Official Journal of the European Union

L 333

English edition

Legislation

Volume 65

27 December 2022

Contents

[1] Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance

([1]) OJ C 343, 26.8.2021, p. 1.
([2]) OJ C 155, 30.4.2021, p. 38.
([3]) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

intermediaries offering their services online operating with InsurTech, to digital insurance underwriting. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.

(3) The European Systemic Risk Board (ESRB) reaffirmed in a 2020 report addressing systemic cyber risk how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, could constitute a systemic vulnerability because localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches that occur in the financial sector do not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union's financial system, such as generating liquidity runs and an overall loss of confidence and trust in financial markets.

(4) In recent years, ICT risk has attracted the attention of international, Union and national policy makers, regulators and standard-setting bodies in an attempt to enhance digital resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the Financial Stability Board, the Financial Stability Institute, as well as the G7 and G20 aim to provide competent authorities and market operators across various jurisdictions with tools to bolster the resilience of their financial systems. That work has also been driven by the need to duly consider ICT risk in the context of a highly interconnected global financial system and to seek more consistency of relevant best practices.

(5) Despite Union and national targeted policy and legislative initiatives, ICT risk continues to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reforms that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed to safeguard the competitiveness and stability of the Union from economic, prudential and market conduct perspectives. Although ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-financial crisis regulatory agenda and have developed in only some areas of the Union's financial services policy and regulatory landscape, or in only a few Member States.

(6) In its Communication of 8 March 2018 entitled 'FinTech Action plan: For a more competitive and innovative European financial sector', the Commission highlighted the paramount importance of making the Union financial sector more resilient, including from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling the effective and smooth provision of financial services across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence.

(7) In April 2019, the European Supervisory Authority (European Banking Authority), (EBA) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([4]), the European Supervisory Authority (European Insurance and Occupational Pensions Authority), ('EIOPA') established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([5]) and the European Supervisory Authority (European Securities and Markets Authority), ('ESMA') established by Regulation (EU) No 1095/2010 of the

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

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

European Parliament and of the Council ([6]) (known collectively as 'European Supervisory Authorities' or 'ESAs') jointly issued technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a sector-specific initiative of the Union.

(8) The Union financial sector is regulated by a Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not yet fully or consistently harmonised, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than, for example, common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover digital operational resilience, by strengthening the mandates of competent authorities to enable them to supervise the management of ICT risk in the financial sector in order to protect the integrity and efficiency of the internal market, and to facilitate its orderly functioning.

(9) Legislative disparities and uneven national regulatory or supervisory approaches with regard to ICT risk trigger obstacles to the functioning of the internal market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities operating on a cross-border basis. Competition between the same type of financial entities operating in different Member States could also be distorted. This is the case, in particular, for areas where Union harmonisation has been very limited, such as digital operational resilience testing, or absent, such as the monitoring of ICT third-party risk. Disparities stemming from developments envisaged at national level could generate further obstacles to the functioning of the internal market to the detriment of market participants and financial stability.

(10) To date, due to the ICT risk related provisions being only partially addressed at Union level, there are gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and inconsistencies as a result of emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user such as the financial sector since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, each issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risk and mitigating adverse impacts of ICT incidents on their own and in a coherent cost-effective way.

(11) As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework, further harmonisation of key digital operational resilience requirements for all financial entities is required. The development of ICT capabilities and overall resilience by financial entities, based on those key requirements, with a view to withstanding operational outages, would help preserve the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims to contribute to the smooth functioning of the internal market, it should be based on the provisions of Article 114 of the Treaty on the Functioning of the European Union (TFEU) as interpreted in accordance with the consistent case law of the Court of Justice of the European Union (Court of Justice).

(12) This Regulation aims to consolidate and upgrade ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts. While those acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they did not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk rules, when further developed in those Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risk) rather than targeted qualitative rules for the protection, detection, containment, recovery and repair capabilities against ICT-related

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

incidents, or for reporting and digital testing capabilities. Those acts were primarily meant to cover and update essential rules on prudential supervision, market integrity or conduct. By consolidating and upgrading the different rules on ICT risk, all provisions addressing digital risk in the financial sector should for the first time be brought together in a consistent manner in one single legislative act. Therefore, this Regulation fills in the gaps or remedies inconsistencies in some of the prior legal acts, including in relation to the terminology used therein, and explicitly refers to ICT risk via targeted rules on ICT risk-management capabilities, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation should thus also raise awareness of ICT risk and acknowledge that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of financial entities.

(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of high reliance on ICT systems, platforms and infrastructures, which entails increased digital risk. Observing basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.

(14) A Regulation helps reduce regulatory complexity, fosters supervisory convergence and increases legal certainty, and also contributes to limiting compliance costs, especially for financial entities operating across borders, and to reducing competitive distortions. Therefore, the choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities is the most appropriate way to guarantee a homogenous and coherent application of all components of ICT risk management by the Union financial sector.

(15) Directive (EU) 2016/1148 of the European Parliament and of the Council ([7]) was the first horizontal cybersecurity framework enacted at Union level, applying also to three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 set out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties that were identified by the Member States, have been brought into its scope in practice, and hence required to comply with the ICT security and incident notification requirements laid down in it. Directive (EU) 2022/2555 of the European Parliament and of the Council ([8]) sets a uniform criterion to determine the entities falling within its scope of application (size-cap rule) while also keeping the three types of financial entities in its scope.

(16) However, as this Regulation increases the level of harmonisation of the various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law, this higher level constitutes an increased harmonisation also in comparison with the requirements laid down in Directive (EU) 2022/2555. Consequently, this Regulation constitutes *lex specialis* with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive.

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

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

(17) In accordance with Article 4(2) of the Treaty on European Union and without prejudice to the judicial review by the Court of Justice, this Regulation should not affect the responsibility of Member States with regard to essential State functions concerning public security, defence and the safeguarding of national security, for example concerning the supply of information which would be contrary to the safeguarding of national security.

(18) To enable cross-sector learning and to effectively draw on experiences of other sectors in dealing with cyber threats, the financial entities referred to in Directive (EU) 2022/2555 should remain part of the 'ecosystem' of that Directive (for example, Cooperation Group and computer security incident response teams (CSIRTs)).The ESAs and national competent authorities should be able to participate in the strategic policy discussions and the technical workings of the Cooperation Group under that Directive, and to exchange information and further cooperate with the single points of contact designated or established in accordance with that Directive. The competent authorities under this Regulation should also consult and cooperate with the CSIRTs. The competent authorities should also be able to request technical advice from the competent authorities designated or established in accordance with Directive (EU) 2022/2555 and establish cooperation arrangements that aim to ensure effective and fast-response coordination mechanisms.

(19) Given the strong interlinkages between the digital resilience and the physical resilience of financial entities, a coherent approach with regard to the resilience of critical entities is necessary in this Regulation and Directive (EU) 2022/2557 of the European Parliament and the Council ([9]). Given that the physical resilience of financial entities is addressed in a comprehensive manner by the ICT risk management and reporting obligations covered by this Regulation, the obligations laid down in Chapters III and IV of Directive (EU) 2022/2557 should not apply to financial entities falling within the scope of that Directive.

(20) Cloud computing service providers are one category of digital infrastructure covered by Directive (EU) 2022/2555. The Union Oversight Framework ('Oversight Framework') established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers providing ICT services to financial entities, and should be considered complementary to the supervision carried out pursuant to Directive (EU) 2022/2555. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal framework establishing a digital oversight authority.

(21) In order to maintain full control over ICT risk, financial entities need to have comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Likewise, financial entities should have policies in place for the testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. The digital operational resilience baseline for financial entities should be increased while also allowing for a proportionate application of requirements for certain financial entities, particularly microenterprises, as well as financial entities subject to a simplified ICT risk management framework. To facilitate an efficient supervision of institutions for occupational retirement provision that is proportionate and addresses the need to reduce administrative burdens on the competent authorities, the relevant national supervisory arrangements in respect of such financial entities should take into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations even when the relevant thresholds established in Article 5 of Directive (EU) 2016/2341 of the European Parliament and of the Council ([10]) are exceeded. In particular, supervisory activities should focus primarily on the need to address serious risks associated with the ICT risk management of a particular entity.

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

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

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

(22) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through the relevant work undertaken by the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council ([11]) and the Cooperation Group under Directive (EU) 2022/2555, divergent approaches on setting the thresholds and use of taxonomies still exist, or can emerge, for the remainder of financial entities. Due to those divergences, there are multiple requirements that financial entities must comply with, especially when operating across several Member States and when part of a financial group. Moreover, such divergences have the potential to hinder the creation of further uniform or centralised Union mechanisms that speed up the reporting process and support a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risk in the event of large-scale attacks with potentially systemic consequences.

(23) To reduce the administrative burden and potentially duplicative reporting obligations for certain financial entities, the requirement for the incident reporting pursuant to Directive (EU) 2015/2366 of the European Parliament and of the Council ([12]) should cease to apply to payment service providers that fall within the scope of this Regulation. Consequently, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of that Directive, should, from the date of application of this Regulation, report pursuant to this Regulation, all operational or security payment-related incidents which have been previously reported pursuant to that Directive, irrespective of whether such incidents are ICT-related.

(24) To enable competent authorities to fulfil supervisory roles by acquiring a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to enhance the exchange of information between relevant public authorities, including law enforcement authorities and resolution authorities, this Regulation should lay down a robust ICT-related incident reporting regime whereby the relevant requirements address current gaps in financial services law, and remove existing overlaps and duplications to alleviate costs. It is essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities through a single streamlined framework as set out in this Regulation. In addition, the ESAs should be empowered to further specify relevant elements for the ICT-related incident reporting framework, such as taxonomy, timeframes, data sets, templates and applicable thresholds. To ensure full consistency with Directive (EU) 2022/2555, financial entities should be allowed, on a voluntary basis, to notify significant cyber threats to the relevant competent authority, when they consider that the cyber threat is of relevance to the financial system, service users or clients.

(25) Digital operational resilience testing requirements have been developed in certain financial subsectors setting out frameworks that are not always fully aligned. This leads to a potential duplication of costs for cross-border financial entities and makes the mutual recognition of the results of digital operational resilience testing complex which, in turn, can fragment the internal market.

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

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

(26) In addition, where no ICT testing is required, vulnerabilities remain undetected and result in exposing a financial entity to ICT risk and ultimately create a higher risk to the stability and integrity of the financial sector. Without Union intervention, digital operational resilience testing would continue to be inconsistent and would lack a system of mutual recognition of ICT testing results across different jurisdictions. In addition, as it is unlikely that other financial subsectors would adopt testing schemes on a meaningful scale, they would miss out on the potential benefits of a testing framework, in terms of revealing ICT vulnerabilities and risks, and testing defence capabilities and business continuity, which contributes to increasing the trust of customers, suppliers and business partners. To remedy those overlaps, divergences and gaps, it is necessary to lay down rules for a coordinated testing regime and thereby facilitate the mutual recognition of advanced testing for financial entities meeting the criteria set out in this Regulation.

(27) Financial entities' reliance on the use of ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in recent years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.

(28) The extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements to which they are subject, or otherwise in enforcing specific rights, such as access or audit rights, even when the latter are enshrined in their contractual arrangements. Moreover, many of those contractual arrangements do not provide for sufficient safeguards allowing for the fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess the associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors.

(29) Even though Union financial services law contains certain general rules on outsourcing, monitoring of the contractual dimension is not fully anchored into Union law. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. Those principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contractual arrangements with a view to providing certain minimum safeguards in order to strengthen financial entities' ability to effectively monitor all ICT risk emerging at the level of third-party service providers. Those principles are complementary to the sectoral law applicable to outsourcing.

(30) A certain lack of homogeneity and convergence regarding the monitoring of ICT third-party risk and ICT third-party dependencies is evident today. Despite efforts to address outsourcing, such as EBA Guidelines on outsourcing of 2019 and ESMA Guidelines on outsourcing to cloud service providers of 2021 the broader issue of counteracting systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is not sufficiently addressed by Union law. The lack of rules at Union level is compounded by the absence of national rules on mandates and tools that allow financial supervisors to acquire a good understanding of ICT third-party dependencies and to monitor adequately risks arising from the concentration of ICT third-party dependencies.

(31) Taking into account the potential systemic risk entailed by increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms in providing financial supervisors with adequate tools to quantify, qualify and redress the consequences of ICT risk occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical ICT third-party service providers to financial entities, while ensuring that the confidentiality and security of customers other than financial entities is preserved. While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment.

(32) With ICT risk becoming more and more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and to recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust and liability rules.

(33) In addition, doubts about the type of information that can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead to useful information being withheld. Therefore, the extent and quality of information sharing currently remains limited and fragmented, with relevant exchanges mostly being local (by way of national initiatives) and with no consistent Union-wide information-sharing arrangements tailored to the needs of an integrated financial system. It is therefore important to strengthen those communication channels.

(34) Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, and to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements. It is therefore necessary to enable the emergence at Union level of mechanisms for voluntary information-sharing arrangements which, when conducted in trusted environments, would help the community of the financial industry to prevent and collectively respond to cyber threats by quickly limiting the spread of ICT risk and impeding potential contagion throughout the financial channels. Those mechanisms should comply with the applicable competition law rules of the Union set out in the Communication from the Commission of 14 January 2011 entitled 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements', as well as with Union data protection rules, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council ([13]). They should operate based on the use of one or more of the legal bases that are laid down in Article 6 of that Regulation, such as in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in Article 6(1), point (f), of that Regulation, as well as in the context of the processing of personal data necessary for compliance with a legal obligation to which the controller is subject, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as referred to in Article 6(1), points (c) and (e), respectively, of that Regulation.

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

(35) In order to maintain a high level of digital operational resilience for the whole financial sector, and at the same time to keep pace with technological developments, this Regulation should address risk stemming from all types of ICT services. To that end, the definition of ICT services in the context of this Regulation should be understood in a broad manner, encompassing digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. That definition should, for instance, include so called 'over the top' services, which fall within the category of electronic communications services. It should exclude only the limited category of traditional analogue telephone services qualifying as Public Switched Telephone Network (PSTN) services, landline services, Plain Old Telephone Service (POTS), or fixed-line telephone services.

(36) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into account the significant differences between financial entities in terms of their size and overall risk profile. As a general principle, when distributing resources and capabilities for the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations, while competent authorities should continue to assess and review the approach of such distribution.

