. Information shall also include list and description of major incidents with direct or indirect impact on financial entities within the Union, including relevant details to determine the significance of the incident on financial entities and assess possible cross-border impacts. Information about the change management framework, including policies, procedures, and controls of the critical ICT third-party service provider and its subcontractors
- (m) information about the overall response and recovery framework of the critical ICT third-party service provider, including business continuity plans and related arrangements and procedures, software development lifecycle policy, response and recovery plans and related arrangements and procedures, backup policies arrangements and procedures;
- (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with

---

agreed-upon service level agreements (SLAs) and service level objectives (SLOs) or similar arrangements between critical ICT third-party service providers and financial entities in the Union;

- (o) information about the ICT third-party management framework of the critical ICT third-party service provider, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk assessment performed by the critical ICT third-party service provider on its subcontractors before entering into an agreement with them and to monitor the relationship covering all relevant ICT and counterparty risks;
- (p) extractions from the monitoring and scanning systems of the critical ICT third-party service provider and of its subcontractors, covering but not limited to network monitoring, server monitoring, application monitoring, security monitoring, vulnerability scanning, log management, performance monitoring and measurements against reliability goals, such as Service Level Objectives;
- (q) extractions from any production, pre-production and test system or application used by the critical ICT third-party service provider and its subcontractors, to provide directly or indirectly services to financial entities in the Union;
- (r) compliance and audit reports as well as any relevant audit findings, including audits performed by national authorities in the Union and outside the Union where cooperation agreements with the relevant authorities provide for such information exchange, or certifications achieved by the critical ICT third-party service provider or its subcontractors, including reports from internal and external auditors, certifications, or compliance assessments with industry-specific standards. This includes information about any type of independent testing of the resilience of the ICT systems of the critical ICT third-party service provider, including any type of threat led penetration testing carried out by the ICT third-party service provider;
- (s) information about any assessments carried out by the critical ICT third-party service provider upon its request or on its behalf evaluating the suitability and integrity of individuals holding key positions within the critical ICT third-party service provider;
- (t) information about the remediation plan to address recommendations according to Article 4 of this Regulation, and relevant related information to confirm remedies have been implemented;
- (u) information about employee training schemes and security awareness programs, which shall include information about the investments, resources and methods of the critical ICT third-party service provider in training its staff to handle sensitive financial data and maintain high levels of security;
- (v) information about the activities of the critical ICT third-party service provider and financial statements, including information on the budget and resources related to ICT and security.

*Article 4*

**Information from critical ICT third-party providers after the issuance of recommendations**

1. In accordance with Article 35(1), point (c), of Regulation (EU) 2022/2554 and as part of the notification to the Lead Overseer of its intention to comply with the recommendations pursuant to Article 42(1) of that Regulation, the critical ICT third-party service provider shall provide to the Lead Overseer a remediation plan outlining the actions and remedies that the critical ICT third-party service provider plans to implement in order to mitigate the risks identified in the recommendations. The remediation plan shall be consistent with the timeline set by the Lead Overseer for each recommendation.
2. To enable the monitoring of the implementation of the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider in relation to the recommendations received, the critical ICT third-party service provider shall share with the Lead Overseer upon request:
  - (i) interim progress reports and related supporting documents specifying the progress of the implementation of the actions and measures set out in the remediation plan provided by the critical ICT third party provider to the Lead Overseer within the timeline defined by the Lead Overseer;

- (ii) final reports and related supporting documents specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider in order to mitigate the risks identified in the recommendations received.

*Article 5*

**Structure and format of information provided by critical ICT third-party service providers**

1. The critical ICT third-party service provider shall provide the requested information to the Lead Overseer through the dedicated secure electronic channels indicated by the Lead Overseer in its request.
2. When providing information to the Lead Overseer, the critical ICT third-party providers shall:
  - (a) follow the structure indicated by the Lead Overseer in its information request;
  - (b) clearly locate the relevant piece of information in the submitted documentation
3. Information submitted, disclosed or reported to the Lead Overseer by the critical ICT third-party service provider shall be in English

*Article 6*

**Information on subcontracting arrangements provided by critical ICT third-party service providers**

A critical ICT third-party service provider which is required to share information on subcontracting arrangements shall provide the information according to the structure and the template set out in Annex I of this Regulation.

CHAPTER III

**COMPETENT AUTHORITIES' ASSESSMENT OF THE MEASURES TAKEN BY CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS BASED ON RECOMMENDATIONS OF THE LEAD OVERSEER**

*Article 7*

**Competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer**

1. As part of their supervision of financial entities, competent authorities shall assess the impact on the financial entities of the measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer. This assessment shall reflect a risk-based approach and the principle of proportionality.
2. When conducting the assessment referred to in paragraph 1, competent authorities shall take into account all of the following:
  - (a) the adequacy and the coherence of the corrective and remedial measures implemented by the financial entities under their remit to mitigate those risks, if any;
  - (b) the assessment made by the Lead Overseer of the compliance with the measures and actions included in the remediation plan by the critical ICT third-party service provider where it has impacts on the exposure of the financial entities under their remit to the risks identified in the recommendations;
  - (c) the view of competent authorities designated or established in accordance with Directive (EU) 2022/2555, where those competent authorities have been consulted in accordance with Article 42(5) of Regulation (EU) 2022/2554;

(d) whether the Lead Overseer has considered the actions and remedies implemented by the critical ICT third-party service provider as adequate to mitigate the exposure of the financial entities under their remit to the risks identified in the in recommendations.

3. Upon request from the Lead Overseer, the competent authority shall provide in reasonable time the results of the assessment set out in paragraph 1. When requesting the results of this assessment, the Lead Overseer shall consider the principle of proportionality and the magnitude of risks associated with the recommendation, including the cross-border impacts of these risks when impacting financial entities operating in more than one Member State.

4. Where relevant, competent authorities shall request to financial entities any information necessary to carry out the assessment specified in paragraph 1.

## CHAPTER IV

### FINAL PROVISIONS

#### *Article 8*

#### **Entry into force**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 17 January 2025. This Regulation shall be binding in its entirety and directly applicable in all Member States.

**ANNEX I**

**Template for sharing information on subcontracting arrangements**

Information Category	Key Information Elements
General Information	<ul style="list-style-type: none"> <li>• Name of the critical ICT third-party service provider</li> <li>• Identification code of the critical ICT third-party service provider</li> <li>• Name of contact person and contact details of the critical ICT third-party service provider</li> <li>• Date of sharing the information</li> </ul>
Overview of Subcontracting Arrangements	<ul style="list-style-type: none"> <li>• Mapping of the subcontracting arrangements, including a short description of the purpose and scope of the subcontracting relationships (including an indication on the level of criticality or importance of the subcontracting arrangements for the critical ICT third-party provider)</li> <li>• Specification and description of the types of ICT services subcontracted and their significance to the ICT services provided to financial entities, in line with *ITS to establish the templates composing the register of information*.</li> <li>• When specifying the types of ICT services, please refer to the list in Annex IV of the *ITS to establish the templates composing the register of information*</li> </ul>
Subcontractors' Information	<ul style="list-style-type: none"> <li>• Name and legal entity details (including identification code) of each subcontractor involved</li> <li>• Contact information of key staff responsible for each of the subcontracting relationships in the critical ICT third-party provider management structure</li> <li>• Overview for each subcontractor of the expertise, experience and qualifications related to the contracted ICT services</li> </ul>
Description of Services Provided by Subcontractors	<ul style="list-style-type: none"> <li>• Detailed description of the specific ICT services provided by each subcontractor</li> <li>• Breakdown of the responsibilities and tasks allocated to subcontractors</li> <li>• Information on the level of access subcontractors have to sensitive data or systems regarding the ICT services provided to financial entities</li> <li>• Information on the sites from which the services of subcontractors are provided and on the measures taken to address risks arising from services provided outside the Union</li> </ul>
Subcontracting Governance and Oversight	<ul style="list-style-type: none"> <li>• Description of the contractual and governance framework in place to manage subcontracting relationships, including clauses restricting the usage of sensitive data</li> </ul>

APPENDIX IX: RTS ON HARMONISATION OF CONDITIONS ENABLING THE CONDUCT OF THE  
OVERSIGHT ACTIVITIES

Information Category	Key Information Elements
	<ul style="list-style-type: none"> <li>• Explanation of the processes for selecting, engaging and monitoring subcontractors</li> <li>• Overview of performance metrics, service level objectives and agreements, and key performance indicators used to assess subcontractors' performance and reliability monitoring</li> </ul>
Risk Management and Compliance	<ul style="list-style-type: none"> <li>• Assessment of the subcontractors' risk profiles and potential impact on the ICT services provided to financial entities</li> <li>• Explanation of the risk mitigation measures implemented to address subcontracting-related risks</li> <li>• Details of subcontractors' compliance with relevant regulations, data protection requirements and industry standards</li> </ul>
Business Continuity and Contingency Planning	<ul style="list-style-type: none"> <li>• Overview of the subcontractors' business continuity and response and recovery plans</li> <li>• Description of the arrangements in place to ensure service continuity in case of disruptions or termination by the subcontractor</li> <li>• Frequency of tests of the business continuity plans and response and recovery plans by the subcontractors, dates of the latest tests over the past 3 years, and specification if the critical ICT third-party service provider has been involved in those tests</li> </ul>
Reporting	<ul style="list-style-type: none"> <li>• Description of the reporting mechanisms and frequency of reporting between the critical ICT third-party service provider and its subcontractors</li> </ul>
Remediation and Incident Management	<ul style="list-style-type: none"> <li>• Outline of the procedures for addressing subcontractor-related incidents, breaches or non-compliance</li> </ul>
Certifications and Audits	<ul style="list-style-type: none"> <li>• Information on any certifications, independent audits or assessments conducted on subcontractors to validate their security controls, quality standards or regulatory compliance</li> <li>• Date and frequency of the audits of the subcontractors conducted by the critical ICT third-party service provider</li> </ul>

## **APPENDIX X: RTS specifying the criteria for determining the composition of the joint examination team (JET)**

[\(JC 2024 54 – 17 July 2024\)](#)

**COMMISSION DELEGATED REGULATION (EU) .../...**

**of DD Month YYYY**

**supplementing Regulation 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards to specify the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements**

**(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<sup>78</sup>, and in particular Article 41(2), second subparagraph, thereof, Whereas;

- (1) The oversight framework established by Regulation (EU) 2022/2554 should be built on a structured and continuous cooperation between the European Supervisory Authorities (ESAs) and the competent authorities through the Oversight Forum and the joint examination teams.
- (2) After the designation of the critical information and communication technology (ICT) third-party service providers and taking into account the annual oversight plans for all critical ICT third-party service providers, the authorities listed in Article 40(2) of Regulation (EU) 2022/2554 should be asked to nominate their staff as member of the joint examination teams. These authorities should ensure that the nominated staff meet the specific technical expertise required in the profiles needed in the joint examination teams. The demonstration that an authority does not have staff meeting the specific technical expertise needed in the joint examination teams should be considered by the Lead Overseer as justification to discharge, at that point in time, the authorities of their obligation to nominate staff members to the joint examination teams. In that case, the authority should nevertheless commit on the best effort basis to address this shortfall of expertise and try to reinforce its capabilities to contribute to the joint examination teams in the context of the next exercise. The staff members designated as members of a joint examination team should continue to be employees of the nominating authority and therefore subject to working hours and permanent location of work as included in their employment contracts.
- (3) In order to ensure the most effective use of resources in the execution of oversight activities, a joint examination team should be able to oversee multiple critical ICT thirdparty service providers. The grouping of the critical ICT third-party service providers to be assigned to a specific joint examination team, and its overall staffing needs should take into account the risk profile of the critical ICT third-party service providers, and the envisaged level of intensity of oversight activities. This should result in a strategic multi-annual oversight plan, updated annually by the Lead Overseer to the extent necessary, and reflected into the individual annual oversight plan. To ensure the reliability of the planned and ongoing commitment of resource staffing of the joint examination teams by the nominating authorities, the Lead Overseer should consult both the joint oversight network and the Oversight Forum.

---

<sup>78</sup> OJ L 333, 27.12.2022, p. 1.



- (4) The Lead Overseer should apply a combination of criteria and principles when identifying the number of staff members in each joint examination team and the resulting composition. Those criteria and principles should take into account the technical nature of the oversight tasks, the different grade of dependency of financial entities on the services provided by the critical ICT third-party service providers, the geographical distribution, the size and the number of financial entities relying on those services and, where possible, a proportionate cross-sectoral representation. In performing this task, the Lead Overseer should rely on the information provided by competent authorities in the context of designation of the critical ICT third-party service providers, including the results of the calculation of all the sub-criteria as defined in Commission Delegated Regulation (EU) 2024/1502<sup>79</sup> and consider the criticality of the critical ICT third-party service providers for the provisioning of specific financial services both at Member State and Union level.
- (5) The Lead Overseer and the members of the joint examination teams should periodically assess the achievements of the joint examination teams to ensure that the structure and the composition of the joint examination teams are fit for purpose and continuously improving the efficiency and effectiveness of the Oversight Framework. The Lead Overseer and the nominating authorities should make use of these assessments to review the membership of the joint examination teams, when appropriate.
- (6) The ESAs should define the oversight procedures to be followed by the members of the joint examination teams and the Lead Overseer coordinator in the performance of their duties.
- (7) Since the oversight tasks involve the processing of confidential information, the Lead Overseer should grant members of the joint examination team access to such information and to the relating IT (e.g. tools, applications, datasets) and non-IT (e.g. policy, procedures, documentation) resources on a need-to-know basis and within the defined scope of their assignments if this is necessary for members of the joint examination team to assist the Lead Overseer in the fulfilment of its statutory functions or tasks.
- (8) When defining arrangements between the Lead Overseer and the competent authorities to implement this Regulation, consistently with the Commission Delegated Regulation (EU) 2024/1505 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid, the Lead Overseer should include in such arrangements a section detailing the procedure of reimbursement of the direct and indirect costs of all nominating authorities involved in the joint examination teams. The arrangements should also ensure that the members of the joint examination teams are free from any conflict of interests while performing their duties.
- (9) This Regulation is based on the draft regulatory technical standards submitted to the European Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority.
- (10) 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<sup>80</sup>, in Article 54 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>81</sup> and in Article 54 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>82</sup> 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

---

<sup>79</sup> Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers

<sup>80</sup> 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).

