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

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 ([31]), 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 ([32]);

(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;

(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;

(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

(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

(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;

(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 (35);

(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 (36);

(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.

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. 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.

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.

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:

(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.

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 via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 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 via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 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 (37), 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.

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:

(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.

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:

(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-par ty 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. 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.

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.

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.

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-par ty ser vice 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:

   (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 places 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 (38);

(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;

(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.

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 .

(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 .

(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 (*), 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.

(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 .

(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

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.