(37) Account information service providers, referred to in Article 33(1) of Directive (EU) 2015/2366, are explicitly included in the scope of this Regulation, taking into account the specific nature of their activities and the risks arising therefrom. In addition, electronic money institutions and payment institutions exempted pursuant to Article 9(1) of Directive 2009/110/EC of the European Parliament and of the Council ([14]) and Article 32(1) of Directive (EU) 2015/2366 are included in the scope of this Regulation even if they have not been granted authorisation in accordance Directive 2009/110/EC to issue electronic money, or if they have not been granted authorisation in accordance with Directive (EU) 2015/2366 to provide and execute payment services. However, post office giro institutions, referred to in Article 2(5), point (3), of Directive 2013/36/EU of the European Parliament and of the Council ([15]), are excluded from the scope of this Regulation. The competent authority for payment institutions exempted pursuant to Directive (EU) 2015/2366, electronic money institutions exempted pursuant to Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, should be the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366.

(38) As larger financial entities might enjoy wider resources and can swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities that are not microenterprises in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to set up an internal risk management and control model, and to submit their ICT risk management framework to internal audits.

(39) Some financial entities benefit from exemptions or are subject to a very light regulatory framework under the relevant sector-specific Union law. Such financial entities include managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU of the European Parliament and of the Council ([16]), insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC of the European Parliament and of the Council ([17]), and institutions for occupational retirement provision which operate pension schemes which together

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

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

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

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

do not have more than 15 members in total. In light of those exemptions it would not be proportionate to include such financial entities in the scope of this Regulation. In addition, this Regulation acknowledges the specificities of the insurance intermediation market structure, with the result that insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries qualifying as microenterprises or as small or medium-sized enterprises should not be subject to this Regulation.

(40) Since the entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU are excluded from the scope of that Directive, Member States should consequently be able to choose to exempt from the application of this Regulation such entities located within their respective territories.

(41) Similarly, in order to align this Regulation to the scope of Directive 2014/65/EU of the European Parliament and of the Council ([18]), it is also appropriate to exclude from the scope of this Regulation natural and legal persons referred in Articles 2 and 3 of that Directive which are allowed to provide investment services without having to obtain an authorisation under Directive 2014/65/EU. However, Article 2 of Directive 2014/65/EU also excludes from the scope of that Directive entities which qualify as financial entities for the purposes of this Regulation such as, central securities depositories, collective investment undertakings or insurance and reinsurance undertakings. The exclusion from the scope of this Regulation of the persons and entities referred to in Articles 2 and 3 of that Directive should not encompass those central securities depositories, collective investment undertakings or insurance and reinsurance undertakings.

(42) Under sector-specific Union law, some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. That category of financial entities includes small and non-interconnected investment firms, small institutions for occupational retirement provision which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total, as well as institutions exempted pursuant to Directive 2013/36/EU. Therefore, in accordance with the principle of proportionality and to preserve the spirit of sector-specific Union law, it is also appropriate to subject those financial entities to a simplified ICT risk management framework under this Regulation. The proportionate character of the ICT risk management framework covering those financial entities should not be altered by the regulatory technical standards that are to be developed by the ESAs. Moreover, in accordance with the principle of proportionality, it is appropriate to also subject payment institutions referred to in Article 32(1) of Directive (EU) 2015/2366 and electronic money institutions referred to in Article 9 of Directive 2009/110/EC exempted in accordance with national law transposing those Union legal acts to a simplified ICT risk management framework under this Regulation, while payment institutions and electronic money institutions which have not been exempted in accordance with their respective national law transposing sectoral Union law should comply with the general framework laid down by this Regulation.

(43) Similarly, financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework under this Regulation should not be required to establish a role to monitor their arrangements concluded with ICT third-party service providers on the use of ICT services; or to designate a member of senior management to be responsible for overseeing the related risk exposure and relevant documentation; to assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest; to document and review at least once a year the ICT risk management framework; to subject to internal audit on a regular basis the ICT risk management framework; to perform in-depth assessments after major changes in their network and information system infrastructures and processes; to regularly conduct risk analyses on legacy ICT systems; to subject the implementation of the ICT Response and Recovery plans to independent internal audit reviews; to have a crisis management function, to expand the testing of business continuity and response and recovery plans to capture switchover scenarios between primary ICT infrastructure and redundant facilities; to report to competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents, to maintain redundant ICT capacities; to communicate to national competent authorities implemented

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

changes following post ICT-related incident reviews; to monitor on a continuous basis relevant technological developments, to establish a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework provided for in this Regulation, or to adopt and regularly review a strategy on ICT third-party risk. In addition, microenterprises should only be required to assess the need to maintain such redundant ICT capacities based on their risk profile. Microenterprises should benefit from a more flexible regime as regards digital operational resilience testing programmes. When considering the type and frequency of testing to be performed, they should properly balance the objective of maintaining a high digital operational resilience, the available resources and their overall risk profile. Microenterprises and financial entities subject to the simplified ICT risk management framework under this Regulation should be exempted from the requirement to perform advanced testing of ICT tools, systems and processes based on threat-led penetration testing (TLPT), as only financial entities meeting the criteria set out in this Regulation should be required to carry out such testing. In light of their limited capabilities, microenterprises should be able to agree with the ICT third-party service provider to delegate the financial entity's rights of access, inspection and audit to an independent third-party, to be appointed by the ICT third-party service provider, provided that the financial entity is able to request, at any time, all relevant information and assurance on the ICT third-party service provider's performance from the respective independent third-party.

(44) As only those financial entities identified for the purposes of the advanced digital resilience testing should be required to conduct threat-led penetration tests, the administrative processes and financial costs entailed in the performance of such tests should be borne by a small percentage of financial entities.

(45) To ensure full alignment and overall consistency between financial entities' business strategies, on the one hand, and the conduct of ICT risk management, on the other hand, the financial entities' management bodies should be required to maintain a pivotal and active role in steering and adapting the ICT risk management framework and the overall digital operational resilience strategy. The approach to be taken by management bodies should not only focus on the means of ensuring the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness about cyber risks and a commitment to observe a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risk should be an overarching principle of that comprehensive approach, further translated into the continuous engagement of the management body in the control of the monitoring of the ICT risk management.

(46) Moreover, the principle of the management body's full and ultimate responsibility for the management of the ICT risk of the financial entity goes hand in hand with the need to secure a level of ICT-related investments and an overall budget for the financial entity that would enable the financial entity to achieve a high level of digital operational resilience.

(47) Inspired by relevant international, national and industry best practices, guidelines, recommendations and approaches to the management of cyber risk, this Regulation promotes a set of principles that facilitate the overall structure of ICT risk management. Consequently, as long as the main capabilities which financial entities put in place address the various functions in the ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities should remain free to use ICT risk management models that are differently framed or categorised.

(48) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and capable, not only for guaranteeing the processing of data required for their services, but also for ensuring sufficient technological resilience to allow them to deal adequately with additional processing needs due to stressed market conditions or other adverse situations.

(49) Efficient business continuity and recovery plans are necessary to allow financial entities to promptly and quickly resolve ICT-related incidents, in particular cyber-attacks, by limiting damage and giving priority to the resumption of activities and recovery actions in accordance with their back-up policies. However, such resumption should in no way jeopardise the integrity and security of the network and information systems or the availability, authenticity, integrity or confidentiality of data.

(50) While this Regulation allows financial entities to determine their recovery time and recovery point objectives in a flexible manner and hence to set such objectives by fully taking into account the nature and the criticality of the relevant functions and any specific business needs, it should nevertheless require them to carry out an assessment of the potential overall impact on market efficiency when determining such objectives.

(51) The propagators of cyber-attacks tend to pursue financial gains directly at the source, thus exposing financial entities to significant consequences. To prevent ICT systems from losing integrity or becoming unavailable, and hence to avoid data breaches and damage to physical ICT infrastructure, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined. ICT-related incident reporting should be harmonised through the introduction of a requirement for all financial entities to report directly to their relevant competent authorities. Where a financial entity is subject to supervision by more than one national competent authority, Member States should designate a single competent authority as the addressee of such reporting. Credit institutions classified as significant in accordance with Article 6(4) of Council Regulation (EU) No 1024/2013 ([19]) should submit such reporting to the national competent authorities, which should subsequently transmit the report to the European Central Bank (ECB).

(52) The direct reporting should enable financial supervisors to have immediate access to information about major ICT-related incidents. Financial supervisors should in turn pass on details of major ICT-related incidents to public non-financial authorities (such as competent authorities and single points of contact under Directive (EU) 2022/2555, national data protection authorities, and to law enforcement authorities for major ICT-related incidents of a criminal nature) in order to enhance such authorities awareness of such incidents and, in the case of CSIRTs, to facilitate prompt assistance that may be given to financial entities, as appropriate. Member States should, in addition, be able to determine that financial entities themselves should provide such information to public authorities outside the financial services area. Those information flows should allow financial entities to swiftly benefit from any relevant technical input, advice about remedies, and subsequent follow-up from such authorities. The information on major ICT-related incidents should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity, while the ESAs should share anonymised data on cyber threats and vulnerabilities relating to an incident, to aid wider collective defence.

(53) While all financial entities should be required to carry out incident reporting, that requirement is not expected to affect all of them in the same manner. Indeed, relevant materiality thresholds, as well as reporting timelines, should be duly adjusted, in the context of delegated acts based on the regulatory technical standards to be developed by the ESAs, with a view to covering only major ICT-related incidents. In addition, the specificities of financial entities should be taken into account when setting timelines for reporting obligations.

(54) This Regulation should require credit institutions, payment institutions, account information service providers and electronic money institutions to report all operational or security payment-related incidents – previously reported under Directive (EU) 2015/2366 – irrespective of the ICT nature of the incident.

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

(55) The ESAs should be tasked with assessing the feasibility and conditions for a possible centralisation of ICT-related incident reports at Union level. Such centralisation could consist of a single EU Hub for major ICT-related incident reporting either directly receiving relevant reports and automatically notifying national competent authorities, or merely centralising relevant reports forwarded by the national competent authorities and thus fulfilling a coordination role. The ESAs should be tasked with preparing, in consultation with the ECB and ENISA, a joint report exploring the feasibility of setting up a single EU Hub.

(56) In order to achieve a high level of digital operational resilience, and in line with both the relevant international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing) and with the frameworks applied in the Union, such as the TIBER-EU, financial entities should regularly test their ICT systems and staff having ICT-related responsibilities with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities. To reflect differences that exist across, and within, the various financial subsectors as regards financial entities' level of cybersecurity preparedness, testing should include a wide variety of tools and actions, ranging from the assessment of basic requirements (e.g. vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing) to more advanced testing by means of TLPT. Such advanced testing should be required only of financial entities that are mature enough from an ICT perspective to reasonably carry it out. The digital operational resilience testing required by this Regulation should thus be more demanding for those financial entities meeting the criteria set out in this Regulation (for example, large, systemic and ICT-mature credit institutions, stock exchanges, central securities depositories and central counterparties) than for other financial entities. At the same time, the digital operational resilience testing by means of TLPT should be more relevant for financial entities operating in core financial services subsectors and playing a systemic role (for example, payments, banking, and clearing and settlement), and less relevant for other subsectors (for example, asset managers and credit rating agencies).

(57) Financial entities involved in cross-border activities and exercising the freedoms of establishment, or of provision of services within the Union, should comply with a single set of advanced testing requirements (i.e. TLPT) in their home Member State, which should include the ICT infrastructures in all jurisdictions where the cross-border financial group operates within the Union, thus allowing such cross-border financial groups to incur related ICT testing costs in one jurisdiction only.

(58) To draw on the expertise already acquired by certain competent authorities, in particular with regard to implementing the TIBER-EU framework, this Regulation should allow Member States to designate a single public authority as responsible in the financial sector, at national level, for all TLPT matters, or competent authorities, to delegate, in the absence of such designation, the exercise of TLPT related tasks to another national financial competent authority.

(59) Since this Regulation does not require financial entities to cover all critical or important functions in one single threat-led penetration test, financial entities should be free to determine which and how many critical or important functions should be included in the scope of such a test.

(60) Pooled testing within the meaning of this Regulation – involving the participation of several financial entities in a TLPT and for which an ICT third-party service provider can directly enter into contractual arrangements with an external tester – should be allowed only where the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or the confidentiality of the data related to such services, are reasonably expected to be adversely impacted. Pooled testing should also be subject to safeguards (direction by one designated financial entity, calibration of the number of participating financial entities) to ensure a rigorous testing exercise for the financial entities involved which meet the objectives of the TLPT pursuant to this Regulation.

(61) In order to take advantage of internal resources available at corporate level, this Regulation should allow the use of internal testers for the purposes of carrying out TLPT, provided there is supervisory approval, no conflicts of interest, and periodical alternation of the use of internal and external testers (every three tests), while also requiring the provider of the threat intelligence in the TLPT to always be external to the financial entity. The responsibility for conducting TLPT should remain fully with the financial entity. Attestations provided by authorities should be solely for the purpose of mutual recognition and should not preclude any follow-up action needed to address the ICT risk to which the financial entity is exposed, nor should they be seen as a supervisory endorsement of a financial entity's ICT risk management and mitigation capabilities.

(62) To ensure a sound monitoring of ICT third-party risk in the financial sector, it is necessary to lay down a set of principle-based rules to guide financial entities' when monitoring risk arising in the context of functions outsourced to ICT third-party service providers, particularly for ICT services supporting critical or important functions, as well as more generally in the context of all ICT third-party dependencies.

(63) To address the complexity of the various sources of ICT risk, while taking into account the multitude and diversity of providers of technological solutions which enable a smooth provision of financial services, this Regulation should cover a wide range of ICT third-party service providers, including providers of cloud computing services, software, data analytics services and providers of data centre services. Similarly, since financial entities should effectively and coherently identify and manage all types of risk, including in the context of ICT services procured within a financial group, it should be clarified that undertakings which are part of a financial group and provide ICT services predominantly to their parent undertaking, or to subsidiaries or branches of their parent undertaking, as well as financial entities providing ICT services to other financial entities, should also be considered as ICT third-party service providers under this Regulation. Lastly, in light of the evolving payment services market becoming increasingly dependent on complex technical solutions, and in view of emerging types of payment services and payment-related solutions, participants in the payment services ecosystem, providing payment-processing activities, or operating payment infrastructures, should also be considered to be ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and public authorities when providing ICT related services in the context of fulfilling State functions.

(64) A financial entity should at all times remain fully responsible for complying with its obligations set out in this Regulation. Financial entities should apply a proportionate approach to the monitoring of risks emerging at the level of the ICT third-party service providers, by duly considering the nature, scale, complexity and importance of their ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.