<sup>81</sup> 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).

<sup>82</sup> 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).

## APPENDIX X: RTS SPECIFYING THE CRITERIA FOR DETERMINING THE COMPOSITION OF THE JOINT EXAMINATION TEAM (JET)

---

Regulation (EU) No 1094/2010, and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010,

HAS ADOPTED THIS REGULATION:

### *Article 1*

#### **Tasks of the members of a joint examination team**

1. The joint examination team shall assist the Lead Overseer in conducting oversight activities, including the individual oversight plan adopted annually according to Article 33(4) of Regulation (EU) 2022/2554.
2. The tasks of the members of the joint examination team shall be performed under the coordination of the Lead Overseer coordinator and shall include any of the following:
  - (a) assisting the Lead Overseer in the preparation and drafting of the individual annual oversight plan describing the annual oversight objectives and the main oversight activities planned for each critical ICT third-party service provider that are to be carried out by the Lead Overseer and the joint examination team;
  - (b) assisting the Lead Overseer in performing the assessment referred to in Article 33(2) of Regulation (EU) 2022/2554;
  - (c) collecting and assessing the information submitted by the critical ICT thirdparty service provider according to Article 37 of Regulation (EU) 2022/2554 and Chapter II of Commission Delegated Regulation xxx [RTS on harmonisation of the conditions of oversight conduct];
  - (d) conducting general investigations on the critical ICT third-party service providers according to Article 38 of Regulation (EU) 2022/2554;
  - (e) conducting inspections of the critical ICT third-party service providers according to Article 39 of Regulation (EU) 2022/2554;
  - (f) drafting the recommendations addressed to the critical ICT third-party service provider as defined in Article 35(1), point (d) of Regulation (EU) 2022/2554;
  - (g) assessing the remediation plan and the progress reports as defined in Article 4 of Commission Delegated Regulation xxx [RTS on harmonisation of the conditions of oversight conduct];
  - (h) preparing and drafting the requests and decisions to the critical ICT third-party service provider referred to in Article 35(6), Article 37(1), Article 38(4), and Article 39(6) of Regulation (EU) 2022/2554;
  - (i) assisting the Lead Overseer in its contribution to horizontal oversight activities, including in the development of benchmarking, as referred to in Article 32(3) of Regulation (EU) 2022/2554;
  - (j) ensuring that the relevant information relating to financial entities making use of the services provided by the critical ICT third-party service providers are shared with the Lead Overseer;
  - (k) assisting the Lead Overseer in unplanned ad hoc activities deemed necessary by the Lead Overseer for the purpose of oversight.
3. In case the individual annual oversight plan is significantly revised during the year by the Lead Overseer, the Lead Overseer shall involve the joint examination team in the process of the revision and execution of the individual annual oversight plan according to point (a) of paragraph 2.

*Article 2*

**Establishment of a joint examination team**

1. After the first designation of the ICT third-party service provider as critical in accordance with Article 31(1) of Regulation (EU) 2022/2554, the Lead Overseer, in agreement with the joint oversight network, shall establish the joint examination team responsible to carry out the oversight activities concerning the assigned critical ICT third-party service provider.
2. When material changes regarding the critical ICT third-party service provider occur, the Lead Overseer may consider to update the composition of the joint examination team responsible to carry out the oversight activities concerning the assigned critical ICT third-party service provider.

For the purpose of this paragraph, material changes regarding the critical ICT thirdparty service provider relate to:

- (a) the services provided by critical ICT third-party service provider;
- (b) the activities performed by financial entities supported by ICT services of the critical ICT third-party service provider; or
- (c) the list of critical ICT third-party service providers at Union level referred in Article 31(9) or Regulation (EU) 2022/2554.

3. The Lead Overseer shall identify the number of members of the joint examination team and its composition according to Article 3(1), and depending on the envisaged level of intensity of oversight activities to be performed in relation to all critical ICT third-party service providers.
4. The authorities referred to in Article 40(2) of Regulation (EU) 2022/2554 shall nominate one or more individuals from their staff to be appointed as members of the joint examination team. An individual may be nominated and appointed as member of one or more joint examination teams.
5. The Lead Overseer shall appoint the nominated individuals as members of the joint examination team either on a full-time or on a part-time basis depending on their availability, the specific needs of the Lead Overseer, and the agreement between the nominating authority and the Lead Overseer.
6. When nominating the members of the joint examination teams, the authorities shall assess their technical expertise, qualifications and skills in ICT and relevant areas, including communication and collaboration skills, as well as audit and supervision skills.
7. The Lead Overseer may require the nominating authorities to modify their nominations only in justified circumstances and when the profiles of the nominated individuals do not match the profile of the resources needed.
8. The Lead Overseer and the authorities shall take all appropriate and possible measures to ensure the joint examination team is staffed adequately in accordance with the annual individual oversight plan.

*Article 3*

**Members of the joint examination team**

1. The Lead Overseer shall define the number of members of the joint examination team and its composition in agreement with the Joint Oversight Network and in consultation with the Oversight Forum, as part of the process of establishment of the joint examination team, and as required over time, taking into account the tasks included in the individual annual oversight plans drafted for each critical ICT third-party service provider overseen by the joint examination team. To define the number and the composition of members in the joint examination team, the Lead Overseer shall consider at least the following:

## APPENDIX X: RTS SPECIFYING THE CRITERIA FOR DETERMINING THE COMPOSITION OF THE JOINT EXAMINATION TEAM (JET)

---

- (i) the number of critical ICT third-party service providers overseen by the joint examination team and by the ESAs as Lead Overseers;
  - (ii) the specific individual oversight needs related to the specific critical ICT thirdparty service provider, as assessed by the Lead Overseer;
  - (iii) the stability of the composition of the joint examination team, ensuring a proper knowledge retention ;
  - (iv) the necessary skills required for the execution of the tasks by the joint examination team, considering the technical and non-technical ICT knowledge requirements;
  - (v) the Member States in which the critical ICT third-party service provider provides ICT services supporting critical or important functions of the financial entities, and the competent authorities which supervise the financial entities making use of those services;
  - (vi) the different types, sizes and number of financial entities to which the critical ICT third-party service provider provides ICT services supporting critical or important functions;
  - (vii) the competent authorities which supervise the financial entities which are the most dependent on the ICT services provided by the critical ICT third-party service providers;
  - (viii) a proportionate cross-sectoral representation of the nominating authorities of the joint examination team.
2. When nominating members of the joint examination team, the authorities referred to in Article 40(2) of Regulation (EU) 2022/2554 shall consider at least points (b), (c), (d), (f) and (g) of paragraph 1.
  3. The members of the joint examination team shall be involved either in the execution of specific tasks, or in the ongoing support of the activities carried out by the Lead Overseer, considering the tasks defined in Article 1(2) of this Regulation.

### *Article 4*

#### **Renewal of the membership in the joint examination team**

Periodically, or in cases where the appointed Lead Overseer changes, or in cases where material changes as defined in Article 2(2) occur, the Lead Overseer, after consulting the members of the joint examination team, shall assess the achievements of the joint examination team. The results of this assessment shall be used by both the nominating authorities and Lead Overseer to decide whether it is appropriate to renew the membership of the joint examination team.

### *Article 5*

#### **Working arrangements of the members of the joint examination team**

1. The members of the joint examination team shall carry out their tasks identified in the individual annual oversight plan with due skill, care and diligence without any bias and in accordance with the instructions of the Lead Overseer coordinator.
2. When carrying out oversight tasks, the members of the joint examination team shall follow oversight procedures drafted jointly by the European Supervisory Authorities in relation to the conduct of oversight activities and any relevant operational area, including but not limited to specifications relating to the use of IT tools and equipment, and time management.
3. The members of the joint examination team shall follow the information and data handling specifications and instructions as provided by the Lead Overseer coordinator and shall comply with the confidentiality regime of the European Supervisory Authorities.

4. The Lead Overseer and the nominating authorities shall establish arrangements to implement the requirements in this Regulation, including arrangements on the time spent and estimated costs related to the oversight activities performed by the joint examination team, training and ethical and conduct considerations in relation to the role of the member of the joint examination team, where appropriate.

5. The Lead Overseer and the nominating authorities shall ensure that the arrangements referred to in paragraph 4 are timely implemented, reviewed and kept up to date.

*Article 6*

**Entry into force**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from 17 January 2025.

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

## APPENDIX XI: RTS on threat-led penetration testing (TLPT)

[\(JC 2024 29 – 17 July 2024\)](#)

[Art. 26(11)]

### COMMISSION DELEGATED REGULATION (EU) .../...

of XXX

**supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition.**

**(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<sup>83</sup>, and in particular Article 26(11), fourth subparagraph thereof,

Whereas:

- (1) This Regulation has been drafted in accordance with the TIBER-EU framework and mirrors the methodology, process and structure of TLPT as described in TIBER-EU. Financial entities subject to TLPT may refer to and apply the TIBER-EU framework, or one of its national implementations, in as much as that framework or implementation is consistent with the requirements set out in Articles 26 and 27 of Regulation (EU) 2022/2554 and this Regulation.
- (2) The designation of a single public authority in the financial sector responsible for TLPT-related matters at national level according to Article 26(9) of Regulation (EU) 2022/2554 should be without prejudice to the competence for the TLPT of competent authorities entrusted with supervision at Union level of certain financial entities to which Regulation (EU) 2022/2554 applies, such as, for instance, the European Central Bank for significant credit institutions. Where only some tasks are delegated in a Member State in accordance with the national implementation of Article 26(10) of Regulation (EU) 2022/2554, the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554 should remain the authority for those TLPT-related tasks that have been not delegated.
- (3) Considering the complexity of the TLPT and the risks relating to it, the test should be performed only by financial entities for which it is justified. Hence, authorities responsible for TLPT matters (TLPT authorities, either at national or Union level) should exclude from the scope of TLPT those financial entities operating in core financial services subsectors for which a TLPT is not justified. It means that credit institutions, payment and electronic money institutions, central security depositories, central counterparties, trading venues, insurance and reinsurance undertakings, even though when meeting the quantitative criteria

---

<sup>83</sup> OJ L 333, 27.12.2022, p. 1.

identified in this Regulation, could be opted out of the TLPT scope in light of an overall assessment of their ICT risk profile and maturity, impact on the financial sector and related financial stability concerns.

- (4) TLPT authorities should assess, in light of an overall assessment of the ICT risk profile and maturity, of the impact on the financial sector and related financial stability concerns, whether any type of financial entity other than credit institutions, payment institutions, electronic money institutions, central counterparties, central securities depositories, trading venues, insurance and reinsurance undertakings should be subject to TLPT. The assessment of the abovementioned qualitative elements should aim at identifying financial entities for which the TLPT is appropriate by using cross-sector and objective indicators. At the same time, the assessment of these elements should limit the entities subject to TLPT to those for which the test is justified. These elements should also be assessed with reference to new market participants (such as crypto asset service providers referred to in Title V of Regulation (EU) 2023/1114) which might have a more important role for the financial sector in the future.
- (5) Where financial entities have the same ICT intra-group service provider or where they belong to the same group and rely on common ICT systems, it is important that TLPT authorities consider the structure and its systemic character or importance for the financial sector at national or Union level in the assessment of whether a financial entity should be subject to TLPT and of whether the TLPT should be conducted at entity level or at group level (through a joint TLPT).
- (6) In order to mirror the TIBER-EU framework, it is necessary that the testing methodology provides for the involvement of the following main participants: the financial entity, with a control team (mirroring the TIBER-EU so-called 'white team') and a blue team (mirroring the TIBER-EU 'blue team'), the TLPT authority, in the form of a TLPT cyber team (mirroring the TIBER-EU so-called 'TIBER cyber teams'), a threat intelligence provider and testers (the latter mirroring the TIBER so-called 'red team provider').
- (7) In order to ensure that the TLPT benefits from the experience developed in the framework of TIBER-EU implementation and to reduce the risks associated to the performance of TLPT, it should be ensured that the responsibilities of the TLPT cyber teams to be set up at the level of TLPT authorities match as closely as possible those of the TIBER cyber teams under TIBER-EU. Hence, the TLPT cyber teams should include test managers responsible for overseeing the individual TLPTs and be responsible for planning and coordination of individual tests. TLPT cyber teams should serve as single point of contact for test-related communication to internal and external stakeholders, collect and process feedback and lessons learned from previously conducted tests and provide support to financial entities undergoing TLPT testing.
- (8) To mirror the TIBER-EU framework methodology, test managers should have sufficient skills and capabilities to provide advice and challenge tester proposals. Building on the experience under the TIBER-EU framework, it has proven to be valuable to have a team of at least two test managers assigned to each test. To reflect that the TLPT is used to encourage the learning experience, to safeguard the confidentiality of tests, and unless they have resources or expertise issues, TLPT authorities are strongly encouraged to consider that, for the duration of a TLPT, test managers should not conduct supervisory activities on the same financial entity undergoing a TLPT.
- (9) It is important, for consistency with the TIBER-EU framework, that the TLPT authority closely follows the test in each of its stages. Considering the nature of the test and the risks associated to it, it is fundamental that the approach to be followed for each specific phase of the testing refers, where relevant, to the role of the TLPT authority. In particular, the TLPT authority should be consulted and should validate those assessments or decisions of the financial entities that may, on the one hand, have an effect on the effectiveness of the test and, on the other hand, have an impact on the risks associated with the test. Examples of the fundamental steps on which a specific involvement of the TLPT authority is necessary include the validation of certain fundamental documentation of the test, the selection of threat intelligence providers and testers and risk management measures. The involvement of the TLPT authority, with

particular reference to validations, should not result in an excessive burden for the authorities and should therefore be limited to those documentation and decisions directly affecting the positive outcome of the TLPT. The involvement of the TLPT authority as described in this Regulation is also necessary for the purposes of the issuance of the attestation pursuant to Article 26(7) of Regulation (EU) 2022/2554. Through the active participation to each phase of the testing the TLPT authorities may effectively assess compliance of the financial entities with the relevant requirements.