(65) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated ICT third-party risk strategy, rooted in a continuous screening of all ICT third-party dependencies. To enhance supervisory awareness of ICT third-party dependencies, and with a view to further supporting the work in the context of the Oversight Framework established by this Regulation, all financial entities should be required to maintain a register of information with all contractual arrangements about the use of ICT services provided by ICT third-party service providers. Financial supervisors should be able to request the full register, or to ask for specific sections thereof, and thus to obtain essential information for acquiring a broader understanding of the ICT dependencies of financial entities.

(66) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, in particular by focusing on elements such as the criticality or importance of the services supported by the envisaged ICT contract, the necessary supervisory approvals or other conditions, the possible concentration risk entailed, as well as applying due diligence in the process of selection and assessment of ICT third-party service providers and assessing potential conflicts of interest. For contractual arrangements concerning critical or important functions, financial entities should take into consideration the use by ICT third-party service providers of the most up-to-date and highest information security standards. Termination of contractual arrangements could be prompted at least by a series of circumstances showing shortfalls at the ICT third-party service provider level, in

particular significant breaches of laws or contractual terms, circumstances revealing a potential alteration of the performance of the functions provided for in the contractual arrangements, evidence of weaknesses of the ICT third-party service provider in its overall ICT risk management, or circumstances indicating the inability of the relevant competent authority to effectively supervise the financial entity.

(67) To address the systemic impact of ICT third-party concentration risk, this Regulation promotes a balanced solution by means of taking a flexible and gradual approach to such concentration risk since the imposition of any rigid caps or strict limitations might hinder the conduct of business and restrain the contractual freedom. Financial entities should thoroughly assess their envisaged contractual arrangements to identify the likelihood of such risk emerging, including by means of in-depth analyses of subcontracting arrangements, in particular when concluded with ICT third-party service providers established in a third country. At this stage, and with a view to striking a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to set out rules on strict caps and limits to ICT third-party exposures. In the context of the Oversight Framework, a Lead Overseer, appointed pursuant to this Regulation, should, in respect to critical ICT third-party service providers, pay particular attention to fully grasp the magnitude of interdependences, discover specific instances where a high degree of concentration of critical ICT third-party service providers in the Union is likely to put a strain on the Union financial system's stability and integrity and maintain a dialogue with critical ICT third-party service providers where that specific risk is identified.

(68) To evaluate and monitor on a regular basis the ability of an ICT third party service provider to securely provide services to a financial entity without adverse effects on a financial entity's digital operational resilience, several key contractual elements with ICT third-party service providers should be harmonised. Such harmonisation should cover minimum areas which are crucial for enabling a full monitoring by the financial entity of the risks that could emerge from the ICT third-party service provider, from the perspective of a financial entity's need to secure its digital resilience because it is deeply dependent on the stability, functionality, availability and security of the ICT services received.

(69) When renegotiating contractual arrangements to seek alignment with the requirements of this Regulation, financial entities and ICT third-party service providers should ensure the coverage of the key contractual provisions as provided for in this Regulation.

(70) The definition of 'critical or important function' provided for in this Regulation encompasses the 'critical functions' as defined in Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council ([20]). Accordingly, functions deemed to be critical pursuant to Directive 2014/59/EU are included in the definition of critical functions within the meaning of this Regulation.

(71) Irrespective of the criticality or importance of the function supported by the ICT services, contractual arrangements should, in particular, provide for a specification of the complete descriptions of functions and services, of the locations where such functions are provided and where data is to be processed, as well as an indication of service level descriptions. Other essential elements to enable a financial entity's monitoring of ICT third party risk are: contractual provisions specifying how the accessibility, availability, integrity, security and protection of personal data are ensured by the ICT third-party service provider, provisions laying down the relevant guarantees for enabling the access, recovery and return of data in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, as well as provisions requiring the ICT third-party service provider to provide assistance in case of ICT incidents in connection with the services provided, at no additional cost or at a cost determined *ex-ante*; provisions on the obligation of the ICT third-party service provider

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

to fully cooperate with the competent authorities and resolution authorities of the financial entity; and provisions on termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities.

(72) In addition to such contractual provisions, and with a view to ensuring that financial entities remain in full control of all developments occurring at third-party level which may impair their ICT security, the contracts for the provision of ICT services supporting critical or important functions should also provide for the following: the specification of the full service level descriptions, with precise quantitative and qualitative performance targets, to enable without undue delay appropriate corrective actions when the agreed service levels are not met; the relevant notice periods and reporting obligations of the ICT third-party service provider in the event of developments with a potential material impact on the ICT third-party service provider's ability to effectively provide their respective ICT services; a requirement upon the ICT third-party service provider to implement and test business contingency plans and have ICT security measures, tools and policies allowing for the secure provision of services, and to participate and fully cooperate in the TLPT carried out by the financial entity.

(73) Contracts for the provision of ICT services supporting critical or important functions should also contain provisions enabling the rights of access, inspection and audit by the financial entity, or an appointed third party, and the right to take copies as crucial instruments in the financial entities' ongoing monitoring of the ICT third-party service provider's performance, coupled with the service provider's full cooperation during inspections. Similarly, the competent authority of the financial entity should have the right, based on notices, to inspect and audit the ICT third-party service provider, subject to the protection of confidential information.

(74) Such contractual arrangements should also provide for dedicated exit strategies to enable, in particular, mandatory transition periods during which ICT third-party service providers should continue providing the relevant services with a view to reducing the risk of disruptions at the level of the financial entity, or to allow the latter effectively to switch to the use of other ICT third-party service providers or, alternatively, to change to in-house solutions, consistent with the complexity of the provided ICT service. Moreover, financial entities within the scope of Directive 2014/59/EU should ensure that the relevant contracts for ICT services are robust and fully enforceable in the event of resolution of those financial entities. Therefore, in line with the expectations of the resolution authorities, those financial entities should ensure that the relevant contracts for ICT services are resolution resilient. As long as they continue meeting their payment obligations, those financial entities should ensure, among other requirements, that the relevant contracts for ICT services contain clauses for non-termination, non-suspension and non-modification on grounds of restructuring or resolution.

(75) Moreover, the voluntary use of standard contractual clauses developed by public authorities or Union institutions, in particular the use of contractual clauses developed by the Commission for cloud computing services could provide further comfort to the financial entities and ICT third-party service providers, by enhancing their level of legal certainty regarding the use of cloud computing services in the financial sector, in full alignment with the requirements and expectations set out by the Union financial services law. The development of standard contractual clauses builds on measures already envisaged in the 2018 Fintech Action Plan that announced the Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders' efforts, which the Commission has facilitated with the help of the financial sector's involvement.

(76) With a view to promoting convergence and efficiency in relation to supervisory approaches when addressing ICT third-party risk in the financial sector, as well as to strengthening the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the provision of ICT services that support the supply of financial services, and thereby to contributing to the preservation of the Union's financial system stability and the integrity of the internal market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework. While the set-up of the Oversight Framework is justified by the added value of taking action at Union level and by virtue of the inherent role and specificities of the use of ICT services in

the provision of financial services, it should be recalled, at the same time, that this solution appears suitable only in the context of this Regulation specifically dealing with digital operational resilience in the financial sector. However, such Oversight Framework should not be regarded as a new model for Union supervision in other areas of financial services and activities.

(77) The Oversight Framework should apply only to critical ICT third-party service providers. There should therefore be a designation mechanism to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers. That mechanism should involve a set of quantitative and qualitative criteria to set the criticality parameters as a basis for inclusion in the Oversight Framework. In order to ensure the accuracy of that assessment, and regardless of the corporate structure of the ICT third-party service provider, such criteria should, in the case of a ICT third-party service provider that is part of a wider group, take into consideration the entire ICT third-party service provider's group structure. On the one hand, critical ICT third-party service providers, which are not automatically designated by virtue of the application of those criteria, should have the possibility to opt in to the Oversight Framework on a voluntary basis, on the other hand, ICT third-party service providers, that are already subject to oversight mechanism frameworks supporting the fulfilment of the tasks of the European System of Central Banks as referred to in Article 127(2) TFEU, should be exempted.

(78) Similarly, financial entities providing ICT services to other financial entities, while belonging to the category of ICT third-party service providers under this Regulation, should also be exempted from the Oversight Framework since they are already subject to supervisory mechanisms established by the relevant Union financial services law. Where applicable, competent authorities should take into account, in the context of their supervisory activities, the ICT risk posed to financial entities by financial entities providing ICT services. Likewise, due to the existing risk monitoring mechanisms at group level, the same exemption should be introduced for ICT third-party service providers delivering services predominantly to the entities of their own group. ICT third-party service providers providing ICT services solely in one Member State to financial entities that are active only in that Member State should also be exempted from the designation mechanism because of their limited activities and lack of cross-border impact.

(79) The digital transformation experienced in financial services has brought about an unprecedented level of use of, and reliance upon, ICT services. Since it has become inconceivable to provide financial services without the use of cloud computing services, software solutions and data-related services, the Union financial ecosystem has become intrinsically co-dependent on certain ICT services provided by ICT service suppliers. Some of those suppliers, innovators in developing and applying ICT-based technologies, play a significant role in the delivery of financial services, or have become integrated into the financial services value chain. They have thus become critical to the stability and integrity of the Union financial system. This widespread reliance on services supplied by critical ICT third-party service providers, combined with the interdependence of the information systems of various market operators, create a direct, and potentially severe, risk to the Union financial services system and to the continuity of delivery of financial services if critical ICT third-party service providers were to be affected by operational disruptions or major cyber incidents. Cyber incidents have a distinctive ability to multiply and propagate throughout the financial system at a considerably faster pace than other types of risk monitored in the financial sector and can extend across sectors and beyond geographical borders. They have the potential to evolve into a systemic crisis, where trust in the financial system has been eroded due to the disruption of functions supporting the real economy, or to substantial financial losses, reaching a level which the financial system is unable to withstand, or which requires the deployment of heavy shock absorption measures. To prevent these scenarios from taking place and thereby endangering the financial stability and integrity of the Union, it is essential to provide the convergence of supervisory practices relating to ICT third-party risk in finance, in particular through new rules enabling the Union oversight of critical ICT third-party service providers.

(80) The Oversight Framework largely depends on the degree of collaboration between the Lead Overseer and the critical ICT third-party service provider delivering to financial entities services affecting the supply of financial services. Successful oversight is predicated, inter alia, upon the ability of the Lead Overseer to effectively conduct monitoring missions and inspections to assess the rules, controls and processes used by the critical ICT third-party service providers, as well as to assess the potential cumulative impact of their activities on financial stability and the integrity of the financial system. At the same time, it is crucial that critical ICT third-party service providers follow the Lead Overseer's recommendations and address its concerns. Since a lack of cooperation by a critical ICT third-party service provider providing services that affect the supply of financial services, such as the refusal to grant access to its premises or to submit information, would ultimately deprive the Lead Overseer of its essential tools in appraising ICT third-party risk, and could adversely impact the financial stability and the integrity of the financial system, it is necessary to also provide for a commensurate sanctioning regime.

(81) Against this background, the need of the Lead Overseer to impose penalty payments to compel critical ICT third-party service providers to comply with the transparency and access-related obligations set out in this Regulation should not be jeopardised by difficulties raised by the enforcement of those penalty payments in relation to critical ICT third-party service providers established in third countries. In order to ensure the enforceability of such penalties, and to allow a swift roll out of procedures upholding the critical ICT third-party service providers' rights of defence in the context of the designation mechanism and the issuance of recommendations, those critical ICT third-party service providers, providing services to financial entities that affect the supply of financial services, should be required to maintain an adequate business presence in the Union. Due to the nature of the oversight, and the absence of comparable arrangements in other jurisdictions, there are no suitable alternative mechanisms ensuring this objective by way of effective cooperation with financial supervisors in third countries in relation to the monitoring of the impact of digital operational risks posed by systemic ICT third-party service providers, qualifying as critical ICT third-party service providers established in third countries. Therefore, in order to continue its provision of ICT services to financial entities in the Union, an ICT third-party service provider established in a third country which has been designated as critical in accordance with this Regulation should undertake, within 12 months of such designation, all necessary arrangements to ensure its incorporation within the Union, by means of establishing a subsidiary, as defined throughout the Union *acquis*, namely in Directive 2013/34/EU of the European Parliament and of the Council ([21]).

(82) The requirement to set up a subsidiary in the Union should not prevent the critical ICT third-party service provider from supplying ICT services and related technical support from facilities and infrastructure located outside the Union. This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union.

(83) Critical ICT third-party service providers should be able to provide ICT services from anywhere in the world, not necessarily or not only from premises located in the Union. Oversight activities should be first conducted on premises located in the Union and by interacting with entities located in the Union, including the subsidiaries established by critical ICT third-party service providers pursuant to this Regulation. However, such actions within the Union might be insufficient to allow the Lead Overseer to fully and effectively perform its duties under this Regulation. The Lead Overseer should therefore also be able to exercise its relevant oversight powers in third countries. Exercising those powers in third countries should allow the Lead Overseer to examine the facilities from which the ICT services or the technical support services are actually provided or managed by the critical ICT third-party service provider, and should give the Lead Overseer a comprehensive and operational understanding of the ICT risk management of the critical ICT third-party service provider. The possibility for the Lead Overseer, as a Union agency, to exercise powers outside the territory of the Union should be duly framed by relevant conditions, in particular the consent of the critical ICT third-party service provider concerned. Similarly, the relevant authorities of the third country should be informed of, and not have objected to, the exercise on their own territory of the activities of the Lead Overseer. However, in order to ensure efficient implementation, and without prejudice to the respective competences of the Union institutions and the Member States, such powers also need to be fully anchored in the conclusion of administrative cooperation arrangements with the relevant authorities of the third

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

country concerned. This Regulation should therefore enable the ESAs to conclude administrative cooperation arrangements with the relevant authorities of third countries, which should not otherwise create legal obligations in respect of the Union and its Member States.

(84) To facilitate communication with the Lead Overseer and to ensure adequate representation, critical ICT third-party service providers which are part of a group should designate one legal person as their coordination point.

(85) The Oversight Framework should be without prejudice to Member States' competence to conduct their own oversight or monitoring missions in respect to ICT third-party service providers which are not designated as critical under this Regulation, but which are regarded as important at national level.

(86) To leverage the multi-layered institutional architecture in the financial services area, the Joint Committee of the ESAs should continue to ensure overall cross-sectoral coordination in relation to all matters pertaining to ICT risk, in accordance with its tasks on cybersecurity. It should be supported by a new Subcommittee (the 'Oversight Forum') carrying out preparatory work both for the individual decisions addressed to critical ICT third-party service providers, and for the issuing of collective recommendations, in particular in relation to benchmarking the oversight programmes for critical ICT third-party service providers, and identifying best practices for addressing ICT concentration risk issues.

(87) To ensure that critical ICT third-party service providers are appropriately and effectively overseen on a Union level, this Regulation provides that any of the three ESAs could be designated as a Lead Overseer. The individual assignment of a critical ICT third-party service provider to one of the three ESAs should result from an assessment of the preponderance of financial entities operating in the financial sectors for which that ESA has responsibilities. This approach should lead to a balanced allocation of tasks and responsibilities between the three ESAs, in the context of exercising the oversight functions, and should make the best use of the human resources and technical expertise available in each of the three ESAs.

(88) Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third-party service providers and to obtain complete and updated information. Those powers should enable the Lead Overseer to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to financial entities and ultimately to the Union's financial system. Entrusting the ESAs with the lead oversight role is a prerequisite for understanding and addressing the systemic dimension of ICT risk in finance. The impact of critical ICT third-party service providers on the Union financial sector and the potential issues caused by the ICT concentration risk entailed call for taking a collective approach at Union level. The simultaneous carrying out of multiple audits and access rights, performed separately by numerous competent authorities, with little or no coordination among them, would prevent financial supervisors from obtaining a complete and comprehensive overview of ICT third-party risk in the Union, while also creating redundancy, burden and complexity for critical ICT third-party service providers if they were subject to numerous monitoring and inspection requests.

(89) Due to the significant impact of being designated as critical, this Regulation should ensure that the rights of critical ICT third-party service providers are observed throughout the implementation of the Oversight Framework. Prior to being designated as critical, such providers should, for example, have the right to submit to the Lead Overseer a reasoned statement containing any relevant information for the purposes of the assessment related to their designation. Since the Lead Overseer should be empowered to submit recommendations on ICT risk matters and suitable remedies thereto, which include the power to oppose certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system, critical ICT third-party service providers should also be given the opportunity to provide, prior to the finalisation of those recommendations, explanations regarding the expected impact of the solutions, envisaged in the recommendations, on customers that are entities falling outside the scope of this Regulation and to formulate solutions to mitigate risks. Critical ICT third-party service providers

disagreeing with the recommendations should submit a reasoned explanation of their intention not to endorse the recommendation. Where such reasoned explanation is not submitted or where it is considered to be insufficient, the Lead Overseer should issue a public notice summarily describing the matter of non-compliance.

(90) Competent authorities should duly include the task of verifying substantive compliance with recommendations issued by the Lead Overseer in their functions with regard to prudential supervision of financial entities. Competent authorities should be able to require financial entities to take additional measures to address the risks identified in the Lead Overseer's recommendations, and should, in due course, issue notifications to that effect. Where the Lead Overseer addresses recommendations to critical ICT third-party service providers that are supervised under Directive (EU) 2022/2555, the competent authorities should be able, on a voluntary basis and before adopting additional measures, to consult the competent authorities under that Directive in order to foster a coordinated approach to dealing with the critical ICT third-party service providers in question.

(91) The exercise of the oversight should be guided by three operational principles seeking to ensure: (a) close coordination among the ESAs in their Lead Overseer roles, through a joint oversight network (JON), (b) consistency with the framework established by Directive (EU) 2022/2555 (through a voluntary consultation of bodies under that Directive to avoid duplication of measures directed at critical ICT third-party service providers), and (c) applying diligence to minimise the potential risk of disruption to services provided by the critical ICT third-party service providers to customers that are entities falling outside the scope of this Regulation.

(92) The Oversight Framework should not replace, or in any way or for any part substitute for, the requirement for financial entities to manage themselves the risks entailed by the use of ICT third-party service providers, including their obligation to maintain an ongoing monitoring of contractual arrangements concluded with critical ICT third-party service providers. Similarly, the Oversight Framework should not affect the full responsibility of financial entities for complying with, and discharging, all the legal obligations laid down in this Regulation and in the relevant financial services law.

(93) To avoid duplications and overlaps, competent authorities should refrain from taking individually any measures aiming to monitor the critical ICT third-party service provider's risks and should, in that respect, rely on the relevant Lead Overseer's assessment. Any measures should in any case be coordinated and agreed in advance with the Lead Overseer in the context of the exercise of tasks in the Oversight Framework.

(94) To promote convergence at international level as regards the use of best practices in the review and monitoring of ICT third-party service providers' digital risk-management, the ESAs should be encouraged to conclude cooperation arrangements with relevant supervisory and regulatory third-country authorities.

(95) To leverage the specific competences, technical skills and expertise of staff specialising in operational and ICT risk within the competent authorities, the three ESAs and, on a voluntary basis, the competent authorities under Directive (EU) 2022/2555, the Lead Overseer should draw on national supervisory capabilities and knowledge and set up dedicated examination teams for each critical ICT third-party service provider, pooling multidisciplinary teams in support of the preparation and execution of oversight activities, including general investigations and inspections of critical ICT third-party service providers, as well as for any necessary follow-up thereto.

(96) Whereas costs resulting from oversight tasks would be fully funded from fees levied on critical ICT third-party service providers, the ESAs are. however, likely to incur, before the start of the Oversight Framework, costs for the implementation of dedicated ICT systems supporting the upcoming oversight, since dedicated ICT systems would need to be developed and deployed beforehand. This Regulation therefore provides for a hybrid funding model, whereby the Oversight Framework would, as such, be fully fee-funded, while the development of the ESAs' ICT systems would be funded from Union and national competent authorities' contributions.

(97) Competent authorities should have all required supervisory, investigative and sanctioning powers to ensure the proper exercise of their duties under this Regulation. They should, in principle, publish notices of the administrative penalties they impose. Since financial entities and ICT third-party service providers can be established in different Member States and supervised by different competent authorities, the application of this Regulation should be facilitated by, on the one hand, close cooperation among relevant competent authorities, including the ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013, and, on the other hand, by consultation with the ESAs through the mutual exchange of information and the provision of assistance in the context of relevant supervisory activities.

(98) In order to further quantify and qualify the criteria for the designation of ICT third-party service providers as critical and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Regulation by further specifying the systemic impact that a failure or operational outage of an ICT third-party service provider could have on the financial entities it provides ICT services to, the number of global systemically important institutions (G-SIIs), or other systemically important institutions (O-SIIs), that rely on the ICT third-party service provider in question, the number of ICT third-party service providers active on a given market, the costs of migrating data and ICT workloads to other ICT third-party service providers, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([22]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(99) Regulatory technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. In their roles as bodies endowed with highly specialised expertise, the ESAs should develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, major ICT-related incident reporting, testing, as well as in relation to key requirements for a sound monitoring of ICT third-party risk. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations. The Commission should be empowered to adopt those regulatory technical standards by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

(100) To facilitate the comparability of reports on major ICT-related incidents and major operational or security payment-related incidents, as well as to ensure transparency regarding contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident and a major operational or security payment-related incident, as well as standardised templates for the register of information. When developing those standards, the ESAs should take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

([22]) OJ L 123, 12.5.2016, p. 1.

(101) Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009 ([23]), (EU) No 648/2012 ([24]), (EU) No 600/2014 ([25]) and (EU) No 909/2014 ([26]) of the European Parliament and of the Council, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.

(102) Since this Regulation, together with Directive (EU) 2022/2556 of the European Parliament and of the Council ([27]), entails a consolidation of the ICT risk management provisions across multiple regulations and directives of the Union's financial services *acquis*, including Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, and Regulation (EU) 2016/1011 of the European Parliament and of the Council ([28]), in order to ensure full consistency, those Regulations should be amended to clarify that the applicable ICT risk-related provisions are laid down in this Regulation.

(103) Consequently, the scope of the relevant articles related to operational risk, upon which empowerments laid down in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 had mandated the adoption of delegated and implementing acts, should be narrowed down with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those Regulations.

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

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

([24]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

([25]) Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

([26]) Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

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

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

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

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

HAVE ADOPTED THIS REGULATION:

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.

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

[30] OJ C 229, 15.6.2021, p. 16.

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 ([33]);

(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 2009/138/EC;

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

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

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

(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 ([34]);

(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.

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

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

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

Article 4

Proportionality principle

1. Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

2. In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.

3. The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework on the basis of the reports submitted upon the request of competent authorities pursuant to Article 6(5) and Article 16(2).

CHAPTER II

ICT risk management

Section I

Article 5

Governance and organisation

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

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

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

(a) bear the ultimate responsibility for managing the financial entity's ICT risk;

(b) put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;

(c) set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;

(d) bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);

(e) approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan;

(f) approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;

(g) allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff;

(h) approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;

(i) put in place, at corporate level, reporting channels enabling it to be duly informed of the following:

(i) arrangements concluded with ICT third-party service providers on the use of ICT services,

(ii) any relevant planned material changes regarding the ICT third-party service providers,

(iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.

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

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

Section II

Article 6

ICT risk management framework

1. Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.

2. The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.

3. In accordance with their ICT risk management framework, financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.

4. Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.

5. The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.

6. The ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.

7. Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings.

8. The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:

(a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;

(b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;

(c) setting out clear information security objectives, including key performance indicators and key risk metrics;

(d) explaining the ICT reference architecture and any changes needed to reach specific business objectives;

(e) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;

(f) evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;

(g) implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;

(h) outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.

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

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

Article 7

ICT systems, protocols and tools

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

(a) appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4;

(b) reliable;

(c) equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced;

(d) technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.

Article 8

Identification

1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.

2. Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.

3. Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.

4. Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.

5. Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.

6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.

7. Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.

Article 9

Protection and prevention

1. For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.

2. Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.

3. In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4. Those ICT solutions and processes shall:

(a) ensure the security of the means of transfer of data;

(b) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;

(c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;

(d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

4. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:

(a) develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable;

(b) following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks;

(c) implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;

(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;

(e) implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;

(f) have appropriate and comprehensive documented policies for patches and updates.

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

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

Article 10

Detection

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

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

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

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

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

Article 11

Response and recovery

1. As part of the ICT risk management framework referred to in Article 6(1) and based on the identification requirements set out in Article 8, financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.

2. Financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to:

(a) ensure the continuity of the financial entity's critical or important functions;

(b) quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions;

(c) activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12;

(d) estimate preliminary impacts, damages and losses;

(e) set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.

3. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to independent internal audit reviews.

4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.

5. As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities shall assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.

6. As part of their comprehensive ICT risk management, financial entities shall:

(a) test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions;

(b) test the crisis communication plans established in accordance with Article 14.

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

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

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

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

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

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

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

Article 12

Backup policies and procedures, restoration and recovery procedures and methods

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

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

(b) restoration and recovery procedures and methods.

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

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

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

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

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

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

The secondary processing site shall be:

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

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

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

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

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

Article 13

Learning and evolving

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

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

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

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

(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;

(b) the quality and speed of performing a forensic analysis, where deemed appropriate;

(c) the effectiveness of incident escalation within the financial entity;

(d) the effectiveness of internal and external communication.

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

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

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

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

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

Article 14

Communication

1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.

2. As part of the ICT risk management framework, financial entities shall implement communication policies for internal staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed.

3. At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose.

Article 15

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

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

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

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

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

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

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

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

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

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

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

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 in accordance with paragraph 4 of this Article.

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

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

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

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

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

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

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

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

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

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

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

(a) an initial notification;

(b) an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;

(c) a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.

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

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

(a) EBA, ESMA or EIOPA;

(b) the ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d);

(c) the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;

(d) the resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014 of the European Parliament and of the Council ([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.

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

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-party risk

Article 28

General principles

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

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

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

(i) the nature, scale, complexity and importance of ICT-related dependencies,

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

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

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

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

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

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

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

4. Before entering into a contractual arrangement on the use of ICT services, financial entities shall:

(a) assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;

(b) assess if supervisory conditions for contracting are met;

(c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29;

(d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;

(e) identify and assess conflicts of interest that the contractual arrangement may cause.

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

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

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

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

(a) significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;

(b) circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;

(c) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;

(d) where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.

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

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

(a) disruption to their business activities,

(b) limiting compliance with regulatory requirements,

(c) detriment to the continuity and quality of services provided to clients.

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

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

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

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

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-party service providers

Article 31

Designation of critical ICT third-party service providers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) financial entities providing ICT services to other financial entities;

(ii) ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union;

(iii) ICT intra-group service providers;

(iv) ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State.

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

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

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

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

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

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

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

Article 32

Structure of the Oversight Framework

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

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

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

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

4. The Oversight Forum shall be composed of:

(a) the Chairpersons of the ESAs;

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

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

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

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

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

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

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

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

The independent experts shall be appointed on the basis of their expertise in financial stability, digital operational resilience and ICT security matters. They shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.

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

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

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

Article 33

Tasks of the Lead Overseer

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

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

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

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

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

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

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

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

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

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

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

(h) the ICT audits;

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

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

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

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

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

Article 34

Operational coordination between Lead Overseers

1. To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed in accordance with Article 31(1), point (b), shall set up a JON to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third-party service providers, as well as in the course of any action that may be needed pursuant to Article 42.

2. For the purposes of paragraph 1, the Lead Overseers shall draw up a common oversight protocol specifying the detailed procedures to be followed for carrying out the day-to-day coordination and for ensuring swift exchanges and reactions. The protocol shall be periodically revised to reflect operational needs, in particular the evolution of practical oversight arrangements.

3. The Lead Overseers may, on an ad-hoc basis, call on the ECB and ENISA to provide technical advice, share hands-on experience or join specific coordination meetings of the JON.

Article 35

Powers of the Lead Overseer

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

(a) to request all relevant information and documentation in accordance with Article 37;

(b) to conduct general investigations and inspections in accordance with Articles 38 and 39, respectively;

(c) to request, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to the recommendations referred to in point (d) of this paragraph;

(d) to issue recommendations on the areas referred to in Article 33(3), in particular concerning the following:

(i) the use of specific ICT security and quality requirements or processes, in particular in relation to the roll-out of patches, updates, encryption and other security measures which the Lead Overseer deems relevant for ensuring the ICT security of services provided to financial entities;

(ii) the use of conditions and terms, including their technical implementation, under which the critical ICT third-party service providers provide ICT services to financial entities, which the Lead Overseer deems relevant for preventing the generation of single points of failure, the amplification thereof, or for minimising the possible systemic impact across the Union's financial sector in the event of ICT concentration risk;

(iii) any planned subcontracting, where the Lead Overseer deems that further subcontracting, including subcontracting arrangements which the critical ICT third-party service providers plan to enter into with ICT third-party service providers or with ICT subcontractors established in a third country, may trigger risks for the provision of services by the financial entity, or risks to the financial stability, based on the examination of the information gathered in accordance with Articles 37 and 38;

(iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:

— the envisaged subcontractor is an ICT third-party service provider or an ICT subcontractor established in a third country;

— the subcontracting concerns critical or important functions of the financial entity; and

— the Lead Overseer deems that the use of such subcontracting poses a clear and serious risk to the financial stability of the Union or to financial entities, including to the ability of financial entities to comply with supervisory requirements.