- (10) The secrecy of a TLPT is of utmost importance to ensure that the conditions of the test are realistic, therefore, testing should be covert, and precautions should be taken in order to keep the TLPT confidential, including the choice of codenames designed in such a way as not allowing the identification of the TLPT by third parties. Should staff members responsible for the security of the financial team be aware of a planned or ongoing TLPT, it is likely that they would be more observant and alert than during normal working conditions, thereby resulting in an altered outcome of the test. Therefore, staff members of the financial entity outside of the control team should be made aware of any planned or ongoing TLPT only in presence of cogent reasons and subject to prior agreement of the test managers. This may for example be to ensure the secrecy of the test in case a blue team member has detected the test.
- (11) As evidenced through the experience gathered in the TIBER-EU framework with respect to the 'white team', the selection of an adequate control team lead (CTL) is indispensable for the safe conduct of a TLPT. The CTL should have the necessary mandate within the financial entity to guide all the aspects of the test, without compromising the confidentiality of the test. Aspects such as deep knowledge of the financial entity, the CTL's job role and strategic positioning, seniority and access to the management board should be considered for the purposes of the appointment. The control team should be as small as possible in order to reduce the risk of compromising the TLPT.
- (12) There are inherent elements of risks associated with TLPT as critical functions are tested in live production environment, with the possibility of causing denial-of-service incidents, unexpected system crashes, damages to critical live production systems, or the loss, modification, or disclosure of data, highlights the need for robust risk management measures. Hence, it is very important that financial entities are at all points aware of the particular risks that arise in a TLPT and that these are mitigated, to ensure the TLPT is conducted in a controlled manner all along the test. In that respect, without prejudice to the internal processes of the financial entity and the responsibility and delegations already provided to the control team lead, information or, in particular cases, approval of the TLPT risk management measures by the financial entity's management body itself may be appropriate. It is also essential that the testers and threat intelligence providers have the highest level of skills and expertise and an appropriate experience in threat intelligence and TLPT in the financial services industry to be able to deliver effective and most qualified professional services and to reduce the abovementioned risks.
- (13) Intelligence-led red team tests differ from conventional penetration tests, which provide a detailed and useful assessment of technical and configuration vulnerabilities often of a single system or environment in isolation, but contrary to the former, do not assess the full scenario of a targeted attack against an entire entity, including the complete scope of its people, processes and technologies. During the selection process, financial entities should ensure that testers possess the requisite skills to perform intelligence-led red team tests, and not only penetration tests. This Regulation establishes comprehensive criteria for testers, both internal and external, and threat intelligence providers, always external. In case the threat intelligence provider and the external testers are part of the same company, the staff assigned to the test should be adequately separated. Acknowledging the evolving state of this market, there may be exceptional circumstances where financial entities are unable to secure suitable providers who meet these standards. Therefore, financial entities, upon evidencing the unavailability of fully compliant and suitable providers, should be permitted to engage those who do not satisfy all criteria, conditional upon the proper mitigation of any resultant additional risks and to an assessment of all these elements by TLPT authority.



- (14) When several financial entities and several TLPT authorities are involved in a TLPT, the roles of all parties in the TLPT process should be specified to conduct the most efficient and safe test. For the purposes of pooled testing, specific requirements are necessary to specify the role of the designated financial entity, and namely that it should be in charge of providing all necessary documentation to the lead TLPT authority and monitoring the test process. The designated financial entity should also be in charge of the common aspects of the risk management assessment. Notwithstanding the role of the designated financial entity, the obligations of each financial entity participating to the pooled TLPT process remain unaffected during the pooled test. The same principle is valid for joint TLPTs.
- (15) As evidenced by the experience of the implementations of the TIBER-EU framework, holding in-person or virtual meetings including all relevant stakeholders (financial entities, authorities, testers and threat intelligence providers) is the most efficient way to ensure the appropriate conduct of the test. Therefore in-person and virtual meetings are strongly encouraged and should be held at various steps of the process, and in particular: during the preparation phase at the launch of the TLPT and to finalise on its scope; during the testing phase, to finalise the threat intelligence report and the red team test plan and for the weekly updates; and during the closure phase, for the purposes of replaying testers and blue team actions, purple teaming and to exchange feedback on the TLPT.
- (16) In order to ensure the smooth performance of the TLPT, the TLPT authority should clearly present its expectations with respect to the test to the financial entity. In that respect, the test managers should ensure that an appropriate flow of information is established with the control team within the financial entity, with the testers and threat intelligence providers.
- (17) The financial entity should select the critical or important functions that will be in scope of the TLPT based on various criteria relating to the importance of the function for the financial entity itself and the financial sector, at national and at Union level, not only in economic terms but also considering for instance the symbolic or political status of the function. If the testers and threat intelligence provider are not involved during the scoping process, the control team should provide them with detailed information on the agreed scoping, to facilitate a smooth transition to the phase of threat intelligence gathering.
- (18) The threat intelligence provider should collect intelligence or information that cover at least two key areas of interest: the targets, by identifying potential attack surfaces across the financial entity, and the threats, by identifying relevant threat actors and probable threat scenarios in order to provide the testers with the information needed to simulate a real-life and realistic attack on the financial entity's live systems underpinning its critical or important functions. In order to ensure that the threat intelligence provider considers the relevant threats for the financial entity, the threat intelligence provider should exchange on the draft threat intelligence report and on the draft red team test plan with the testers, the control team and the test managers. The threat intelligence provider may take into account a generic threat landscape provided by the TLPT authority for the financial sector of a member state, if applicable, as a baseline for the national threat landscape. Based on the TIBER-EU framework application, the threat intelligence gathering process is typically lasting approximately four weeks.
- (19) It is essential that, prior to the red team testing phase of the TLPT, the testers receive detailed explanations on the targeted threat intelligence report and analysis of possible threat scenarios from the threat intelligence provider, to allow the tester to gain insight and further review the scope specification document and target threat intelligence report to finalise the red team test plan.
- (20) It is important that sufficient time be allocated to the active red team testing phase to allow testers to conduct a realistic and comprehensive test in which all attack phases are executed, and flags are reached. On the basis of the experience gathered with the TIBER-EU framework, the time allocated should be at least twelve weeks and be determined taking into account the number of parties involved, the TLPT scope, the

resources of the involved financial entity or entities, any external requirements and the availability of supporting information supplied by the financial entity.

- (21) During the active red team testing phase, the testers should deploy a range of tactics, techniques and procedures (TTPs) to adequately test the live production systems of the financial entity. The TTPs should include, as appropriate, reconnaissance (i.e. collecting as much information as possible on a target), weaponization (i.e. analysing information on the infrastructure, facilities and employees and preparing for the operations specific to the target), delivery (i.e. the active launch of the full operation on the target), exploitation (i.e. where the testers' goal is to compromise the servers, networks of the financial entity and exploit its staff through social engineering), control and movement (i.e. attempts to move from the compromise systems to further vulnerable or high value ones) and actions on target (i.e. gaining further access to compromise systems and acquiring access to the previously agreed target information and data, as previously agreed in the red team test plan).
- (22) While carrying out a TLPT, testers should act considering the time available to perform the attack, resources and ethical and legal boundaries. Should the testers be unable to progress to the programmed next stage of the attack, occasional assistance should be provided by the control team, upon agreement of the TLPT authority, in the form of 'leg-ups'. Leg-ups can broadly be categorized in information and access leg-ups and may for instance consist of the provision of access to ICT system or internal networks to continue with the test and focus on the following attack steps.
- (23) During the active red teaming in the testing phase, purple teaming activities should be used as a last resort in exceptional circumstances and once all alternative options have been exhausted. In the context of this limited purple teaming exercise, the following methods can be used: "catch-and-release", where testers attempt to continue the scenarios, get detected and then resume the testing again; "war gaming", which allows for more complex scenarios to test strategic decision making; or "collaborative proof-of-concept" which allows testers and blue team members to jointly validate specific security measures, tools, or techniques in a controlled and cooperative environment.
- (24) The TLPT should be used as a learning experience to enhance the digital operational resilience of financial entities. In that respect, the blue team and testers should replay the attack and review the steps taken in order to learn from the testing experience in collaboration with the testers. For this purpose and to allow for adequate preparation, the red team test report and the blue team test report should be made available to all parties involved in the replay activities, prior to conducting any replay activities. Additionally, a purple teaming exercise, in the closure phase, should be carried out to maximize the learning experience. Methods that may be used for purple teaming in the closure phase include discussions of alternative attack scenarios, exploration on live systems of alternative scenarios or the re-exploration of planned scenarios on live systems that the testers had been unable to complete or execute during the testing phase.
- (25) To further facilitate the learning experience of all parties involved in the TLPT, for the benefit of future tests and to further the digital operational resilience of financial entities parties concerned should provide feedback to each other on the overall process, and in particular identifying which activities progressed well or could have been improved, which aspects of the TLPT process worked well or could be improved.
- (26) Competent authorities referred to in Article 46 of Regulation (EU) 2022/2554 and TLPT authorities, where different, should work together to incorporate advanced testing by means of TLPT into the existing supervisory processes. In that respect it is appropriate that, especially, for the test summary report and remediation plans, a close cooperation between test managers who were involved in the TLPT and the responsible supervisors is established, in order to share the correct understanding of the TLPT findings and of how they should be interpreted.

- (27) Financial entities should ensure that, as required by Article 26(8), first subparagraph, of Regulation (EU) 2022/2554, every three tests they contract external testers. Where financial entities include in the team of testers both internal and external testers, this should be considered as a TLPT performed with internal testers for the purposes of Article 26(8), first subparagraph, of Regulation (EU) 2022/2554.
- (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, the European Securities and Markets Authority (European Supervisory Authorities), in agreement with the European Central Bank.
- (29) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council<sup>84</sup>, the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council<sup>85</sup> and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>86</sup>,

HAS ADOPTED THIS REGULATION:

## CHAPTER I

### GENERAL PROVISIONS

#### *Article 1*

#### **Definitions**

For the purposes of this Regulation, the following definitions shall apply:

- (1) ‘control team’ means the team composed of staff of the tested financial entity and, where relevant in consideration of the scope of the TLPT, staff of its third-party service providers and any other party, who manages the test.
- (2) ‘control team lead’ means the staff member of the financial entity responsible for the conduct of all TLPT-related activities for the financial entity in the context of a given test;
- (3) ‘blue team’ means the staff of the financial entity and, where relevant, staff of the financial entity’s third-party service providers and any other party deemed relevant in consideration of the scope of the TLPT, of the financial entity’s third-party service providers, that are defending a financial entity’s use of network and information systems by maintaining its security posture against simulated or real attacks and that is not aware of the TLPT;

---

<sup>84</sup> 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).

<sup>85</sup> 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).

<sup>86</sup> 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).

- (4) 'blue team tasks' means tasks that are typically carried out by the blue team such as security operation centre (SOC), ICT infrastructure services, helpdesk services, incident management services at operational level;
- (5) 'purple teaming' means a collaborative testing activity that involves both the testers and the blue team;
- (6) 'TLPT authority' means:
- (a) the single public authority in the financial sector designated in accordance with Article 26(9) of Regulation (EU) 2022/2554, or
- a. the authority in the financial sector to which the exercise of some or all of the tasks in relation to TLPT is delegated in accordance with Article 26(10) of Regulation (EU) 2022/2554, or
- b. the competent authority in accordance with Article 46 of Regulation (EU) 2022/2554;
- (7) 'TLPT Cyber Team' or 'TCT' means the staff within the TLPT authority(ies), that is responsible for TLPT-related matters;
- (8) 'test managers' means staff designated to lead the activities of the TLPT authority for a specific TLPT to monitor compliance with the requirements of this Regulation;
- (9) 'threat intelligence provider' means the expert(s), external to the financial entity and to ICT intra-group service providers if any, who collect and analyse targeted threat intelligence relevant for the financial entities in scope of a specific TLPT exercise and develop matching relevant and realistic threat scenarios;
- (10) 'leg-up' means the assistance or information provided by the control team to the testers to allow the testers to continue the execution of an attack path where they are not able to advance on their own, and where no other reasonable alternative exists, including for insufficient time or resources in a given TLPT;
- (11) 'attack path' means the route followed by testers during the active red team testing phase of the TLPT in order to reach the flags defined for that TLPT;
- (12) 'flags' are key objectives in the ICT systems supporting critical or important functions of a financial entity that the testers try to achieve through the test;
- (13) 'sensitive information' means information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the financial entity and its ecosystem would it fall in the hands of malicious actors;
- (14) 'pool' means all the financial entities participating in a pooled TLPT pursuant to Article 26(4) of Regulation (EU) 2022/2554;
- (15) 'host Member State' means host Member State in accordance with applicable sectoral legislation;
- (16) 'joint TLPT' means a TLPT, other than a pooled TLPT referred to in Article 26(4) of Regulation (EU) 2022/2554, involving several financial entities using the same ICT intra-group service provider, or belonging to the same group and using common ICT systems.