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

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

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

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

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

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

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

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

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

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

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

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

(a) the gravity and the duration of non-compliance;

(b) whether non-compliance has been committed intentionally or negligently;

(c) the level of cooperation of the ICT third-party service provider with the Lead Overseer.

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

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

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

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

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

Article 36

Exercise of the powers of the Lead Overseer outside the Union

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

(a) in Article 35(1), point (a); and

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

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

(i) the conduct of an inspection in a third-country is deemed necessary by the Lead Overseer to allow it to fully and effectively perform its duties under this Regulation;

(ii) the inspection in a third-country is directly related to the provision of ICT services to financial entities in the Union;

(iii) the critical ICT third-party service provider concerned consents to the conduct of an inspection in a third-country; and

(iv) the relevant authority of the third-country concerned has been officially notified by the Lead Overseer and raised no objection thereto.

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

Those cooperation arrangements shall specify at least the following elements:

(a) the procedures for the coordination of oversight activities carried out under this Regulation and any analogous monitoring of ICT third-party risk in the financial sector exercised by the relevant authority of the third country concerned, including details for transmitting the agreement of the latter to allow the conduct, by the Lead Overseer and its designated team, of general investigations and on-site inspections as referred to in paragraph 1, first subparagraph, on the territory under its jurisdiction;

(b) the mechanism for the transmission of any relevant information between EBA, ESMA or EIOPA and the relevant authority of the third country concerned, in particular in connection with information that may be requested by the Lead Overseer pursuant to Article 37;

(c) the mechanisms for the prompt notification by the relevant authority of the third-country concerned to EBA, ESMA or EIOPA of cases where an ICT third-party service provider established in a third country and designated as critical in accordance with Article 31(1), point (a), is deemed to have infringed the requirements to which it is obliged to adhere pursuant to the applicable law of the third country concerned when providing services to financial institutions in that third country, as well as the remedies and penalties applied;

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

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

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

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

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

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

Article 37

Request for information

1. The Lead Overseer may, by simple request or by decision, require critical ICT third-party service providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.

2. When sending a simple request for information under paragraph 1, the Lead Overseer shall:

(a) refer to this Article as the legal basis of the request;

(b) state the purpose of the request;

(c) specify what information is required;

(d) set a time limit within which the information is to be provided;

(e) inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but in the event of a voluntary reply to the request the information provided must not be incorrect or misleading.

3. When requiring by decision to supply information under paragraph 1, the Lead Overseer shall:

(a) refer to this Article as the legal basis of the request;

(b) state the purpose of the request;

(c) specify what information is required;

(d) set a time limit within which the information is to be provided;

(e) indicate the periodic penalty payments provided for in Article 35(6) where the production of the required information is incomplete or when such information is not provided within the time limit referred to in point (d) of this paragraph;

(f) indicate the right to appeal the decision to ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union (Court of Justice) in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

4. The representatives of the critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.

5. The Lead Overseer shall, without delay, transmit a copy of the decision to supply information to the competent authorities of the financial entities using the services of the relevant critical ICT third-party service providers and to the JON.

Article 38

General investigations

1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the joint examination team referred to in Article 40(1), may, where necessary, conduct investigations of critical ICT third-party service providers.

2. The Lead Overseer shall have the power to:

(a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;

(b) take or obtain certified copies of, or extracts from, such records, data, documented procedures and any other material;

(c) summon representatives of the critical ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;

(d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(e) request records of telephone and data traffic.

3. The officials and other persons authorised by the Lead Overseer for the purposes of the investigation referred to in paragraph 1 shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the investigation.

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

4. The representatives of the critical ICT third-party service providers are required to submit to the investigations on the basis of a decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the investigation, the periodic penalty payments provided for in Article 35(6), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, and the right to have the decision reviewed by the Court of Justice.

5. In good time before the start of the investigation, the Lead Overseer shall inform competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider of the envisaged investigation and of the identity of the authorised persons.

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

Article 39

Inspections

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

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

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

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

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

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

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

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

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

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

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

Article 40

Ongoing oversight

1. When conducting oversight activities, in particular general investigations or inspections, the Lead Overseer shall be assisted by a joint examination team established for each critical ICT third-party service provider.

2. The joint examination team referred to in paragraph 1 shall be composed of staff members from:

(a) the ESAs;

(b) the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides ICT services;

(c) the national competent authority referred to in Article 32(4), point (e), on a voluntary basis;

(d) one national competent authority from the Member State where the critical ICT third-party service provider is established, on a voluntary basis.

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

3. Within 3 months of the completion of an investigation or inspection, the Lead Overseer, after consulting the Oversight Forum, shall adopt recommendations to be addressed to the critical ICT third-party service provider pursuant to the powers referred to in Article 35.

4. The recommendations referred to in paragraph 3 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides ICT services.

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

Article 41

Harmonisation of conditions enabling the conduct of the oversight activities

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

(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;

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

(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 ([39]).

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 (*).

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

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

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

Article 60

Amendments to Regulation (EU) No 648/2012

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

(1) Article 26 is amended as follows:

(a) paragraph 3 is replaced by the following:

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

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

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

(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.

_____

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

(2) paragraph 2 is deleted;

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

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

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

(4) paragraph 6 is replaced by the following:

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

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

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

Article 62

Amendments to Regulation (EU) No 600/2014

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

(1) Article 27g is amended as follows:

(a) paragraph 4 is replaced by the following:

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

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

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

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

(2) Article 27h is amended as follows:

(a) paragraph 5 is replaced by the following:

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

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

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

(3) Article 27i is amended as follows:

(a) paragraph 3 is replaced by the following:

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

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

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

Article 63

Amendment to Regulation (EU) 2016/1011

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

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

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

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.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council ([4]) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

([1]) OJ C 233, 16.6.2022, p. 22.
([2]) OJ C 286, 16.7.2021, p. 170.
([3]) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.
([4]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

undermine user confidence and cause major damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.

(4) The legal basis of Directive (EU) 2016/1148 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for entities that offer goods or services across borders. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities. Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards the implementation of the security and incident reporting obligations laid down therein. Those obligations were therefore implemented in significantly different ways at national level. There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

(5) All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures. Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

(6) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market. In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

(7) Under Directive (EU) 2016/1148, Member States were responsible for identifying the entities which met the criteria to qualify as operators of essential services. In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty as regards the cybersecurity risk-management measures and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of this Directive. That criterion should consist of the application of a size-cap rule, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC ([5]), or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which operate within the sectors and provide the types of service or carry out the activities covered by this

([5]) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Directive fall within its scope. Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service to fall within the scope of this Directive.

(8) The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should not be excluded from the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries or to their network and information systems, insofar as such systems are located in the premises of the mission or are operated for users in a third country.

(9) Member States should be able to take the necessary measures to ensure the protection of the essential interests of national security, to safeguard public policy and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences. To that end, Member States should be able to exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, from certain obligations laid down in this Directive with regard to those activities. Where an entity provides services exclusively to a public administration entity that is excluded from the scope of this Directive, Member States should be able to exempt that entity from certain obligations laid down in this Directive with regard to those services. Furthermore, no Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security, public security or defence. Union or national rules for the protection of classified information, non-disclosure agreements, and informal non-disclosure agreements such as the traffic light protocol should be taken into account in that context. The traffic light protocol is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.

(10) Although this Directive applies to entities carrying out activities in the production of electricity from nuclear power plants, some of those activities may be linked to national security. Where that is the case, a Member State should be able to exercise its responsibility for safeguarding national security with respect to those activities, including activities within the nuclear value chain, in accordance with the Treaties.

(11) Some entities carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, while also providing trust services. Trust service providers which fall within the scope of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([6]) should fall within the scope of this Directive in order to secure the same level of security requirements and supervision as that which was previously laid down in that Regulation in respect of trust service providers. In line with the exclusion of certain specific services from Regulation (EU) No 910/2014, this Directive should not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

([6]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

(12) Postal service providers as defined in Directive 97/67/EC of the European Parliament and of the Council ([7]), including providers of courier services, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain, in particular clearance, sorting, transport or distribution of postal items, including pick-up services, while taking account of the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should be excluded from the scope of postal services.

(13) Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure that entities that are excluded from the scope of this Directive achieve a high level of cybersecurity and to support the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of those entities.

(14) Union data protection law and Union privacy law applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council ([8]) and Directive 2002/58/EC of the European Parliament and of the Council ([9]). This Directive should therefore not affect, inter alia, the tasks and powers of the authorities competent to monitor compliance with the applicable Union data protection law and Union privacy law.

(15) Entities falling within the scope of this Directive for the purpose of compliance with cybersecurity risk-management measures and reporting obligations should be classified into two categories, essential entities and important entities, reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. In that regard, due account should be taken of any relevant sectoral risk assessments or guidance by the competent authorities, where applicable. The supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other.

(16) In order to avoid entities that have partner enterprises or that are linked enterprises being considered to be essential or important entities where this would be disproportionate, Member States are able to take into account the degree of independence an entity enjoys in relation to its partner or linked enterprises when applying Article 6(2) of the Annex to Recommendation 2003/361/EC. In particular, Member States are able to take into account the fact that an entity is independent from its partner or linked enterprises in terms of the network and information systems that that entity uses in the provision of its services and in terms of the services that the entity provides. On that basis, where appropriate, Member States are able to consider that such an entity does not qualify as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC, or does not exceed the ceilings for a medium-sized enterprise provided for in paragraph 1 of that Article, if, after taking into account the degree of independence of that entity, that entity would not have been considered to qualify as a medium-sized enterprise or to exceed those ceilings in the event that only its own data had been taken into account. This leaves unaffected the obligations laid down in this Directive of partner and linked enterprises which fall within the scope of this Directive.

(17) Member States should be able to decide that entities identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 are to be considered to be essential entities.

([7]) Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

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

([9]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(18) In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should establish a list of essential and important entities as well as entities providing domain name registration services. For that purpose, Member States should require entities to submit at least the following information to the competent authorities, namely, the name, address and up-to-date contact details, including the email addresses, IP ranges and telephone numbers of the entity, and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable, a list of the Member States where they provide services falling within the scope of this Directive. To that end, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), should, without undue delay, provide guidelines and templates regarding the obligation to submit information. To facilitate the establishing and updating of the list of essential and important entities as well as entities providing domain name registration services, Member States should be able to establish national mechanisms for entities to register themselves. Where registers exist at national level, Member States can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive.

(19) Member States should be responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in this Directive, on the basis of which they were identified, and the type of service that they provide. Member States are encouraged to exchange with the Commission information about essential and important entities and, in the case of a large-scale cybersecurity incident, relevant information such as the name of the entity concerned.

(20) The Commission should, in cooperation with the Cooperation Group and after consulting the relevant stakeholders, provide guidelines on the implementation of the criteria applicable to microenterprises and small enterprises for the assessment of whether they fall within the scope of this Directive. The Commission should also ensure that appropriate guidance is given to microenterprises and small enterprises falling within the scope of this Directive. The Commission should, with the assistance of the Member States, make information available to microenterprises and small enterprises in that regard.

(21) The Commission could provide guidance to assist Member States in implementing the provisions of this Directive on scope and evaluating the proportionality of the measures to be taken pursuant to this Directive, in particular as regards entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities or may simultaneously carry out activities, some of which fall within and some of which are excluded from the scope of this Directive.

(22) This Directive sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope. In order to avoid the fragmentation of cybersecurity provisions of Union legal acts, where further sector-specific Union legal acts pertaining to cybersecurity risk-management measures and reporting obligations are considered to be necessary to ensure a high level of cybersecurity across the Union, the Commission should assess whether such further provisions could be stipulated in an implementing act under this Directive. Should such an implementing act not be suitable for that purpose, sector-specific Union legal acts could contribute to ensuring a high level of cybersecurity across the Union, while taking full account of the specificities and complexities of the sectors concerned. To that end, this Directive does not preclude the adoption of further sector-specific Union legal acts addressing cybersecurity risk-management measures and reporting obligations that take due account of the need for a comprehensive and consistent cybersecurity framework. This Directive is without prejudice to the existing implementing powers that have been conferred on the Commission in a number of sectors, including transport and energy.

(23) Where a sector-specific Union legal act contains provisions requiring essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions, including on supervision

and enforcement, should apply to such entities. If a sector-specific Union legal act does not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by that act.

(24) Where provisions of a sector-specific Union legal act require essential or important entities to comply with reporting obligations that are at least equivalent in effect to the reporting obligations laid down in this Directive, the consistency and effectiveness of the handling of incident notifications should be ensured. To that end, the provisions relating to incident notifications of the sector-specific Union legal act should provide the CSIRTs, the competent authorities or the single points of contact on cybersecurity (single points of contact) under this Directive with an immediate access to the incident notifications submitted in accordance with the sector-specific Union legal act. In particular, such immediate access can be ensured if incident notifications are being forwarded without undue delay to the CSIRT, the competent authority or the single point of contact under this Directive. Where appropriate, Member States should put in place an automatic and direct reporting mechanism that ensures systematic and immediate sharing of information with the CSIRTs, the competent authorities or the single points of contact concerning the handling of such incident notifications. For the purpose of simplifying reporting and of implementing the automatic and direct reporting mechanism, Member States could, in accordance with the sector-specific Union legal act, use a single entry point.

(25) Sector-specific Union legal acts which provide for cybersecurity risk-management measures or reporting obligations that are at least equivalent in effect to those laid down in this Directive could provide that the competent authorities under such acts exercise their supervisory and enforcement powers in relation to such measures or obligations with the assistance of the competent authorities under this Directive. The competent authorities concerned could establish cooperation arrangements for that purpose. Such cooperation arrangements could specify, inter alia, the procedures concerning the coordination of supervisory activities, including the procedures of investigations and on-site inspections in accordance with national law, and a mechanism for the exchange of relevant information on supervision and enforcement between the competent authorities, including access to cyber-related information requested by the competent authorities under this Directive.