## CHAPTER II

**CRITERIA TO IDENTIFY FINANCIAL ENTITIES REQUIRED TO PERFORM TLPT***Article 2***Identification of financial entities required to perform TLPT**

1. TLPT authorities shall require all of the following financial entities to perform TLPT:
  - (a) Credit institutions identified as global systemically important institutions (G-SIIs) in accordance with Article 131 of Directive 2013/36/EU of the European Parliament and of the Council<sup>15</sup> or as other systemically important institutions (O-SIIs) or that are part of a G-SIIs or O-SIIs.
  - (b) Payment institutions, exceeding in each of the previous two financial years EUR 150 billion of total value of payment transactions as defined in point (5) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council<sup>16</sup>.
  - (c) Electronic money institutions, exceeding in each of the previous two financial years EUR 150 billion of total value of payment transactions as defined in point (5) of Article 4 of Directive (EU) 2015/2366 or EUR 40 billion of total value of the amount of outstanding electronic money.
  - (d) Central securities depositories;
  - (e) Central counterparties;
  - (f) Trading venues with an electronic trading system that meet at least one of the following criteria:
    - (i) the trading venue with the highest market share in terms of turnover at national level in each of the preceding two financial years in one or more of the following:
      - transferable securities as defined in point (44)(a) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council<sup>17</sup>;
      - transferable securities as defined in point (44)(b) of Article 4(1) of Directive 2014/65/EU;
      - derivatives as defined in Article 2(1)(29) of Regulation (EU) No 600/2014 of the European Parliament and of the Council<sup>18</sup>;
      - structured finance products as defined in Article 2(1)(28) of Regulation (EU) No 600/2014 ;
      - emission allowances as defined in point (11) of Section C of Annex I to Directive 2014/65/EU;
    - (ii) the trading venue whose market share in terms of turnover at Union level exceeds 5% in each of the preceding two financial years in one or more of the following:
      - transferable securities as defined in point (44)(a) of Article 4(1) of Directive 2014/65/EU<sup>19</sup>,
      - transferable securities as defined in point (44)(b) of Article 4(1) of directive Directive 2014/65/EU,
      - derivatives as defined in Article 2(1)(29) of Regulation (EU) No 600/2014,
      - structured finance products as defined in Article 2(1)(28) of Regulation (EU) No 600/2014;

- emission allowances as defined in point (11) of Section C of Annex I to Directive 2014/65/EU;

For the purposes of point (ii) of this point (f), where the trading venue is part of a group using common ICT systems or the same ICT intra-group service provider, the turnover of the securities and derivatives contracts on all trading venues pertaining to the same group and established in the Union shall be considered.

- (g) Insurance and reinsurance undertakings that meet all the following criteria:

- (i) gross written premium (GWP) exceeding EUR 1 500 000 000;
- (ii) technical provisions exceeding EUR 10 000 000 000;
- (iii) in case of life insurance undertakings, as referred to in Article 13, point (1), of Directive 2009/138/EC of the European Parliament and of the Council<sup>20</sup>, and of insurance undertakings pursuing both life and non-life activities, total assets exceeding 3.5% of the sum of the total assets valued according to Article 75 of Directive 2009/138/EC of the insurance and reinsurance undertakings established in the Member State.

TLPT authorities shall create a subset of all insurance and reinsurance undertakings by applying the criteria listed in the first subparagraph. Insurance and reinsurance undertakings included in this subset shall be required to perform TLPT where they also meet one or more of the following criteria:

- (i) gross written premium (GWP) exceeding EUR 3 000 000 000;
- (ii) technical provisions exceeding EUR 30 000 000 000;
- (iii) total assets exceeding 10% of the sum of the total assets valued according to Article 75 of Directive 2009/138/EC of the insurance and reinsurance undertakings established in the Member State.

2. Financial entities referred to in points (a) to (g) of paragraph 1 shall not be required to carry out TLPT where the assessment of the criteria listed in paragraph 4 indicates that the impact of the financial entity, financial stability concerns relating to it or its ICT risk profile do not justify the performance of the TLPT.

3. Where more than one financial entity belonging to the same group and using common ICT systems, or where more than one financial entity using the same ICT intra-group service provider meet the criteria set out in points (a) to (g) of paragraph 1, the TLPT authorities of these financial entities shall decide if the requirement to perform TLPT on an individual basis is relevant for these financial entities, in accordance with Article 14(2). Where the TLPT authority of the parent undertaking of such group is different from the TLPT authority(ies) of the financial entities referred to in the first subparagraph, it shall be consulted.

4. TLPT authorities shall assess whether any financial entities other than those referred to in paragraph 1 shall be required to perform TLPT, taking into account their impact, systemic character and ICT risk profile, assessed on the basis of all of the following criteria:

- (a) impact-related and systemic character related factors:
  - (i) the size of the financial entity, determined taking into account whether the financial entity provides financial services in the national or Union market and by comparing the activities of the financial entity to those of other financial entities providing similar services. Where possible, the TLPT authority shall consider the market share position at national and EU level, the range of activities offered by the financial entity and the market share of the services provided or of the activities undertaken at national and at Union level;

- (ii) the extent and nature of the interconnectedness of the financial entity with other financial entities in the financial sector at national and Union level;
  - (iii) the criticality or importance of the services provided to the financial sector;
  - (iv) the substitutability of the services provided by the financial entity;
  - (v) the complexity of the business model of the financial entity and the related services and processes. Where possible, the TLPT authority shall consider whether the financial entity operates more than one business models and the interconnectedness of different business processes and the related services;
  - (vi) whether the financial entity is part of a group of systemic character at Union or national level in the financial sector and using common ICT systems;
- (b) ICT risk related factors:
- (i) the risk profile of the financial entity;
  - (ii) the threat landscape of the financial entity;
  - (iii) the degree of dependence of critical or important functions or their supporting functions of the financial entity on ICT systems and processes;
  - (iv) the complexity of the ICT architecture of the financial entity;
  - (v) the ICT services and functions supported by ICT third-party service providers, the quantity and type of contractual arrangements with ICT third-party service providers or ICT intra-group service providers;
  - (vi) outcomes of any supervisory reviews relevant for the assessment of the ICT maturity of the financial entity;
  - (vii) the maturity of ICT business continuity plans and ICT response and recovery plans;
  - (viii) the maturity of the operational ICT security detection and mitigation measures including the ability to monitor the financial entity's ICT infrastructure on a permanent basis, to detect ICT-related events in real time, to analyse events, to respond to them in a timely and effective manner;
  - (ix) whether the financial entity is part of a group active in the financial sector at Union or national level and using common ICT systems.

### CHAPTER III

#### **REQUIREMENTS REGARDING TEST SCOPE, TESTING METHODOLOGY AND RESULTS OF TLPT**

##### Section I

#### **TESTING METHODOLOGY**

*Article 3*

**TCT and TLPT Test Managers**

1. A TLPT authority shall assign the responsibility for coordinating TLPT-related activities to a TCT. A TCT shall include test managers that are assigned to oversee an individual TLPT.
2. For each test, a test manager and at least one alternate shall be designated.
3. The test managers shall monitor and ensure that the requirements laid out in this Regulation are complied with.
4. The contact details of the TCT shall be communicated to the financial entity through the notification referred to in Article 8(1).
5. The TLPT authority shall participate to all the phases of the TLPT and shall endeavour to provide feedback, validations or approvals in a period of time adequate to expediently carry out the TLPT

*Article 4*

**Organisational arrangements for financial entities**

1. Financial entities shall appoint a control team lead who shall be responsible for the day-to-day management of the TLPT and the decisions and actions of the control team.
2. Financial entities shall establish organisational and procedural measures ensuring that:
  - (a) access to information pertaining to any planned or ongoing TLPT is limited on a need-to-know basis to the control team, the management body, the testers, the threat intelligence provider and the TLPT authority;
  - (b) the control team consults the test managers prior to involving any member of the blue team in a TLPT;
  - (c) the control team is informed of any detection of the TLPT by staff members of the financial entity or of its third-party service providers, where relevant, and the control team contains the escalation of the resulting incident response, where needed;
  - (d) arrangements relating to the secrecy of the TLPT, applicable to staff of the financial entity, to the staff of relevant ICT third party service providers, to testers and to the threat intelligence provider are in place;
  - (e) the control team provides any information pertaining to the TLPT to the test managers upon request;
  - (f) where possible, parties involved in the TLPT refer to it by code name only.

*Article 5*

**Risk management for TLPT**

1. During the preparation phase referred to in Article 8, the control team shall conduct an assessment of the risks associated with the testing of live production systems of critical or important functions of the financial entity, including potential impacts on the financial sector, as well as on financial stability at Union or national level, and shall review it throughout the conduct of the test.
2. The control team shall take measures to manage the risks referred to in paragraph 1 and in particular shall ensure that, for each TLPT:



- (a) the threat intelligence provider and external testers provide copies of certifications that are appropriate according to recognised market standards for the performance of their activities;
- (b) the threat intelligence provider and external tester are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence;
- (c) the threat intelligence provider provides at least three references from previous assignments in the context of penetration testing and red team testing;
- (d) the external testers provide at least five references from previous assignments related to penetration testing and red team testing;
- (e) the staff of the threat intelligence provider assigned to the TLPT shall:
  - i. be composed of at least a manager with at least five years of experience in threat intelligence as well as at least one additional member with at least two years of experience in threat intelligence;
  - ii. display a broad range and appropriate level of professional knowledge and skills including intelligence gathering tactics, techniques and procedures, geopolitical, technical and sectorial knowledge as well as adequate communication skills to clearly present and report on the result of the engagement.
  - iii. have a combined participation in at least three previous assignments in threat intelligence in the context of penetration testing and red team testing;
  - iv. not simultaneously perform any blue team tasks or other services that may present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in TLPT to which they are assigned;
  - v. be separated from and not reporting to staff of the same provider providing external testers for the same TLPT;
- (f) for external testers, the staff of the red team assigned to the TLPT shall:
  - i. be composed of at least a manager, with at least five years of experience in penetration testing and red team testing as well as at least two additional testers, each with penetration testing and red team testing of at least two years;
  - ii. display a broad range and appropriate level of professional knowledge and skills, including, knowledge about the business of the financial entity, reconnaissance, risk management, exploit development, physical penetration, social engineering, vulnerability analysis, as well as adequate communication skills to clearly present and report on the result of the engagement;
  - iii. have a combined participation in at least five previous assignments related to penetration testing and red team testing.;
  - iv. not be employed by, nor provide services to, a provider that simultaneously performs blue team tasks for a financial entity, ICT third-party service provider or an ICT intra-group service provider involved in the TLPT;
  - v. be separated from any staff of the same provider simultaneously providing threat-intelligence services for the same TLPT.
- (g) the testers and the threat intelligence provider shall carry out restoration procedures at the end of testing, including secure deletion of information related to passwords, credentials and other secret keys compromised during the TLPT, secure communication to the financial entities of the accounts compromised, secure collection, storage, management, and disposal of data collected;
- (h) in addition to the restoration procedures at the end of testing as referred to in point (g), testers shall carry out the following restoration procedures:

- i. command and control deactivation;
  - ii. scope and date kill switch(es);
  - iii. removal of backdoors and other malware;
  - iv. potential breach notification;
  - v. procedures for future back-up restoration which may contain malware or tools installed during the test;
  - vi. monitoring of the blue team activities and information to the control team of any possible detections; and
- (i) testers and the threat intelligence provider are prohibited from the following activities:
- i. unauthorised destruction of equipment of the financial entity and of its ICT third-party service providers, if any;
  - ii. uncontrolled modification of information and ICT assets of the financial entity and of its ICT third-party service providers, if any;
  - iii. intentionally compromising the continuity of critical or important functions of the financial entity;
  - iv. unauthorised inclusion of out-of-scope systems;
  - v. unauthorised disclosure of test results.
3. The control team shall keep record of the documentation provided by the testers and the threat intelligence providers to evidence compliance with the points (a) to (f) above, including detailed curriculum vitae of the staff of the external tester and of the threat intelligence provider employed for the TLPT.
- In exceptional circumstances, financial entities may contract external testers and threat intelligence providers that are not meeting one or more of the requirements listed in points (a) to (f) of paragraph 2, provided that they adopt appropriate measures to mitigate the risks relating to the lack of compliance with such points and record them.
4. In the performance of risk assessment and management, the control team shall at least consider the following types of risks related to:
- (a) granting access to threat intelligence provider and external testers, where applicable, to sensitive information and confidential information on the financial entity;
  - (b) lack of compliance of the TLPT with Regulation (EU) 2022/2554 and with this Regulation resulting in lack of the attestation referred to in Article 26(7) of Regulation (EU) 2022/2554, including where due to breaches of confidentiality on the TLPT or to lack of ethical conduct;
  - (c) crisis and incident escalation
  - (d) active red team phase, including risks related to interruption of critical activities and corruption of data due to the activities of the testers and potential impacts on third parties;
  - (e) blue team activity, including risks related to interruption of critical activities and corruption of data due to the activities of the blue team and potential impacts on third parties;
  - (f) incomplete restoration of systems affected by the TLPT.

*Article 6*

**Risk management for pooled and joint TLPTs**

1. In the case of a joint TLPT or a pooled TLPT, the control team of each financial entity shall conduct its own risk assessment and establish its own risk management measures.
2. The control team of the designated financial entity referred to in Article 14(3)(b) or in Article 26(4) of Regulation (EU) 2022/2554 shall consider, in conducting the risk assessment, aspects relating to the involvement in the TLPT of multiple financial entities. The control teams of the involved financial entities shall cooperate to identify potential joint risks.

Section II

**Testing Process**

*Article 7*

**Specificities for pooled and joint TLPTs**

1. Unless otherwise decided by the lead TLPT authority, where several financial entities, selected according to Article 14(2) or 14(4) are involved in a TLPT, each financial entity shall follow each of the steps described in Articles 8 to 13.
2. Unless otherwise provided in this Regulation, where several TLPT authorities are involved in a joint TLPT or in a pooled TLPT, references in Articles 8 to 13 to the “TLPT authority” shall be understood as a reference to the lead TLPT authority for such pooled or joint TLPT, as referred to in Article 14(3) or 14(5).

*Article 8*

**Preparation phase**

1. The financial entity shall submit to the test managers within three months from having received a notification from the TLPT authority that a TLPT shall be carried out, all of the following TLPT initiation documents:
  - (a) a project charter including a high-level project plan, containing the information set out in Annex I;
  - (b) the contact details of the control team lead;
  - (c) information on intended use of internal or external testers or both, where relevant as detailed in Article 13;
  - (d) information on the communication channels to be used during the TLPT;
  - (e) the code name for the TLPT.
2. Where the documents referred to in points (a) to (e) of paragraph 1 are complete and ensure the suitability and effective performance of the TLPT, the TLPT authority shall validate the TLPT initiation documents of the financial entity and notify the latter thereof.
3. Following the validation of the TLPT initiation documents by the TLPT authority, the financial entity shall set up a control team to support the control team lead in its tasks of:
  - (a) defining communications channels and processes within the control team, with the testers and the threat intelligence providers in all matters related to the TLPT;

- (b) informing the management body of the financial entity about the progress of the TLPT and the associated risks;
  - (c) taking decisions based on subject matter expertise throughout the TLPT;
  - (d) executing the TLPT in compliance with the requirements set out in this Regulation;
  - (e) selecting the threat intelligence provider for the TLPT;
  - (f) selecting the external testers, the internal testers or both; and
  - (g) preparing the scope specification document.
4. Where the TLPT authority considers that the initial composition of the control team and any subsequent changes to it are adequate for the performance of the tasks referred to in paragraph 3, the TLPT authority shall validate the control team and notify the control team lead thereof.
5. The financial entity shall submit a scope specification document containing all information set out in Annex II to the test managers within six months from the receipt of the notification from the TLPT authority referred to in paragraph 1. The scope specification document shall be approved by the management body of the financial entity.
6. Financial entities shall consider the following criteria for the inclusion of critical or important functions in the scope of the TLPT:
- (a) the criticality or importance of the function and its possible impact to the financial sector and on financial stability at national and Union level;
  - (b) the importance of the function for the day-to-day business operations of the financial entity;
  - (c) the exchangeability of the function;
  - (d) the interconnectedness with other functions;
  - (e) the geographical location of the function;
  - (f) the sectoral dependence of other entities on the function;
  - (g) where available, threat intelligence concerning the function.
7. The control team shall share the initiation documents and the scope specification document with the testers and threat intelligence providers once these are contracted. The control team shall inform the testers and threat intelligence providers about the testing process to be followed.
8. The financial entity shall ensure that the procurement or assignment of testers and threat intelligence providers is completed prior to the initiation of the testing phase.
9. Prior to the initiation of the testing phase, the control team shall consult the test managers on the TLPT risk assessment and on the risk management measures. The control team shall review the risk assessment or the risk management measures where the TLPT authority assesses that they do not adequately address the risks of the TLPT.
10. The control team shall assess the compliance of threat intelligence providers and testers they consider involving in the TLPT with the requirements laid out in Article 27 of Regulation (EU) 2022/2554 and with Article 5(2) of this Regulation and document the outcome of this assessment. The control team shall select provider(s) in accordance with this assessment and its risk management practices. Prior to contracting the selected threat

intelligence provider and external tester, the control team shall provide evidence of compliance to the test managers. The control team shall not proceed with contracting the selected threat intelligence provider and external testers where the TLPT authority assesses that the selected threat intelligence providers and external testers do not ensure compliance with, where appropriate, national security legislations or Article 5(2), or when the financial entity does not comply with Article 5(3), first subparagraph, or when the circumstances described in Article 5(3), second subparagraph, are not met.

11. Where the scope specification document is complete and ensures the performance of an appropriate and effective TLPT, the TLPT authority shall inform the control team lead of its validation thereof.

*Article 9*

**Testing phase: Threat intelligence**

1. Following approval of the scope specification document by the TLPT authority, the threat intelligence provider shall analyse generic and sector-specific threat intelligence relevant for the financial entity. The threat intelligence provider shall identify cyber threats and existing or potential vulnerabilities concerning the financial entity. Furthermore, the threat intelligence provider shall gather information on, and analyse concrete, actionable and contextualized target and threat intelligence concerning the financial entity, including through consulting the control team and the test managers.

2. The threat intelligence provider shall present the relevant threats and targeted threat intelligence, and propose appropriate scenarios to the control team, testers and test managers. The proposed scenarios shall differ with reference to the identified threat actors and associated tactics, techniques and procedures and shall target each and every critical or important functions in the scope of the TLPT.

3. The control team lead shall select at least three scenarios to conduct the TLPT, on the basis of all of the following elements:

- (a) the recommendation by the threat intelligence provider and the threat-led nature of each scenario;
- (b) the input provided by the test managers;
- (c) the feasibility of the proposed scenarios for execution, based on the expert judgement of the testers;
- (d) the size, complexity and overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations.

4. No more than one of the selected scenarios may be non-threat-led and may be based on a forward looking and potentially fictive threat with high predictive, anticipative, opportunistic or prospective value given the anticipated developments of the threat landscape concerning the financial entity.

For pooled TLPTs, without prejudice to the scenarios targeting directly the critical or important functions of the financial entities involved in the test, at least one scenario shall include the ICT third-party services provider's relevant underlying ICT systems, processes and technologies supporting the critical or important functions of the financial entities in scope.

Where the test is a joint TLPT involving an ICT intra-group service provider, without prejudice to the scenarios targeting directly the critical or important functions of the financial entities involved in the test, at least one scenario shall include the ICT intragroup services provider's relevant underlying ICT systems, processes and technologies supporting the critical or important functions of the financial entities in scope.

5. The threat intelligence provider shall provide the targeted threat intelligence report to the control team, including the scenarios selected according to paragraphs 2 to 4. The threat intelligence report shall include the information set out in Annex III.
6. The control team shall submit the targeted threat intelligence report to the test manager for approval. Where the targeted threat intelligence report is complete and ensure the performance of an effective TLPT, the TLPT authority shall inform the control team lead of its approval thereof.

*Article 10*

**Testing phase: Red Team Test**

1. Following approval of the targeted threat intelligence report by the TLPT authority, the testers shall prepare the red team test plan that shall include the information set out in Annex IV. The testers shall use the scope specification document and the targeted threat intelligence report as a basis for producing the attack scenarios.
2. The testers shall consult the control team, the threat intelligence provider and the test managers on the red team test plan, including the communication, procedural and project management arrangement, the preparation and use-cases for leg-up activation, and the reporting agreements to the control team and test managers.
3. The red team test plan shall be approved by the control team and TLPT authority. Where the red team test plan is complete and ensure the performance of an effective TLPT, the TLPT authority shall inform the control team lead of its approval.
4. Upon approval of the red team test plan in accordance with paragraph 3, the testers shall carry out the TLPT during the active red team testing phase.
5. The duration of the active red team testing phase shall be proportionate to the TLPT scope, to the scale, activity, complexity and number of the financial entities and ICT third-party or ICT intragroup service providers involved in the TLPT, and in any case shall last for at least twelve weeks. Attack scenarios may be executed in sequence or at the same time. The control team, the threat intelligence provider, the testers and the test managers shall agree on the end of the active red team testing phase.
6. Any changes to the red team test plan subsequent to its approval, including to the timeline, scope, target systems or flags, shall be approved by the control team lead and the test managers.
7. During the entire active red team testing phase, testers shall report at least weekly to the control team and test managers on the progress made in the TLPT, and the threat intelligence provider shall remain available for consultation and additional threat intelligence when requested by the control team.
8. The control team shall timely provide leg-ups designed on the basis of the red team test plan. Leg-ups may be added or adapted upon approval by the control team and the test managers.
9. In case of detection of the testing activities by any staff member of the financial entity or of its ICT third-party service providers or ICT intragroup service provider, where relevant, the control team, in consultation with the testers and without prejudice to paragraph 10, shall propose and submit measures allowing to continue the TLPT while ensuring its secrecy to the test managers for validation.
10. Under exceptional circumstances triggering risks of impact on data, damage to assets, and disruption to critical or important functions, services or operations of the financial entity itself, of its ICT third-party service providers or ICT intragroup services providers, or disruptions to its counterparts or to the financial sector, the control team lead may suspend the TLPT, or, as a last resort, if the continuation of the TLPT is not otherwise

possible and subject to prior validation by the TLPT authority, continue the TLPT using a limited purple teaming exercise. The duration of the limited purple teaming exercise shall be counted for the purpose of the twelve week minimum duration of the active red team testing phase.

*Article 11*

**Closure phase**

1. Following the end of the active red team testing phase, the control team lead shall inform the blue team that a TLPT took place.
2. Within four weeks from the end of the active red team testing phase, the testers shall submit to the control team a red team test report containing the information set out in Annex V.
3. Without undue delay, the control team shall provide the red team test report to the blue team and test managers.

At the request of the test managers, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

4. Upon receipt of the red team test report, and no later than ten weeks after the end of the active red team testing phase, the blue team shall submit to the control team a blue team test report containing the information set out in Annex VI. Without undue delay, the control team shall provide the blue team test report to the testers and the test managers.

At the request of the test managers, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

5. No later than ten weeks after the end of the active red team testing phase, the blue team and the testers shall carry out a replay of the offensive and defensive actions performed during the TLPT. The control team shall also conduct a purple teaming exercise on topics jointly identified by the blue team and the testers, based on vulnerabilities identified during the test and, where relevant, on issues that could not be tested during the active red team testing phase.
6. After completion of the replay and purple teaming exercises, the control team, the blue team, the testers and threat intelligence providers shall provide feedback to each other on the TLPT process. The test managers may provide feedback.
7. Once the TLPT authority has notified the control team lead that it has assessed that the blue team test report and the red team test report contain the information set out in Annex V and Annex VI, the financial entity shall within eight weeks submit the report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554, containing the elements set out in Annex VII for approval.
8. At the request of the TLPT authority, the report referred to in the first subparagraph of this paragraph shall not contain sensitive information.

*Article 12*

**Remediation plan**

1. Within eight weeks from the notification referred to in Article 11(7), the financial entity shall provide the remediation plans referred to in Article 26(6) of Regulation (EU) 2022/2554 to the TLPT authority and, where different, to the financial entity's competent authority.

2. The remediation plan referred in paragraph 1 shall include, for each finding occurred in the framework of the TLPT:

- (a) a description of the identified shortcomings;
- (b) a description of the proposed remediation measures and of their prioritisation and expected completion, including where relevant measure to improve the identification, protection, detection and response capabilities;
- (c) a root cause analysis;
- (d) the financial entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements;
- (e) the risks associated to not implementing the measures referred to in point (b) and, where relevant, risks associated to the implementation of such measures.

#### CHAPTER IV

### REQUIREMENTS AND STANDARDS GOVERNING THE USE OF INTERNAL TESTERS

#### *Article 13*

##### **Use of internal testers**

1. Financial entities shall establish all of the following arrangements for the use of internal testers:

- (a) the definition and implementation of a policy for the management of internal testers in a TLPT. Such policy shall:
  - i. include criteria to assess suitability, competence, potential conflicts of interest of the internal testers and define management responsibilities in the testing process. The policy shall be documented and periodically reviewed;
  - ii. provide that the internal testing team includes a test lead, and at least two additional members. The policy shall require that all members of the test team have been employed by the financial entity or by an ICT intra-group service provider for the preceding 12 months;
  - iii. include provisions on training on how to perform penetration testing and red team testing of the internal testers.
- (b) measures to ensure that the use of internal testers to perform TLPT will not negatively impact the financial entity's general defensive or resilience capabilities regarding ICT-related incidents or significantly impact the availability of resources devoted to ICT-related tasks during a TLPT;
- (c) measures to ensure that internal testers have sufficient resources and capabilities available to perform TLPT in accordance with this Regulation;
- (d) when a TLPT authority approves the use of internal testers according to Article 27(2)(a) of Regulation (EU) 2022/2554, the TLPT authority shall consider the requirements laid down in Article 5(2) of this Regulation.

2. When using internal testers, the financial entity shall ensure that such use is mentioned in the following documents:

- (a) the test initiation documents referred to in Article 8;



- (b) the red team test report referred to in Article 11(2);
  - (c) the report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554.
3. For the purposes of this Regulation, testers employed by an ICT intra-group service provider shall be considered as internal testers of the financial entity.