(26) Where sector-specific Union legal acts require or provide incentives to entities to notify significant cyber threats, Member States should also encourage the sharing of significant cyber threats with the CSIRTs, the competent authorities or the single points of contact under this Directive, in order to ensure an enhanced level of those bodies' awareness of the cyber threat landscape and to enable them to respond effectively and in a timely manner should the significant cyber threats materialise.

(27) Future sector-specific Union legal acts should take due account of the definitions and the supervisory and enforcement framework laid down in this Directive.

(28) Regulation (EU) 2022/2554 of the European Parliament and of the Council ([10]) should be considered to be a sector-specific Union legal act in relation to this Directive with regard to financial entities. The provisions of Regulation (EU) 2022/2554 relating to information and communication technology (ICT) risk management, management of ICT-related incidents and, in particular, major ICT-related incident reporting, as well as on digital operational resilience testing, information-sharing arrangements and ICT third-party risk should apply instead of those provided for in this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk-management and reporting obligations, and supervision and enforcement, to financial entities covered by Regulation (EU) 2022/2554. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation (EU) 2022/2554 allows the European Supervisory Authorities (ESAs) and the competent authorities under that Regulation to participate in the activities of the Cooperation Group and to exchange information and cooperate with the single points of contact, as well as with the CSIRTs and the competent authorities under this Directive. The competent authorities under Regulation (EU) 2022/2554 should also transmit details of major ICT-related incidents and, where relevant, significant cyber threats to the CSIRTs, the competent authorities or the single points of contact under this Directive. This is achievable by providing immediate access to incident notifications and forwarding them either

([10]) 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 (see page 1 of this Official Journal).

directly or through a single entry point. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and CSIRTs can cover the financial sector in their activities.

(29) In order to avoid gaps between or duplications of cybersecurity obligations imposed on entities in the aviation sector, national authorities under Regulations (EC) No 300/2008 ([11]) and (EU) 2018/1139 ([12]) of the European Parliament and of the Council and the competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level. The compliance of an entity with the security requirements laid down in Regulations (EC) No 300/2008 and (EU) 2018/1139 and in the relevant delegated and implementing acts adopted pursuant to those Regulations could be considered by the competent authorities under this Directive to constitute compliance with the corresponding requirements laid down in this Directive.

(30) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) 2022/2557 of the European Parliament and of the Council ([13]) and this Directive. To achieve this, entities identified as critical entities under Directive (EU) 2022/2557 should be considered to be essential entities under this Directive. Moreover, each Member State should ensure that its national cybersecurity strategy provides for a policy framework for enhanced coordination within that Member State between its competent authorities under this Directive and those under Directive (EU) 2022/2557 in the context of information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks. The competent authorities under this Directive and those under Directive (EU) 2022/2557 should cooperate and exchange information without undue delay, in particular in relation to the identification of critical entities, risks, cyber threats, and incidents as well as in relation to non-cyber risks, threats and incidents affecting critical entities, including the cybersecurity and physical measures taken by critical entities as well as the results of supervisory activities carried out with regard to such entities.

Furthermore, in order to streamline supervisory activities between the competent authorities under this Directive and those under Directive (EU) 2022/2557 and in order to minimise the administrative burden for the entities concerned, those competent authorities should endeavour to harmonise incident notification templates and supervisory processes. Where appropriate, the competent authorities under Directive (EU) 2022/2557, should be able to request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557. The competent authorities under this Directive and those under Directive (EU) 2022/2557 should, where possible in real time, cooperate and exchange information for that purpose.

(31) Entities belonging to the digital infrastructure sector are in essence based on network and information systems and therefore the obligations imposed on those entities pursuant to this Directive should address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk-management measures and reporting obligations. Since those matters are covered by this Directive, the obligations laid down in Chapters III, IV and VI of Directive (EU) 2022/2557 do not apply to such entities.

([11]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

([12]) Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

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

(32) Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name registries, and DNS service providers that are to be understood as entities providing publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party usage. This Directive should not apply to root name servers.

(33) Cloud computing services should cover digital services that enable on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. Computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. The service models of cloud computing include, inter alia, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). The deployment models of cloud computing should include private, community, public and hybrid cloud. The cloud computing service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration.

The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms, including mobile phones, tablets, laptops and workstations. The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

(34) Given the emergence of innovative technologies and new business models, new cloud computing service and deployment models are expected to appear in the internal market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one (edge computing).

(35) Services offered by data centre service providers may not always be provided in the form of a cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should therefore cover providers of data centre services that are not cloud computing services. For the purposes of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology (IT) and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' should not apply to in-house corporate data centres owned and operated by the entity concerned, for its own purposes.

(36) Research activities play a key role in the development of new products and processes. Many of those activities are carried out by entities that share, disseminate or exploit the results of their research for commercial purposes. Those entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to include entities which focus the essential part of their activities on the conduct of applied

research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof.

(37) The growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in sectors such as energy, transport, digital infrastructure, drinking water and waste water, health, certain aspects of public administration, as well as space in so far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programme. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The intensified cyberattacks during the COVID-19 pandemic have shown the vulnerability of increasingly interdependent societies in the face of low-probability risks.

(38) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks under this Directive.

(39) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.

(40) The single points of contact should ensure effective cross-border cooperation with relevant authorities of other Member States and, where appropriate, with the Commission and ENISA. The single points of contact should therefore be tasked with forwarding notifications of significant incidents with cross-border impact to the single points of contact of other affected Member States upon the request of the CSIRT or the competent authority. At national level, the single points of contact should enable smooth cross-sectoral cooperation with other competent authorities. The single points of contact could also be the addressees of relevant information about incidents concerning financial entities from the competent authorities under Regulation (EU) 2022/2554 which they should be able to forward, as appropriate, to the CSIRTs or the competent authorities under this Directive.

(41) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks. Member States should therefore establish or designate one or more CSIRTs under this Directive and ensure that they have adequate resources and technical capabilities. The CSIRTs should comply with the requirements laid down in this Directive in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. Member States should be able to designate existing computer emergency response teams (CERTs) as CSIRTs. In order to enhance the trust relationship between the entities and the CSIRTs, where a CSIRT is part of a competent authority, Member States should be able to consider functional separation between the operational tasks provided by the CSIRTs, in particular in relation to information sharing and assistance provided to the entities, and the supervisory activities of the competent authorities.

(42) The CSIRTs are tasked with incident handling. This includes the processing of large volumes of sometimes sensitive data. Member States should ensure that the CSIRTs have an infrastructure for information sharing and processing, as well as well-equipped staff, which ensures the confidentiality and trustworthiness of their operations. The CSIRTs could also adopt codes of conduct in that respect.

(43) As regards personal data, the CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679, upon the request of an essential or important entity, a proactive scanning of the network and information systems used for the provision of the entity's services. Where applicable, Member States should aim to ensure an equal level of technical capabilities for all sectoral CSIRTs. Member States should be able to request the assistance of ENISA in developing their CSIRTs.

(44) The CSIRTs should have the ability, upon an essential or important entity's request, to monitor the entity's internet-facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified supply chain compromises or critical vulnerabilities. The entity should be encouraged to communicate to the CSIRT whether it runs a privileged management interface, as this could affect the speed of undertaking mitigating actions.

(45) Given the importance of international cooperation on cybersecurity, the CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. Therefore, for the purpose of carrying out their tasks, the CSIRTs and the competent authorities should be able to exchange information, including personal data, with the national computer security incident response teams or competent authorities of third countries provided that the conditions under Union data protection law for transfers of personal data to third countries, inter alia those of Article 49 of Regulation (EU) 2016/679, are met.

(46) Ensuring adequate resources to meet the objectives of this Directive and to enable the competent authorities and the CSIRTs to carry out the tasks laid down herein is essential. The Member States can introduce at the national level a financing mechanism to cover necessary expenditure in relation to the conduct of tasks of public entities responsible for cybersecurity in the Member State pursuant to this Directive. Such mechanism should comply with Union law and should be proportionate and non-discriminatory and should take into account different approaches to providing secure services.

(47) The CSIRTs network should continue to contribute to strengthening confidence and trust and to promote swift and effective operational cooperation among Member States. In order to enhance operational cooperation at Union level, the CSIRTs network should consider inviting Union bodies and agencies involved in cybersecurity policy, such as Europol, to participate in its work.

(48) For the purpose of achieving and maintaining a high level of cybersecurity, the national cybersecurity strategies required under this Directive should consist of coherent frameworks providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them. Those strategies can be composed of one or more legislative or non-legislative instruments.

(49) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats. ENISA should monitor and analyse Member States' cyber hygiene policies.

(50) Cybersecurity awareness and cyber hygiene are essential to enhance the level of cybersecurity within the Union, in particular in light of the growing number of connected devices that are increasingly used in cyberattacks. Efforts should be made to enhance the overall awareness of risks related to such devices, while assessments at Union level could help ensure a common understanding of such risks within the internal market.

(51) Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively. Member States should therefore encourage in their national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity, and, where relevant, the sharing of data needed for training users of such technology and for improving it. The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and data security, such as state-of-the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.

(52) Open-source cybersecurity tools and applications can contribute to a higher degree of openness and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore be able to promote the use of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.

(53) Utilities are increasingly connected to digital networks in cities, for the purpose of improving urban transport networks, upgrading water supply and waste disposal facilities and increasing the efficiency of lighting and the heating of buildings. Those digitalised utilities are vulnerable to cyberattacks and run the risk, in the event of a successful cyberattack, of harming citizens at a large scale due to their interconnectedness. Member States should develop a policy that addresses the development of such connected or smart cities, and their potential effects on society, as part of their national cybersecurity strategy.

(54) In recent years, the Union has faced an exponential increase in ransomware attacks, in which malware encrypts data and systems and demands a ransom payment for release. The increasing frequency and severity of ransomware attacks can be driven by several factors, such as different attack patterns, criminal business models around 'ransomware as a service' and cryptocurrencies, ransom demands, and the rise of supply chain attacks. Member States should develop a policy addressing the rise of ransomware attacks as part of their national cybersecurity strategy.

(55) Public-private partnerships (PPPs) in the field of cybersecurity can provide an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among stakeholders. Member States should promote policies underpinning the establishment of cybersecurity-specific PPPs. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders with regard to PPPs. PPPs can leverage the expertise of private-sector entities to assist the competent authorities in developing state-of-the-art services and processes including information exchange, early warnings, cyber threat and incident exercises, crisis management and resilience planning.

(56) Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of small and medium-sized enterprises. Small and medium-sized enterprises represent, across the Union, a large percentage of the industrial and business market and often struggle to adapt to new business practices in a more connected world and to the digital environment, with employees working from home and business increasingly being conducted online. Some small and medium-sized enterprises face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they should receive guidance and assistance. Small and medium-sized enterprises are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity risk-management measures and attack management, and the fact that they have limited security resources. Such supply chain attacks not only have an impact on small and medium-sized enterprises and their operations in isolation but can also have a cascading effect on larger attacks on entities to which they provided supplies. Member States should, through their national

cybersecurity strategies, help small and medium-sized enterprises to address the challenges faced in their supply chains. Member States should have a point of contact for small and medium-sized enterprises at national or regional level, which either provides guidance and assistance to small and medium-sized enterprises or directs them to the appropriate bodies for guidance and assistance with regard to cybersecurity related issues. Member States are also encouraged to offer services such as website configuration and logging enabling to microenterprises and small enterprises that lack those capabilities.

(57) As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.

(58) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties. In that regard, international standards ISO/IEC 30111 and ISO/IEC 29147 provide guidance on vulnerability handling and vulnerability disclosure. Strengthening the coordination between reporting natural and legal persons and manufacturers or providers of ICT products or ICT services is particularly important for the purpose of facilitating the voluntary framework of vulnerability disclosure. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner allowing it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also include coordination between the reporting natural or legal person and the manufacturer or provider of the potentially vulnerable ICT products or ICT services as regards the timing of remediation and publication of vulnerabilities.

(59) The Commission, ENISA and the Member States should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

(60) Member States, in cooperation with ENISA, should take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. As part of their national policy, Member States should aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with national law. Given that natural and legal persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

(61) Member States should designate one of its CSIRTs as a coordinator, acting as a trusted intermediary between the reporting natural or legal persons and the manufacturers or providers of ICT products or ICT services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT designated as coordinator should include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, negotiating disclosure timelines and managing vulnerabilities that affect multiple entities (multi-party

coordinated vulnerability disclosure). Where the reported vulnerability could have significant impact on entities in more than one Member State, the CSIRTs designated as coordinators should cooperate within the CSIRTs network, where appropriate.

(62) Access to correct and timely information about vulnerabilities affecting ICT products and ICT services contributes to an enhanced cybersecurity risk management. Sources of publicly available information about vulnerabilities are an important tool for the entities and for the users of their services, but also for the competent authorities and the CSIRTs. For that reason, ENISA should establish a European vulnerability database where entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs, can disclose and register, on a voluntary basis, publicly known vulnerabilities for the purpose of allowing users to take appropriate mitigating measures. The aim of that database is to address the unique challenges posed by risks to Union entities. Furthermore, ENISA should establish an appropriate procedure regarding the publication process in order to give entities the time to take mitigating measures as regards their vulnerabilities and employ state-of-the-art cybersecurity risk-management measures as well as machine-readable datasets and corresponding interfaces. To encourage a culture of disclosure of vulnerabilities, disclosure should have no detrimental effects on the reporting natural or legal person.

(63) Although similar vulnerability registries or databases exist, they are hosted and maintained by entities which are not established in the Union. A European vulnerability database maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is publicly disclosed, and resilience in the event of a disruption or an interruption of the provision of similar services. In order, to the extent possible, to avoid a duplication of efforts and to seek complementarity, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries or databases that fall under third-country jurisdiction. In particular, ENISA should explore the possibility of close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system.

(64) The Cooperation Group should support and facilitate strategic cooperation and the exchange of information, as well as strengthen trust and confidence among Member States. The Cooperation Group should establish a work programme every two years. The work programme should include the actions to be undertaken by the Cooperation Group to implement its objectives and tasks. The timeframe for the establishment of the first work programme under this Directive should be aligned with the timeframe of the last work programme established under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Cooperation Group.

(65) When developing guidance documents, the Cooperation Group should consistently map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations, in particular as regards facilitating an alignment of the transposition of this Directive among Member States, to be addressed through a better implementation of existing rules. The Cooperation Group could also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union. This is particularly relevant to sectors that have an international or cross-border nature.

(66) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It could organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather data and input on emerging policy challenges. Additionally, the Cooperation Group should carry out a regular assessment of the state of play of cyber threats or incidents, such as ransomware. In order to enhance cooperation at Union level, the Cooperation Group should consider inviting relevant Union institutions, bodies, offices and agencies involved in cybersecurity policy, such as the European Parliament, Europol, the European Data

Protection Board, the European Union Aviation Safety Agency, established by Regulation (EU) 2018/1139, and the European Union Agency for Space Programme, established by Regulation (EU) 2021/696 of the European Parliament and the Council ([14]), to participate in its work.

(67) The competent authorities and the CSIRTs should be able to participate in exchange schemes for officials from other Member States, within a specific framework and, where applicable, subject to the required security clearance of officials participating in such exchange schemes, in order to improve cooperation and strengthen trust among Member States. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority or the host CSIRT.

(68) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework as set out in Commission Recommendation (EU) 2017/1584 ([15]) through the existing cooperation networks, in particular the European cyber crisis liaison organisation network (EU-CyCLONe), the CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements that specify the details of that cooperation and avoid any duplication of tasks. EU-CyCLONe's rules of procedure should further specify the arrangements through which that network should function, including the network's roles, means of cooperation, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the EU Integrated Political Crisis Response arrangements under Council Implementing Decision (EU) 2018/1993 ([16]) (IPCR arrangements). The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for that purpose. If the crisis entails an important external or Common Security and Defence Policy dimension, the European External Action Service Crisis Response Mechanism should be activated.

(69) In accordance with the Annex to Recommendation (EU) 2017/1584, a large-scale cybersecurity incident should mean an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States. Depending on their cause and impact, large-scale cybersecurity incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and the relevant Union institutions, bodies, offices and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

(70) Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response because of the high degree of interdependence between sectors and Member States. The availability of cyber-resilient network and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union and for the protection of its citizens, businesses and institutions against incidents and cyber threats, as well as for enhancing the trust of individuals and organisations in the Union's ability to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

([14]) Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

([15]) Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

([16]) Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28).

(71) EU-CyCLONe should work as an intermediary between the technical and political level during large-scale cybersecurity incidents and crises and should enhance cooperation at operational level and support decision-making at political level. In cooperation with the Commission, having regard to the Commission's competence in the area of crisis management, EU-CyCLONe should build on the CSIRTs network findings and use its own capabilities to create impact analysis of large-scale cybersecurity incidents and crises.

(72) Cyberattacks are of a cross-border nature, and a significant incident can disrupt and damage critical information infrastructures on which the smooth functioning of the internal market depends. Recommendation (EU) 2017/1584 addresses the role of all relevant actors. Furthermore, the Commission is responsible, within the framework of the Union Civil Protection Mechanism, established by Decision No 1313/2013/EU of the European Parliament and of the Council ([17]), for general preparedness actions including managing the Emergency Response Coordination Centre and the Common Emergency Communication and Information System, maintaining and further developing situational awareness and analysis capability, and establishing and managing the capability to mobilise and dispatch expert teams in the event of a request for assistance from a Member State or third country. The Commission is also responsible for providing analytical reports for the IPCR arrangements under Implementing Decision (EU) 2018/1993, including in relation to cybersecurity situational awareness and preparedness, as well as for situational awareness and crisis response in the areas of agriculture, adverse weather conditions, conflict mapping and forecasts, early warning systems for natural disasters, health emergencies, infection disease surveillance, plant health, chemical incidents, food and feed safety, animal health, migration, customs, nuclear and radiological emergencies, and energy.

(73) The Union can, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements should ensure the Union's interests and the adequate protection of data. This should not preclude the right of Member States to cooperate with third countries on management of vulnerabilities and cybersecurity risk management, facilitating reporting and general information sharing in accordance with Union law.

(74) In order to facilitate the effective implementation of this Directive with regard, inter alia, to the management of vulnerabilities, cybersecurity risk-management measures, reporting obligations and cybersecurity information-sharing arrangements, Member States can cooperate with third countries and undertake activities that are considered to be appropriate for that purpose, including information exchange on cyber threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cybersecurity crisis management preparedness and exercises, training, trust building and structured information-sharing arrangements.

(75) Peer reviews should be introduced to help learn from shared experiences, strengthen mutual trust and achieve a high common level of cybersecurity. Peer reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities, creating another functional path for the sharing of best practices across Member States and contributing to enhance the Member States' levels of maturity in cybersecurity. Furthermore, peer reviews should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, and should add value and avoid duplication. The implementation of peer reviews should be without prejudice to Union or national law on the protection of confidential or classified information.

(76) The Cooperation Group should establish a self-assessment methodology for Member States, aiming to cover factors such as the level of implementation of the cybersecurity risk-management measures and reporting obligations, the level of capabilities and the effectiveness of the exercise of the tasks of the competent authorities, the operational capabilities of the CSIRTs, the level of implementation of mutual assistance, the level of implementation of the cybersecurity information-sharing arrangements, or specific issues of cross-border or cross-sector nature. Member States should be encouraged to carry out self-assessments on a regular basis, and to present and discuss the results of their self-assessment within the Cooperation Group.

([17]) Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

(77) Responsibility for ensuring the security of network and information system lies, to a great extent, with essential and important entities. A culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures appropriate to the risks faced, should be promoted and developed.

(78) Cybersecurity risk-management measures should take into account the degree of dependence of the essential or important entity on network and information systems and include measures to identify any risks of incidents, to prevent, detect, respond to and recover from incidents and to mitigate their impact. The security of network and information systems should include the security of stored, transmitted and processed data. Cybersecurity risk-management measures should provide for systemic analysis, taking into account the human factor, in order to have a complete picture of the security of the network and information system.

(79) As threats to the security of network and information systems can have different origins, cybersecurity risk-management measures should be based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557.

(80) For the purpose of demonstrating compliance with cybersecurity risk-management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council ([18]), Member States should, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, promote the use of relevant European and international standards by essential and important entities or may require entities to use certified ICT products, ICT services and ICT processes.

(81) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk-management measures should be proportionate to the risks posed to the network and information system concerned, taking into account the state-of-the-art of such measures, and, where applicable, relevant European and international standards, as well as the cost for their implementation.

(82) Cybersecurity risk-management measures should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. When establishing cybersecurity risk-management measures adapted to essential and important entities, due account should be taken of the divergent risk exposure of essential and important entities, such as the criticality of the entity, the risks, including societal risks, to which it is exposed, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

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

(83) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those systems are primarily private network and information systems managed by the essential and important entities' internal IT staff or the security of which has been outsourced. The cybersecurity risk-management measures and reporting obligations laid down in this Directive should apply to the relevant essential and important entities regardless of whether those entities maintain their network and information systems internally or outsource the maintenance thereof.

(84) Taking account of their cross-border nature, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers should be subject to a high degree of harmonisation at Union level. The implementation of cybersecurity risk-management measures with regard to those entities should therefore be facilitated by an implementing act.

(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

(86) Among service providers, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and, because of their close integration in the operations of entities pose a particular risk. Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider.

(87) The competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits, penetration testing or incident responses.

(88) Essential and important entities should also address risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem, including with regard to countering industrial espionage and protecting trade secrets. In particular, those entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of essential and important entities, when relying on data transformation and data analytics services from third parties, those entities should take all appropriate cybersecurity risk-management measures.

(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

(90) To further address key supply chain risks and assist essential and important entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related risks, the Cooperation Group, in cooperation with the Commission and ENISA, and where appropriate after consulting relevant stakeholders including from the industry, should carry out coordinated security risk assessments of critical supply chains, as carried out for 5G networks following Commission Recommendation (EU) 2019/534 ([19]), with the aim of identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities. Such coordinated security risk assessments should identify measures, mitigation plans and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by essential and important entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency.

(91) The coordinated security risk assessments of critical supply chains, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated security risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, ICT systems or ICT products; (ii) the relevance of specific critical ICT services, ICT systems or ICT products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, ICT systems or ICT products; (iv) the resilience of the overall supply chain of ICT services, ICT systems or ICT products throughout their lifecycle against disruptive events; and (v) for emerging ICT services, ICT systems or ICT products, their potential future significance for the entities' activities. Furthermore, particular emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements stemming from third countries.

(92) In order to streamline the obligations imposed on providers of public electronic communications networks or of publicly available electronic communications services, and trust service providers, related to the security of their network and information systems, as well as to enable those entities and the competent authorities under Directive (EU) 2018/1972 of the European Parliament and of the Council ([20]) and Regulation (EU) No 910/2014 respectively to benefit from the legal framework established by this Directive, including the designation of a CSIRT responsible for incident handling, the participation of the competent authorities concerned in the activities of the Cooperation Group and the CSIRTs network, those entities should fall within the scope of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 related to the imposition of security and notification requirements on those types of entity should therefore be deleted. The rules on reporting obligations laid down in this Directive should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

(93) The cybersecurity obligations laid down in this Directive should be considered to be complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014. Trust service providers should be required to take all appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and relying third parties, and to report incidents under this Directive. Such cybersecurity and reporting obligations should also concern the physical protection of the services provided. The requirements for qualified trust service providers laid down in Article 24 of Regulation (EU) No 910/2014 continue to apply.

([19]) Commission Recommendation (EU) 2019/534 of 26 March 2019 – Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

([20]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(94) Member States can assign the role of the competent authorities for trust services to the supervisory bodies under Regulation (EU) No 910/2014 in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of that Regulation. In such a case, the competent authorities under this Directive should cooperate closely and in a timely manner with those supervisory bodies by exchanging relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements laid down in this Directive and in Regulation (EU) No 910/2014. Where applicable, the CSIRT or the competent authority under this Directive should immediately inform the supervisory body under Regulation (EU) No 910/2014 about any notified significant cyber threat or incident affecting trust services as well as about any infringements by a trust service provider of this Directive. For the purpose of reporting, Member States can, where applicable, use the single entry point established to achieve a common and automatic incident reporting to both the supervisory body under Regulation (EU) No 910/2014 and the CSIRT or the competent authority under this Directive.

(95) Where appropriate and in order to avoid unnecessary disruption, existing national guidelines adopted for the transposition of the rules related to security measures laid down in Articles 40 and 41 of Directive (EU) 2018/1972 should be taken into account in the transposition of this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security measures and incident notifications. ENISA can also develop guidance on security requirements and on reporting obligations for providers of public electronic communications networks or of publicly available electronic communications services to facilitate harmonisation and transition and to minimise disruption. Member States can assign the role of the competent authorities for electronic communications to the national regulatory authorities under Directive (EU) 2018/1972 in order to ensure the continuation of current practices and to build on the knowledge and experience gained as a result of the implementation of that Directive.

(96) Given the growing importance of number-independent interpersonal communications services as defined in Directive (EU) 2018/1972, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. As the attack surface continues to expand, number-independent interpersonal communications services, such as messaging services, are becoming widespread attack vectors. Malicious perpetrators use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and, by extension, the security of network and information systems. Providers of number-independent interpersonal communications services should ensure a level of security of network and information systems appropriate to the risks posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risks posed to such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services as defined in Directive (EU) 2018/1972 which make use of numbers and which do not exercise actual control over signal transmission.

(97) The internal market is more reliant on the functioning of the internet than ever. The services of almost all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that all providers of public electronic communications networks have appropriate cybersecurity risk-management measures in place and report significant incidents in relation thereto. Member States should ensure that the security of the public electronic communications networks is maintained and that their vital security interests are protected from sabotage and espionage. Since international connectivity enhances and accelerates the competitive digitalisation of the Union and its economy, incidents affecting undersea communications cables should be reported to the CSIRT or, where applicable, the competent authority. The national cybersecurity strategy should, where relevant, take into account the cybersecurity of undersea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

(98) In order to safeguard the security of public electronic communications networks and publicly available electronic communications services, the use of encryption technologies, in particular end-to-end encryption as well as data-centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted. Where necessary, the use of encryption, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive. The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences in accordance with Union law. However, this should not weaken end-to-end encryption, which is a critical technology for the effective protection of data and privacy and the security of communications.

(99) In order to safeguard the security, and to prevent abuse and manipulation, of public electronic communications networks and of publicly available electronic communications services, the use of secure routing standards should be promoted to ensure the integrity and robustness of routing functions across the ecosystem of internet access service providers.

(100) In order to safeguard the functionality and integrity of the internet and to promote the security and resilience of the DNS, relevant stakeholders including Union private-sector entities, providers of publicly available electronic communications services, in particular internet access service providers, and providers of online search engines should be encouraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.

(101) This Directive lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows essential and important entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual entities and entire sectors. In that regard, this Directive should include the reporting of incidents that, based on an initial assessment carried out by the entity concerned, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the affected network and information systems, in particular their importance in the provision of the entity's services, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident or the number of affected recipients of services could play an important role in identifying whether the operational disruption of the service is severe.

(102) Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification. The early warning should only include the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact. Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect.

In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident.

(103) Where applicable, essential and important entities should communicate, without undue delay, to their service recipients any measures or remedies that they can take to mitigate the resulting risks from a significant cyber threat. Those entities should, where appropriate and in particular where the significant cyber threat is likely to materialise, also inform their service recipients of the threat itself. The requirement to inform those recipients of significant cyber threats should be met on a best efforts basis but should not discharge those entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any such threats and restore the normal security level of the service. The provision of such information about significant cyber threats to the service recipients should be free of charge and drafted in easily comprehensible language.

(104) Providers of public electronic communications networks or of publicly available electronic communications services should implement security by design and by default, and inform their service recipients of significant cyber threats and of measures they can take to protect the security of their devices and communications, for example by using specific types of software or encryption technologies.

(105) A proactive approach to cyber threats is a vital component of cybersecurity risk management that should enable the competent authorities to effectively prevent cyber threats from materialising into incidents that may cause considerable material or non-material damage. For that purpose, the notification of cyber threats is of key importance. To that end, entities are encouraged to report on a voluntary basis cyber threats.

(106) In order to simplify the reporting of information required under this Directive as well as to decrease the administrative burden for entities, Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported. Union funding supporting the implementation of this Directive, in particular within the Digital Europe programme, established by Regulation (EU) 2021/694 of the European Parliament and of the Council ([21]), could include support for single entry points. Furthermore, entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional administrative burden and could also lead to uncertainties with regard to the format and procedures of such notifications. Where a single entry point is established, Member States are encouraged also to use that single entry point for notifications of security incidents required under other Union law, such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The use of such single entry point for reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law and decrease the administrative burden on notifying entities.