## CHAPTER V

### COOPERATION AND MUTUAL RECOGNITION AND FINAL PROVISIONS

#### *Article 14*

#### **Cooperation**

1. For the purposes of conducting a TLPT in relation to a financial entity providing services in more than one Member State, including through a branch, its TLPT authority shall:
- (a) determine which TLPT authorities in host Member States shall be involved, taking into account whether one or more critical or important functions are operated in, or shared across, host Member States;
  - (b) inform the TLPT authorities identified according to point (a) of the decision to carry out a TLPT test on the financial entity. Within 20 working days from the receipt of the information on a future conduct of a TLPT, the TLPT authorities of the host Member States may either express their interest in following the TLPT as observers or assign a test manager to participate in the TLPT;
  - (c) unless otherwise agreed by the TLPT authorities, the TLPT authority of the financial entity shall lead the TLPT. The lead TLPT authority shall provide all TLPT authorities acting as observers in TLPT with the scope specification document, the test summary report, remediation plan and attestation. The lead TLPT authority shall coordinate all participating TLPT authorities throughout the test and adopt all the decisions necessary to carry out the TLPT appropriately and effectively. The lead TLPT authority may set a maximum number of participating TLPT authorities, where the efficient conduct of the TLPT might otherwise be compromised.
2. Where a financial entity uses the same ICT intra-group service provider as financial entities established in other Member States, or belongs to a group and uses ICT systems common to financial entities of the same group established in other Member States, the TLPT authority of the financial entity shall contact the TLPT authorities of the other financial entities using the same ICT intra-group service provider or using the same ICT systems as part of the group and assess with them the feasibility and suitability of conducting a joint TLPT in their respect. A joint TLPT shall be preferred to an individual TLPT where it may result in reduction of costs and resources for the financial entities and for the TLPT authorities, provided that the soundness and efficacy of the test is not prejudiced.
3. For the purposes of conducting a joint TLPT:
- (a) the TLPT authorities of the financial entities shall agree on which financial entity shall be designated to conduct the TLPT, considering the group structure and the efficiency of the test;
  - (b) the TLPT authority of the financial entity designated in accordance with point (a) shall lead the TLPT, unless otherwise agreed by the TLPT authorities of the financial entities participating in the joint TLPT;
  - (c) the TLPT authorities of the financial entities other than the designated financial entity to lead the joint TLPT may either express their interest in following the TLPT as observers or assign a test manager for that TLPT. The

lead TLPT authority shall coordinate all TLPT authorities involved in the joint TLPT and adopt all the decisions necessary to carry out the joint TLPT in a sound and effective way.

4. Where a financial entity intends to conduct a pooled TLPT as referred to in Article 26(4) of Regulation (EU) 2022/2554 possibly involving financial entities established in other Member States, its TLPT authority shall contact the TLPT authorities of the other financial entities and assess with them the feasibility and suitability of conducting a pooled TLPT in their respect in accordance with Article 26(4) of Regulation (EU) 2022/2554.

5. For the purposes of conducting a pooled TLPT as referred to in Article 26(4) of Regulation (EU) 2022/2554:

(a) the TLPT authorities of the financial entities shall agree on which financial entity shall be designated to conduct the pooled TLPT, considering the ICT services provided by the ICT third-party service provider to the financial entities and the efficiency of the test;

(b) the TLPT authority of the financial entity designated in accordance with point (a) shall lead the TLPT, unless otherwise agreed by the TLPT authorities of the financial entities participating in the pooled or joint TLPT;

(c) the TLPT authorities of the financial entities other than the designated financial entity to lead the pooled TLPT may either express their interest in following the TLPT as observers or assign a test manager to that TLPT. The lead TLPT authority shall coordinate all TLPT authorities involved in the pooled TLPT and adopt all the decisions necessary to carry out the pooled TLPT in a sound and effective way.

6. Where, in relation to a financial entity required to perform a TLPT, its TLPT authority differs from its competent authority as referred to in Article 46 of Regulation (EU) 2022/2554, these authorities shall share any relevant information in respect of all TLPT-related matters for the purposes of carrying out the TLPT or to carry out their duties in accordance with Regulation (EU) 2022/2554.

7. The attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall at least mention the information set out in Annex VIII.

8. Where several TLPT authorities have been involved in a TLPT, the attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall be provided by the lead TLPT authority.

#### *Article 15*

#### **Entry into force and application**

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,

## ANNEX I

## Content of the project charter

Item of information	Information required
Person responsible for the project plan, i.e. the Control Team Lead	Name Contact details
Testers	<input type="checkbox"/> internal <input type="checkbox"/> external <input type="checkbox"/> both
Communication channels selected in accordance with Article 8(1) point d) and 8(2) point a, including: (a) Email encryption to be used (b) Online data rooms to be used (c) Instant messaging to be used	
Codename for the TLPT	
If any, critical or important functions the financial entity operates in other Member States	1. List of critical or important functions operated in another Member State 2. for each critical or important function, indication of the Member State or States in which they are operated
If any, critical or important functions supported by ICT third party service providers	3. List of critical or important functions supported by ICT third-party service providers 4. for each function, identification of the ICT third party service provider
<b>Expected deadlines for the completion of the:</b>	
(1) Preparation Phase, in accordance with Article 8	yyyy-mm-dd
(2) Testing Phase, in accordance with Articles 9 and 10	yyyy-mm-dd
(3) Closure Phase, in accordance with Article 11	yyyy-mm-dd
(4) Remediation plan in accordance with Article 12	yyyy-mm-dd

**ANNEX II**

**Content of the scope specification document**

4. The scope specification document shall include a list of all critical or important functions identified by the financial entity.
5. For each identified critical or important function, the following information shall be included:
  - (a) Where the critical or important function is not included in the scope of the TLPT, the explanation of the reasons for which it is not included;
  - (b) Where the critical or important function is included in the scope of the TLPT:
    - (i) the explanation of the reasons for its inclusion;
    - (ii) the identified ICT system(s) supporting this critical or important function;
    - (iii) for each identified ICT system:
6. whether it is outsourced and if so, the name of the ICT third party service provider;
7. the jurisdictions in which the ICT system is used;
8. a high-level description of preliminary flag(s), indicating which security aspect of confidentiality, integrity, authenticity and/or availability is covered by each flag.

**ANNEX III**

**Content of the targeted threat intelligence report**

The targeted threat intelligence report shall include information on all of the following:

1. Overall scope of the intelligence research including at least the following:
  - a. critical or important functions in scope;
  - b. their geographical location;
  - c. official EU language in use;
  - d. relevant ICT third party services providers;
  - e. period of time over which the research is gathered.
2. Overall assessment of what concrete actionable intelligence can be found about the financial entity, such as:
  - a. employee usernames and passwords;
  - b. look-alike domains which can be mistaken for official domains of the financial entity;
  - c. technical reconnaissance: vulnerable and/or exploitable software, systems and technologies;
  - d. information posted by employees on social media, related to the financial entity, which might be used for the purposes of an attack;
  - e. information for sale on the dark web;
  - f. any other relevant information available on the internet or public networks;
  - g. where relevant, physical targeting information, including ways of access to the premises of the financial entity.
3. Threat intelligence analysis considering the general threat landscape and the particular situation of the financial entity, including, at least:
  - a. Geopolitical environment;
  - b. Economic environment;
  - c. Technological trends and any other trends related to the activities in the financial services sector;
4. Threat profiles of the malicious actors (specific individual/group or generic class) that may target the financial entity, including the systems of the financial entity that malicious actors are most likely to compromise or target, the possible motivation, intent and rationale for the potential targeting and the possible modus operandi of the attackers.

5. Threat scenarios: At least three end-to-end threat scenarios for the threat profiles identified in accordance with point 4 who exhibit the highest threat severity scores. The threat scenarios shall describe the end-to-end attack path and shall include, at least:
  - a. one scenario that includes but is not limited to compromised service availability;
  - b. one scenario that includes but is not limited to compromised data integrity;
  - c. one scenario that includes but is not limited to compromised information confidentiality.
6. Where relevant, description of the scenario referred to in Article 7(4).

**ANNEX IV**

**Content of the red team test plan**

The red team test plan shall include information on all of the following:

- (i) communication channels and procedures;
- (ii) the tactics, techniques and procedures allowed and not-allowed for use in the attack including ethical boundaries for social engineering, and how the privacy of involved parties is being safeguarded;
- (iii) risk management measures to be followed by the testers;
- (iv) a description for each scenario, including:
  - a. the simulated threat actor;
  - b. their intent, motivation and goals;
  - c. the target function(s) and the supporting ICT system or systems;
  - d. the targeted confidentiality, integrity, availability and authenticity aspects;
  - e. flags;
- (v) a detailed description of each expected attack path, including pre-requisites and possible leg-ups to be provided by the control team, including deadlines for their provision and potential usage;
- (vi) scheduling of red teaming activities, including time planning for the execution of each scenario, at a minimum split according to the three phases a tester takes throughout the testing phase, respectively entering financial entities' ICT systems, moving through the ICT systems and ultimately executing actions on objectives and eventually extracting itself from the ICT systems (in, through and out phases);
- (vii) particularities of the financial entities' infrastructure to be considered during testing;
- (viii) if any, additional information or other resources necessary to the testers for executing the scenarios.

**ANNEX V**

**Content of the red team test report**

The red team test report shall include information on at least all of the following:

i. Information on the performed attack, including:

- a. the targeted critical or important functions and identified ICT systems, processes and technologies supporting the critical or important function, as identified in the red team test plan;
- b. summary of each scenario;
- c. flags reached and not reached;
- d. attack paths followed successfully and unsuccessfully;
- e. tactics, techniques and procedures used successfully and unsuccessfully;
- f. deviations from the red team test plan, if any;
- g. leg-ups granted, if any;

ii. All actions that the testers are aware of that were performed by the blue team to reconstruct the attack and to mitigate its effects;

iii. Discovered vulnerabilities and other findings, including:

- a. vulnerability and other finding description including their criticality;
- b. root cause analysis of successful attacks;
- c. recommendations for remediation including indication of the remediation priority.



**ANNEX VI**

**Content for the blue team test report**

The blue team test report shall include information on at least of the following:

1. for each attack step described by the testers in the red team test report:

(a) list of detected attack actions;

iv.log entries corresponding to these detections;

1. assessment of the findings and recommendations of the testers;
2. evidence of the attack by the testers collected by the blue team;
3. blue team root cause analysis of successful attacks by the testers;
4. list of lessons learned and identified potential for improvement;
5. list of topics to be addressed in purple teaming.

**ANNEX VII**

**Details of the report summarizing the relevant findings of the TLPT referred to in Article 26(6) of Regulation (EU) 2022/2554**

The test summary report shall include information on at least of the following:

- (a) the parties involved;
- (b) the project plan;
- (c) the validated scope, including the rationale behind the inclusion or exclusion of critical or important functions and identified ICT systems, processes and technologies supporting the critical or important functions covered by the TLPT;
- (d) selected scenarios and any significant deviation from the targeted threat intelligence report;
- (e) executed attack paths, and used tactics, techniques and procedures;
- (f) captured and non-captured flags;
- (g) deviations from the red team test plan, if any;
- (h) blue team detections, if any;
- (i) purple teaming in testing phase, where conducted and the related conditions;
- (j) leg-ups used, if any;
- (k) risk management measures taken;
- (l) identified vulnerabilities and other findings, including their criticality;
- (m) root cause analysis of successful attacks;
- (n) high level plan for remediation, linking the vulnerabilities and other findings, their root causes and remediation priority;
- (o) lessons derived from feedback received.

**ANNEX VIII**

**Details of the attestation of the TLPT**

The attestation referred to in Article 26(7) of Regulation (EU) 2022/2554 shall include at least the following information:

- (a) on the performed TLPT:
  - a. the starting and end dates of the TLPT;
  - b. the critical or important functions in scope of the test;
  - c. where relevant, information on critical or important functions in scope of the test in relation to which the TLPT was not performed;
  - d. where relevant, other financial entities that were involved in the TLPT;
  - e. where relevant, the ICT third-party services providers that participated in the TLPT;
  - f. in respect of testers:
    - i. whether internal testers were used;
    - ii. whether Article 5(3), second subparagraph, was used by the financial entity;
  - g. the duration, in calendar days, of the active red team testing phase;
- (b) where several TLPT authorities have been involved in the TLPT, the other TLPT authorities, and in which capacity;
- (c) list of the documents examined by the TLPT authority for the purposes of the attestation.

## APPENDIX XII: Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

[\(JC 2024 34 – 17 July 2024\)](#)

These Guidelines contain references to EU Commission delegated and implementing regulations that have not yet been published in the EU Official Journal. Once these forthcoming Regulations will have been published in the Official Journal, these Guidelines will be finalised by including these references. The references will be inserted in the sections highlighted in yellow.

The date of application of these Guidelines can only be determined once these Guidelines are finalised. The expected date of application of these Guidelines is 17 January 2025. In case there is a delay in finalising these Guidelines, the latest day of application of these Guidelines will be two months following the date of the publication of the translations of these Guidelines in all official EU languages.

### Status of these Joint Guidelines

This document contains Joint Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010<sup>87</sup>; Article 16 of Regulation (EU) No 1094/2010<sup>88</sup>; and Article 16 of Regulation (EU) No 1095/2010<sup>89</sup> - ‘the ESAs’ Regulations’. In accordance with Article 16(3) of the respective ESAs’ Regulations, competent authorities and financial institutions must make every effort to comply with the Guidelines. Joint Guidelines set out the ESAs’ view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities to whom the Joint Guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where the Joint Guidelines are directed primarily at institutions.

### Reporting Requirements

In accordance with Article 16(3) of the ESAs’ Regulations, competent authorities must notify the respective ESA whether they comply or intend to comply with these Joint Guidelines/Recommendations, or otherwise with reasons for non-compliance, by dd.mm.yyyy (two months after issuance). In the absence of any notification by this deadline, competent authorities will be considered by the respective ESA to be non-compliant. Notifications should be sent to <mailto:compliance@eba.europa.eu>, <mailto:compliance@eiopa.europa.eu> and <mailto:DORA@esma.europa.eu> with the reference ‘JC/GL/2024/34’. A template for notifications is available on the ESAs’ websites. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the ESAs’ websites, in line with Article 16(3).

---

<sup>87</sup> 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)

<sup>88</sup> 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. 48–83)

<sup>89</sup> 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. 84–119)

## **Title I - Subject matter, scope, addressees, and definitions**

### **Subject matter and Scope of application**

1. These guidelines are aimed at fulfilling the mandate given to the ESAs under Article 11(11) of Regulation (EU) 2022/2554<sup>90</sup>, to develop common guidelines on the estimation of aggregated annual costs and losses of major ICT-related incidents referred to Article 11(10) of that Regulation. These guidelines also specify a common template for the submission of the aggregated annual costs and losses.

### **Addressees**

2. These guidelines are addressed to competent authorities as defined in Article 46 of Regulation 2022/2554 and to financial institutions as defined in Article 4(1) of Regulation (EU) 1093/2010, Article 4(1) of Regulation (EU) 1094/2010 and Article 4(1) of Regulation (EU) 1095/2010.

### **Definitions**

3. Terms used and defined in Regulation (EU) 2022/2554 have the same meaning in these guidelines.

## **Title II- Implementation**

### **Date of application**

4. These Guidelines apply from [expected date of application 17 January 2025, or at the latest two months after the date of publication of the translations of these Guidelines in all official EU languages].

## **Title III- Provisions on the estimation of aggregated annual costs and losses of major ICT-related incidents**

5. Financial entities should estimate the aggregate annual costs and losses of major ICT-related incidents by aggregating the costs and losses for major ICT-related incidents that fall within the reference year for which the competent authority requested the estimation. The financial entity may choose whether the reference year should correspond to either the completed calendar year, or to the completed accounting year of the financial entity for which the financial entity has finalised its financial statements. Once a financial entity has decided whether it will provide the estimation based on the calendar year or its accounting year, such a decision should be applied to future estimations of aggregated annual costs and losses. The financial entity may change that decision by notifying the competent authority, and provided that the competent authority does not object within two months of receiving the notification. Financial entities should not include costs and losses related to those incidents that fall before or after that reference year.

6. Financial entities should include in the estimation all ICT-related incidents that, irrespective of the reason, were classified as major in accordance with Commission Delegated Regulation [insert OJ given number once published for RTS on incident classification]<sup>91</sup> on incident classification and

- (a) for which the financial entity has submitted a final report in accordance with Article 19(4)(c) Regulation (EU) 2022/2554 in the relevant reference year, or

---

<sup>90</sup> Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, (OJ L 333, 27.12.2022, p. 1–79)

<sup>91</sup> INSERT Full title and OJ reference

## APPENDIX XII: JOINT GUIDELINES ON THE ESTIMATION OF AGGREGATED ANNUAL COSTS AND LOSSES CAUSED BY MAJOR ICT-RELATED INCIDENTS

---

- (b) any incident for which the financial entity submitted in previous reference years a final report in accordance with Article 19(4)(c) of Regulation (EU) 2022/2554 that had a quantifiable financial impact on the financial entity in the relevant reference year.
7. Financial entities should estimate the aggregated annual costs and losses by applying the follow sequential steps:
- (a) estimate the costs and losses of each major ICT-related incident as referred to in paragraph 6 individually. Those estimations should produce the gross costs and losses taking into account the types of costs and losses as set out in Article 7(1) and (2) of the Commission Delegated Regulation [insert OJ given number once published for RTS on incident classification];
  - (b) for each major ICT-related incident, financial entities should also estimate the financial recoveries as specified in Annex II to Commission Implementing Regulation [insert OJ given number once published for ITS on incident reporting]<sup>92</sup>;
  - (c) financial entities should aggregate the gross costs and losses and the financial recoveries across major ICT-related incidents.
8. As basis for the estimations, financial entities should refer to the costs, losses and financial recoveries that are reflected in their financial statements such as the profit and loss account, or where applicable in their supervisory reporting, of the relevant reference year. In their estimation, financial entities should also include accounting provisions that are reflected in their financial statements such as the profit and loss account of the relevant reference year. Where accurate data is not available, financial entities should base their estimation on other available data and information to the extent possible.
9. Financial entities should include adjustments on the costs and losses of an estimation that it submitted for a previous year in the estimation of the relevant reference year in which the adjustments are made.
10. Financial entities should include in the report of their estimation of the aggregated annual costs and losses also the breakdown of gross costs and losses and of financial recoveries for each major ICT-related incident that were included in the aggregation.
11. Financial entities should use the template in the Annex to submit to the competent authority the estimation of their aggregated annual costs and losses for the reference year. For each item under paragraph 6 and 9 that is included in the estimation of the reference year, financial entities should use the same incident reference codes provided by the financial entity as the ones used in the final report in accordance with Article 19(4)(c) of Regulation (EU) 2022/2554.

---

<sup>92</sup> INSERT Full title and OJ reference

**Annex: Reporting template for gross costs and losses and financial recoveries in a reference year**

Name of the financial entity				
Legal Entity Identifier				
Start and end date of the reference year of the financial entity				
Currency				
Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the reference year (1000s of units)	Recoveries of the incident in the reference year (1000s of units)
1				
2				
...				
Total for reference year	-----	-----		

## APPENDIX XIII: Guidelines on ESAs-competent authorities oversight cooperation

[\(JC 2024 36 – 17 July 2024\)](#)

[Art. 32(7)]

### Status of the Guidelines

These Guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority); Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) (the ESAs' Regulations)<sup>93</sup>.

The European Supervisory Authorities (ESAs) issue these Guidelines on the basis of Article 32(7) of Regulation (EU) 2022/2554 ("DORA")<sup>94</sup>, according to which the ESAs shall issue guidelines on the cooperation between the ESAs and the competent authorities covering:

- the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs; and
- the details on the exchanges of information which are necessary for competent authorities to ensure the follow-up of recommendations addressed to ICT third party service providers to financial entities designated as critical.

### Reporting requirements

In accordance with Article 16(3) of the ESAs' Regulations, competent authorities shall make every effort to comply with the Guidelines. Competent authorities must notify the respective ESA whether they comply or intend to comply with these Guidelines, or otherwise with reasons for non-compliance, within two months after the issuance of the translated versions of the Guidelines. In the absence of any notification by this deadline, competent authorities will be considered by the respective ESA to be non-compliant. Notifications should be sent to [compliance@eba.europa.eu](mailto:compliance@eba.europa.eu), [compliance@eiopa.europa.eu](mailto:compliance@eiopa.europa.eu) and [DORA@esma.europa.eu](mailto:DORA@esma.europa.eu) with the reference 'JC/GL/2024/36'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Notifications will be published on the ESAs' websites, in line with Article 16(3).

---

<sup>93</sup> 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.12-47). Regulation (EU) No 1094/2010 of the European Parliament and of the Council 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.48-83). 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. 84-119).

<sup>94</sup> Regulation (EU) No 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector 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.01-79).



## Section 1: General considerations

### General aims and principles

These Guidelines aim at ensuring that the ESAs and the competent authorities have:

- an overview of the areas where cooperation and/or exchange of information between competent authorities and the ESAs is needed in accordance with Article 32(7) of the DORA;
- a coordinated and cohesive approach between the ESAs and competent authorities in the exchange of information and when cooperating for the purpose of oversight activities to ensure efficiency and consistency as well as to avoid duplications;
- a common approach to the rules of procedure and timelines that apply in relation to cooperation and information exchange, including roles and responsibilities and means for cooperation and information exchange.

These Guidelines constitute consistent, efficient and effective practices on the oversight cooperation and information exchange between ESAs and competent authorities in the context of Article 32(7) of the DORA. These Guidelines do not hinder the exchange of further information and extended oversight cooperation between ESAs and competent authorities. The practical details of the cooperation and information sharing between ESAs and competent authorities may be subject to bespoke target operating models.

The cooperation and information exchange set out in these Guidelines should take into account a preventive and risk-based approach which should lead to a balanced allocation of tasks and responsibilities between the three ESAs and competent authorities and should make the best use of the human resources and technical expertise available in each of the ESAs and competent authorities.

Unless otherwise specified in these Guidelines, ESAs refers to the three ESAs including the Lead Overseer.

### Scope

The scope of these Guidelines relates only to Section II of Chapter V (Articles 31-44) of the DORA and does not cover articles related to:

- tasks that only apply to either one specific competent authority or ESA (e. g. Article 43 on Oversight fees, being a task for the LO only) or that apply to financial entities and critical ICT third-party service providers (e. g. under Article 35(5) , CTPPs are to cooperate in good faith with LO, and assist it in fulfilment of its tasks);
- the cooperation among competent authorities (e. g. under Article 48(1), CAs shall cooperate closely among themselves), among the ESAs (e. g. under Article 35(2)(a), the LO shall ensure regular coordination within the Joint Oversight Network) and with other EU authorities (e. g. under Article 34(3), the LO may call on the ECB and ENISA to provide technical advice);
- the governance arrangements that are subject to the rules of procedure of the ESAs (e. g. under Article 32, the ESAs need to establish the OF and under Article 34, the LOs need to set up the Joint Oversight Network);
- the separate legal mandates(e. g. the criteria for determining the composition of the JET, their designation, tasks and working arrangements are covered by separate regulatory technical standards to be developed by the ESAs (Article 41(1)(c) of DORA).

### **Guideline 1: Language, communication means, contact points and accessibility**

- 1.1 For cooperation and information exchange purposes, the ESAs and competent authorities should communicate in English, unless agreed otherwise.
- 1.2 The ESAs and competent authorities should make available the information referred to in these Guidelines by electronic means, unless agreed otherwise.
- 1.3 The ESAs and competent authorities should establish single points of contact in the form of a dedicated institutional/functional email address for information exchanges between the ESAs and competent authorities.
- 1.4 The single point of contact should only be used for exchanging non-confidential information. The ESAs and competent authorities may agree on a bilateral and/or multilateral basis on any applicable requirements concerning the secure transmission of information via the single point of contact (e.g. a requirement on electronic signatures of authorised persons).
- 1.5 The information on the contact points should be made available to the competent authorities by the ESAs. The competent authorities should make available and update the information about the contact points without undue delay according to the operational instructions defined by the ESAs.
- 1.6 The ESAs and competent authorities should use a dedicated secure online tool to share information amongst each other on a confidential and secure basis. The online tool should present technical information security measures to guarantee the confidentiality of data against unauthorised access by third-parties.
- 1.7 The information to be exchanged via the dedicated secure online tool should be limited to the information to be submitted according to points 5 to 12 and any additional information necessary for the Lead Overseer and competent authorities to carry out their respective duties under DORA.
- 1.8 The ESAs and competent authorities should ensure that communication and information exchange between the ESAs and competent authorities are accessible to, and inclusive for all parties involved, including those who may have language barriers or accessibility needs. In that context, the ESAs and competent authorities may use translation services or accessible communication tools, such as video conferencing software with closed captioning, provided data is protected from unauthorised use of third parties.

### **Guideline 2: Timelines**

- 2.1 In the event of specific circumstances that require prompt action or additional time to complete the relevant task, the Lead Overseer may, in consultation with relevant competent authorities, reduce or extend the timelines described in points 5 to 12. The Lead Overseer should document the changes and the reasons for such changes.

### **Guideline 3: Difference of opinions between ESAs and competent authorities**

- 3.1 In case of divergent views regarding the oversight cooperation and information exchange, the ESAs and competent authorities should strive to reach a mutually agreed solution. In cases where no such solution can be reached, the Lead Overseer should, in consultation with the Joint Oversight Network, present the difference of opinions to the Oversight Forum, which will present its views to find a mutually agreed solution.

**Guideline 4: Information exchange between ESAs and competent authorities in the context of their respective cooperation with competent authorities designated or established in accordance with NIS2 (NIS2 authorities)**

4.1 Where possible, competent authorities and the Lead Overseer should make available to each other relevant information stemming from their dialogue with NIS2 authorities responsible for the supervision of essential or important entities subject to that Directive, which have been designated as a critical ICT third-party service provider.

**Section 2: Designation of critical ICT third-party service providers****Guideline 5: Information for the criticality assessment to be submitted by competent authorities to the ESAs**

5.1 For the purposes of designating the ICT third-party service providers that are critical for financial entities in accordance with Article 31(1)(a) of the DORA, without undue delay following the receipt of the register of information referred to in Article 28(3) of the DORA, competent authorities should make available the full register of information to the ESAs in accordance with the formats and procedures specified by the ESAs.<sup>95</sup>

5.2 Competent authorities should also make available to the ESAs any relevant quantitative or qualitative information at their disposal to facilitate the criticality assessment envisaged in Article 31(2) of the DORA, taking into account the delegated act referred to in Article 31(6) of the DORA.

5.3 Upon request, competent authorities should make available to the ESAs additional available information acquired in their supervisory activities, in order to facilitate the criticality assessment.

**Guideline 6: Information related to the designation of critical ICT third-party service providers to be submitted by the Lead Overseer or ESAs to competent authorities**

6.1 Within 10 working days following the receipt from the ICT third-party service provider, the ESAs should make available to the competent authorities of the financial entities using the ICT services provided by a ICT third-party service provider, the legal name, identification code<sup>96</sup>, country of the registered office of the ICT third-party service provider and, if it belongs to a group, of the parent group that submitted a request to be designated as critical according to Article 31(11) of the DORA.

6.2 The Lead Overseer should share with the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider:

- a) Within 10 working days following the receipt from the critical ICT third-party service provider, the notification of the critical ICT third-party service provider about any changes to the structure of the management of the subsidiary established in the Union according to Article 31(13) of the DORA;
- b) Within 10 working days after the submission of the notification of a decision to designate the ICT third-party service provider as critical to the ICT third-party service provider, the legal name, identification code<sup>96</sup>, country of the registered office of the ICT third-party service provider and, if it belongs to a group, of the parent group that has been designated as critical according to Article 31(5)

<sup>95</sup> The ESAs will make use of Article 35(2) of the founding regulations of the ESAs to request the full register of information.

<sup>96</sup> "Identification code" refers to the identification code requested for ICT third-party service providers as established by the Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

and (11) of the DORA and the starting date as from which they will effectively be subject to oversight activities as referred to in Article 31(5) of the DORA.

### **Section 3: Core oversight activities**

#### **Guideline 7: Oversight plans**

- 7.1 Prior to the finalisation of the annual oversight plan referred to in Article 33(4) of the DORA, the Lead Overseer should make available the draft annual oversight plan to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider.
- 7.2 The draft annual oversight plan should include the following information on the envisaged general investigations or inspections:
- a) type of oversight activity (general investigation or inspection);
  - b) high-level scope and objectives;
  - c) approximate timeframe.
- 7.3 Competent authorities may provide comments on the draft annual oversight plan within 30 working days following the receipt thereof.
- 7.4 Within 10 working days following the adoption, the Lead Overseer should make available to the competent authorities, the annual oversight plan and the multi-annual oversight plan<sup>97</sup>.
- 7.5 The Lead Overseer should make available any material updates to the annual oversight plan and the multi-annual oversight plan to the competent authorities without undue delay following the adoption of the updates. Competent authorities may provide comments on the material updates to the annual oversight plan within 30 working days following the receipt.

#### **Guideline 8: General investigations and inspections**

- 8.1 At least 3 weeks before the start of the general investigation or inspection according to Articles 38(5), 39(3) and 36(1) of the DORA, or with the shortest possible delay in case of an urgent investigation or inspection, the Lead Overseer should inform the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the identity of the authorised persons for the general investigation or inspection.
- 8.2 The authorised persons include:
- relevant staff members of the Lead Overseer; and
  - the staff members of the Joint Examination Team as referred to in Article 40(2) of the DORA, appointed to carry out the general investigation or inspection.
- 8.3 The Lead Overseer should inform competent authorities of the financial entities using the ICT services provided by that critical ICT third-party service provider where the authorised persons find that a critical ICT

---

<sup>97</sup> See Recital 3 of draft Regulatory Technical Standards on the conduct of oversight activities in relation to the joint examination teams under DORA

third-party service provider opposes the inspection, including imposing any unjustified conditions to the inspection.

### **Guideline 9: Additional information exchanges between the Lead Overseer and competent authorities in relation to oversight activities**

9.1 Within 10 working days following the adoption of the request for information to the critical ICT third-party service provider, the Lead Overseer should make available to the Joint Oversight Network and the competent authorities of the financial entities using ICT services provided by a critical ICT third-party service provider, the relevant scope of the request for information submitted to the critical ICT third-party service provider according to Articles 36(1)<sup>98</sup> and 37(1) of the DORA.

9.2 The Lead Overseer should inform competent authorities of the financial entities using ICT services provided by a critical ICT third-party service provider of any:

- major incidents with direct or indirect impact on financial entities within the Union when reported by the critical ICT third-party service provider, including relevant details to determine the significance of the incident on financial entities and assess possible cross-border impacts;<sup>99</sup>
- relevant changes in the strategy of the critical ICT third-party service provider on ICT third-party risk;
- events that could represent an important risk to the continuity and sustainability of the provision of ICT services;
- reasoned statement that may be submitted by the critical ICT third-party service provider evidencing the expected impact of the draft oversight plan on customers which are entities falling outside of the scope of DORA and where appropriate, formulating solutions to mitigate risks referred to in Article 33(4) of the DORA.

9.3 If a critical ICT third-party service provider liaises with the competent authorities for the purposes of all matters related to the oversight, the competent authorities should make available those communications to the Lead Overseer and remind the critical ICT third-party service provider that the Lead Overseer is its primary point of contact for the purposes of all matters related to the oversight.

## **Section 4: Follow-up of the recommendations**

### **Guideline 10: General principles for follow-up**

10.1 The following general principles should apply to the follow-up of the recommendations issued by the Lead Overseer:

- The competent authorities are the primary point of contact for financial entities under their supervision. The competent authorities are responsible for the follow-up concerning the risks identified in the recommendations concerning financial entities making use of the services of the critical ICT third-party service providers;

---

<sup>98</sup>

<sup>99</sup> See Article 3(2), letter l of Draft regulatory technical standards on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), b) and (d) of Regulation (EU) 2022/2554

- The Lead Overseer is the primary point of contact for critical ICT third-party service providers for the purposes of all matters related to the oversight. The Lead Overseer is responsible for the follow-up of the recommendations addressed to the critical ICT third-party service provider.

### **Guideline 11: Information exchanges between the Lead Overseer and competent authorities to ensure the follow-up of recommendations**

11.1 The Lead Overseer should make available to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the following information:

- a. Within 10 working days following the receipt by the Lead Overseer:
  - the notification of the critical ICT third-party service provider to follow the recommendations issued by the Lead Overseer and the remediation plan prepared by the critical ICT third-party service provider;
  - the reasoned explanation of the critical ICT third-party service provider for not following the recommendations;
  - the reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider according to Article 35(1)(c) of the DORA.
- b. Within 10 working days after the expiration of the 60 calendar days according to Article 42(1) of the DORA:
  - the fact that the critical ICT third-party service provider failed to send the notification within 60 calendar days after the issuance of recommendations to the critical ICT third-party service provider according to Article 35(1)(d) of the DORA.
- c. Within 10 working days after the adoption by the Lead Overseer:
  - the assessment as to whether the critical ICT third-party service provider's explanation for not following the Lead Overseer's recommendations is deemed sufficient and, if it is deemed sufficient, the Lead Overseer's decision concerning amendment of recommendations<sup>100</sup>;
  - the assessment of the reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider according to Articles 35(1)(c) of the DORA. In case the critical ICT third-party service provider has not adequately implemented the recommendations, the assessment should at least cover the criteria a) to d) of Article 42(8) of the DORA;
  - the decision imposing a periodic penalty payment on the critical ICT third-party service provider according to Article 35(6) of the DORA. If the Lead Overseer opted not to disclose the periodic penalty payment to the public as per Article 35(10) of the DORA, the competent authorities receiving the information should not disclose it to the public;
  - assessment as to whether the refusal of a critical ICT-third-party service provider to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer,

---

<sup>100</sup> The Lead Overseer and the Joint Examination Team assess the critical ICT third party service provider's reasoned explanation for not following the recommendations. If the Lead Overseer decides that the explanation is deemed sufficient, the Lead Overseer may amend the respective recommendations.

could adversely impact a large number of financial entities, or a significant part of the financial sector.

11.2 In accordance with Article 42(10) of the DORA, the competent authorities should make available to the Lead Overseer the following information where critical ICT third party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer:

- a. Within 10 working days following the adoption by the competent authority:
  - notification to the financial entity of the possibility of a decision being taken where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations issued by the Lead Overseer according to Article 42(4) of the DORA;
  - individual warnings issued by competent authorities according to Article 42(7) of the DORA and relevant information which allows the Lead Overseer to assess whether such warnings have resulted in consistent approaches mitigating the potential risk to financial stability.
- b. Within 10 working days following the consultation:
  - outcome of the consultation with NIS2 authorities prior to taking a decision, as referred to in Article 42(5) of the DORA, where possible.
- c. Within 10 working days following the receipt of the information from financial entities: - the material changes to existing contractual arrangements of financial entities with critical ICT third-party service providers which were made to address the risks identified in the recommendations issued by the Lead Overseer; - the start of executing exit strategies and transition plans of the financial entities as referred to in Article 28(8) of the DORA.

11.3 The ESAs, in consultation with competent authorities, should develop a template to facilitate the transmission of the information as defined in point 11.3.

## **Guideline 12: Decision requiring financial entities to temporarily suspend the use or deployment of a service provided by the critical ICT third-party service provider or terminate the relevant contractual arrangements concluded with the critical ICT third-party service provider**

12.1 The competent authorities should inform the Lead Overseer of their intention to notify a financial entity of the possibility of a decision being taken if the financial entity does not adopt appropriate contractual arrangements to address the specific risks identified in the recommendations, as referred to in Article 42(4) of the DORA. For the purpose of application of point 12.2, the competent authorities should make available to the Lead Overseer all relevant information regarding the possible decision and highlight if they intend to adopt an urgent decision.

12.2 After the receipt of the information, the Lead Overseer should assess the potential impact such decision might have for the critical ICT third-party service provider whose service would be temporarily suspended or terminated. Within 10 working days from the receipt of the information or with the shortest possible delay in case the competent authorities intend to adopt an urgent decision, the Lead Overseer should make that assessment available to the competent authorities concerned. Competent authorities should consider that non-binding assessment when deciding whether or not to issue the notification referred to in point 12.1.

12.3 Where two or more competent authorities plan to take or have taken decisions regarding financial entities making use of ICT services provided by the same critical ICT third-party service provider, the Lead Overseer should inform them about any inconsistent or divergent supervisory approaches that could lead to an unlevel playing field where financial entities are using the ICT services provided by a critical ICT third-party service provider across Member States.

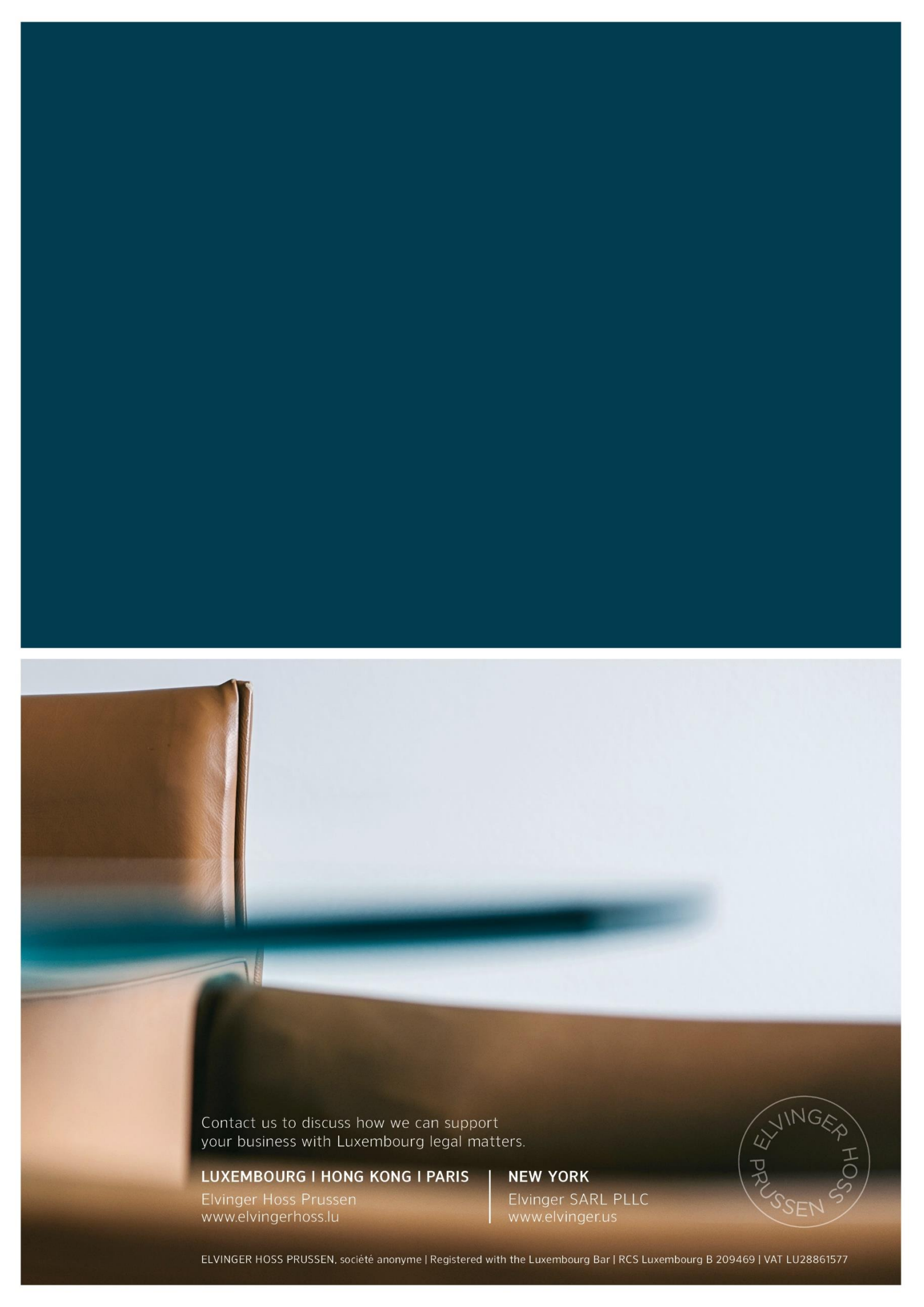
### **Section 5: Final provisions**

These Guidelines apply from 17 January 2025.

These Guidelines will be subject to a review by the ESAs.







Contact us to discuss how we can support  
your business with Luxembourg legal matters.

**LUXEMBOURG | HONG KONG | PARIS**

Elvinger Hoss Prussen  
[www.elvingerhoss.lu](http://www.elvingerhoss.lu)

**NEW YORK**

Elvinger SARL PLLC  
[www.elvinger.us](http://www.elvinger.us)