(107) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in accordance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between the competent authorities and the law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

([21]) Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

(108) Personal data are in many cases compromised as a result of incidents. In that context, the competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.

(109) Maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other Union or national law. That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task.

(110) The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents. Legitimate access seekers are to be understood as any natural or legal person making a request pursuant to Union or national law. They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs. TLD name registries and entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are necessary for the purposes of the access request, to legitimate access seekers in accordance with Union and national law. The request of legitimate access seekers should be accompanied by a statement of reasons permitting the assessment of the necessity of access to the data.

(111) In order to ensure the availability of accurate and complete domain name registration data, TLD name registries and entities providing domain name registration services should collect and guarantee the integrity and availability of domain name registration data. In particular, TLD name registries and entities providing domain name registration services should establish policies and procedures to collect and maintain accurate and complete domain name registration data, as well as to prevent and correct inaccurate registration data, in accordance with Union data protection law. Those policies and procedures should take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. The TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification. Examples of verification procedures may include *ex ante* controls carried out at the time of the registration and *ex post* controls carried out after the registration. The TLD name registries and the entities providing domain name registration services should, in particular, verify at least one means of contact of the registrant.

(112) TLD name registries and entities providing domain name registration services should be required to make publicly available domain name registration data that fall outside the scope of Union data protection law, such as data that concern legal persons, in line with the preamble of Regulation (EU) 2016/679. For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts. TLD name registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should require TLD name registries and entities providing domain name registration services to respond without undue delay to requests for the disclosure of domain name registration data from legitimate access seekers. TLD name registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. Those policies and procedures should take into account, to the extent possible, any guidance and the standards developed by the multi-stakeholder

governance structures at international level. The access procedure could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission can, without prejudice to the competences of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.

(113) Entities falling within the scope of this Directive should be considered to fall under the jurisdiction of the Member State in which they are established. However, providers of public electronic communications networks or providers of publicly available electronic communications services should be considered to fall under the jurisdiction of the Member State in which they provide their services. DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms should be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union. Public administration entities should fall under the jurisdiction of the Member State which established them. If the entity provides services or is established in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of those Member States. The competent authorities of those Member States should cooperate, provide mutual assistance to each other and, where appropriate, carry out joint supervisory actions. Where Member States exercise jurisdiction, they should not impose enforcement measures or penalties more than once for the same conduct, in line with the principle of *ne bis in idem*.

(114) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, only one Member State should have jurisdiction over those entities. Jurisdiction should be attributed to the Member State in which the entity concerned has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether that criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be considered to be in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken in the Union. This will typically correspond to the place of the entities' central administration in the Union. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment should be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment should be considered to be in the Member State where the entity has the establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

(115) Where a publicly available recursive DNS service is provided by a provider of public electronic communications networks or of publicly available electronic communications services only as a part of the internet access service, the entity should be considered to fall under the jurisdiction of all the Member States where its services are provided.

(116) Where a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider or a provider of an online marketplace, of an online search engine or of a social networking services platform, which is not established in the Union, offers services within the Union, it should designate a representative in the Union. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address or other contact details, or the use of a language generally used in the third country where the entity is established, should be considered to be insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that language, or the mentioning of customers or users who are in the Union, could make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for the competent authorities or the CSIRTs to address the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations laid down in this Directive, including incident reporting.

(117) In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, which provide services across the Union that fall within the scope of this Directive, ENISA should create and maintain a registry of such entities, based on the information received by Member States, where applicable through national mechanisms established for entities to register themselves. The single points of contact should forward to ENISA the information and any changes thereto. With a view to ensuring the accuracy and completeness of the information that is to be included in that registry, Member States can submit to ENISA the information available in any national registries on those entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information. ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information and restrict the access, storage, and transmission of such information to intended users.

(118) Where information which is classified in accordance with Union or national law is exchanged, reported or otherwise shared under this Directive, the corresponding rules on the handling of classified information should be applied. In addition, ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information in accordance with the applicable security rules for protecting EU classified information.

(119) With cyber threats becoming more complex and sophisticated, good detection of such threats and their prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to an increased awareness of cyber threats, which, in turn, enhances entities' capacity to prevent such threats from materialising into incidents and enables entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, various factors seem to have inhibited such intelligence sharing, in particular uncertainty over the compatibility with competition and liability rules.

(120) Entities should be encouraged and assisted by Member States to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately prevent, detect, respond to or recover from incidents or to mitigate their impact. It is thus necessary to enable the emergence at Union level of voluntary cybersecurity information-sharing arrangements. To that end, Member States should actively assist and encourage entities, such as those providing cybersecurity services and research, as well as relevant entities not falling within the scope of this Directive, to participate in such cybersecurity information-sharing arrangements. Those arrangements should be established in accordance with the Union competition rules and Union data protection law.

(121) The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679. Processing of personal data could also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with this Directive. Measures related to the prevention, detection, identification, containment, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps. Processing of personal data by the competent authorities, the single points of contact and the CSIRTs, could constitute a legal obligation or be considered to be necessary for carrying out a task in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1), point (c) or (e), and Article 6(3) of Regulation (EU) 2016/679, or for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1), point (f), of that Regulation. Furthermore, national law could lay down rules allowing the competent authorities, the single points of contact and the CSIRTs, to the extent that is necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

(122) In order to strengthen the supervisory powers and measures that help ensure effective compliance, this Directive should provide for a minimum list of supervisory measures and means through which the competent authorities can supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations on those entities and on the competent authorities. Therefore, essential entities should be subject to a comprehensive *ex ante* and *ex post* supervisory regime, while important entities should be subject to a light, *ex post* only, supervisory regime. Important entities should therefore not be required to systematically document compliance with cybersecurity risk-management measures, while the competent authorities should implement a reactive *ex post* approach to supervision and, hence, not have a general obligation to supervise those entities. The *ex post* supervision of important entities may be triggered by evidence, indication or information brought to the attention of the competent authorities considered by those authorities to suggest potential infringements of this Directive. For example, such evidence, indication or information could be of the type provided to the competent authorities by other authorities, entities, citizens, media or other sources or publicly available information, or could emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.

(123) The execution of supervisory tasks by the competent authorities should not unnecessarily hamper the business activities of the entity concerned. Where the competent authorities execute their supervisory tasks in relation to essential entities, including the conduct of on-site inspections and off-site supervision, the investigation of infringements of this Directive and the conduct of security audits or security scans, they should minimise the impact on the business activities of the entity concerned.

(124) In the exercise of *ex ante* supervision, the competent authorities should be able to decide on the prioritisation of the use of supervisory measures and means at their disposal in a proportionate manner. This entails that the competent authorities can decide on such prioritisation based on supervisory methodologies which should follow a risk-based approach. More specifically, such methodologies could include criteria or benchmarks for the classification of essential entities into risk categories and corresponding supervisory measures and means recommended per risk category, such as the use, frequency or types of on-site inspections, targeted security audits or security scans, the type of information to be requested and the level of detail of that information. Such supervisory methodologies

could also be accompanied by work programmes and be assessed and reviewed on a regular basis, including on aspects such as resource allocation and needs. In relation to public administration entities, the supervisory powers should be exercised in line with the national legislative and institutional frameworks.

(125) The competent authorities should ensure that their supervisory tasks in relation to essential and important entities are carried out by trained professionals, who should have the necessary skills to carry out those tasks, in particular with regard to conducting on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Those inspections and that supervision should be conducted in an objective manner.

(126) In duly substantiated cases where it is aware of a significant cyber threat or an imminent risk, the competent authority should be able to take immediate enforcement decisions with the aim of preventing or responding to an incident.

(127) In order to make enforcement effective, a minimum list of enforcement powers that can be exercised for breach of the cybersecurity risk-management measures and reporting obligations provided for in this Directive should be laid down, setting up a clear and consistent framework for such enforcement across the Union. Due regard should be given to the nature, gravity and duration of the infringement of this Directive, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The enforcement measures, including administrative fines, should be proportionate and their imposition should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union (the 'Charter'), including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(128) This Directive does not require Member States to provide for criminal or civil liability with regard to natural persons with responsibility for ensuring that an entity complies with this Directive for damage suffered by third parties as a result of an infringement of this Directive.

(129) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.

(130) Where an administrative fine is imposed on an essential or important entity that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where an administrative fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers of the competent authorities or of other penalties laid down in the national rules transposing this Directive.

(131) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice of the European Union.

(132) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in the event of a serious infringement of this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties and whether they are criminal or administrative should be determined by national law.

(133) In order to further strengthen the effectiveness and dissuasiveness of the enforcement measures applicable to infringements of this Directive, the competent authorities should be empowered to suspend temporarily or to request the temporary suspension of a certification or authorisation concerning part or all of the relevant services provided or activities carried out by an essential entity and request the imposition of a temporary prohibition of the exercise of managerial functions by any natural person discharging managerial responsibilities at chief executive officer or legal representative level. Given their severity and impact on the entities' activities and ultimately on users, such temporary suspensions or prohibitions should only be applied proportionally to the severity of the infringement and taking account of the circumstances of each individual case, including whether the infringement was intentional or negligent, and any actions taken to prevent or mitigate the material or non-material damage. Such temporary suspensions or prohibitions should only be applied as a last resort, namely only after the other relevant enforcement measures laid down in this Directive have been exhausted, and only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such temporary suspensions or prohibitions were applied. The imposition of such temporary suspensions or prohibitions should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(134) For the purpose of ensuring entities' compliance with their obligations laid down in this Directive, Member States should cooperate with and assist each other with regard to supervisory and enforcement measures, in particular where an entity provides services in more than one Member State or where its network and information systems are located in a Member State other than that where it provides services. When providing assistance, the requested competent authority should take supervisory or enforcement measures in accordance with national law. In order to ensure the smooth functioning of mutual assistance under this Directive, the competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance.

(135) In order to ensure effective supervision and enforcement, in particular in a situation with a cross-border dimension, a Member State that has received a request for mutual assistance should, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity that is the subject of that request, and that provides services or has a network and information system on the territory of that Member State.

(136) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities under Regulation (EU) 2016/679 to deal with infringements of this Directive related to personal data.

(137) This Directive should aim to ensure a high level of responsibility for the cybersecurity risk-management measures and reporting obligations at the level of the essential and important entities. Therefore, the management bodies of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.

(138) In order to ensure a high common level of cybersecurity across the Union on the basis of this Directive, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of supplementing this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([22]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

([22]) OJ L 123, 12.5.2016, p. 1.

(139) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to lay down the procedural arrangements necessary for the functioning of the Cooperation Group and the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures, and to further specify the type of information, the format and the procedure of incident, cyber threat and near miss notifications and of significant cyber threat communications, as well as cases in which an incident is to be considered to be significant. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([23]).

(140) The Commission should periodically review this Directive, after consulting stakeholders, in particular with a view to determining whether it is appropriate to propose amendments in light of changes to societal, political, technological or market conditions. As part of those reviews, the Commission should assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in the annexes to this Directive for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether providers, falling within the scope of this Directive, that are designated as very large online platforms within the meaning of Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council ([24]) could be identified as essential entities under this Directive.

(141) This Directive creates new tasks for ENISA, thereby enhancing its role, and could also result in ENISA being required to carry out its existing tasks under Regulation (EU) 2019/881 to a higher level than before. In order to ensure that ENISA has the necessary financial and human resources to carry out existing and new tasks, as well as to meet any higher level of execution of those tasks resulting from its enhanced role, its budget should be increased accordingly. In addition, in order to ensure the efficient use of resources, ENISA should be given greater flexibility in the way that it is able to allocate resources internally for the purpose of effectively carrying out its tasks and meeting expectations.

(142) Since the objective of this Directive, namely to achieve a high common level of cybersecurity across the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(143) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence. The right to an effective remedy extends to the recipients of services provided by essential and important entities. This Directive should be implemented in accordance with those rights and principles.

(144) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([25]) and delivered an opinion on 11 March 2021 ([26]),

---

([23]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

([24]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

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

([26]) OJ C 183, 11.5.2021, p. 3.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

2. To that end, this Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;

(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:

(a) services are provided by:

  (i) providers of public electronic communications networks or of publicly available electronic communications services;

  (ii) trust service providers;

  (iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

4. Regardless of their size, this Directive applies to entities providing domain name registration services.

5. Member States may provide for this Directive to apply to:

(a) public administration entities at local level;

(b) education institutions, in particular where they carry out critical research activities.

6. This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

7. This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

8. Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.

9. Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider.

10. This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.

11. The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

12. This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU ([27]) and 2013/40/EU ([28]) of the European Parliament and of the Council and Directive (EU) 2022/2557.

13. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

([27]) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

([28]) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

14. Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data protection law and Union privacy law, in particular Directive 2002/58/EC.

Article 3

Essential and important entities

1. For the purposes of this Directive, the following entities shall be considered to be essential entities:

(a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;

(b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;

(c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;

(d) public administration entities referred to in Article 2(2), point (f)(i);

(e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);

(f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive;

(g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

2. For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).

3. By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.

4. For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities:

(a) the name of the entity;

(b) the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;

(c) where applicable, the relevant sector and subsector referred to in Annex I or II; and

(d) where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

The entities referred to in paragraph 3 shall notify any changes to the details submitted pursuant to the first subparagraph of this paragraph without delay, and, in any event, within two weeks of the date of the change.

The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph.

Member States may establish national mechanisms for entities to register themselves.

5. By 17 April 2025 and every two years thereafter, the competent authorities shall notify:

(a) the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to paragraph 3 for each sector and subsector referred to in Annex I or II; and

(b) the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.

6. Until 17 April 2025 and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 5, point (b).

Article 4

Sector-specific Union legal acts

1. Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.

2. The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where:

(a) cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or

(b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.

3. The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA.

Article 5

Minimum harmonisation

This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.

Article 6

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'network and information system' means:

(a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

(3) 'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

(4) 'national cybersecurity strategy ' means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;

(5) 'near miss' means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

(6) 'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

(7) 'large-scale cybersecurity incident' means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States;

(8) 'incident handling' means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;

(9) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

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

(11) 'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage;

(12) 'ICT product' means an ICT product as defined in Article 2, point (12), of Regulation (EU) 2019/881;

(13) 'ICT service' means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;

(14) 'ICT process' means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;

(15) 'vulnerability' means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;

(16) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([29]);

(17) 'technical specification' means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

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

(18) 'internet exchange point' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

(19) 'domain name system' or 'DNS' means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

(20) 'DNS service provider' means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

(21) 'top-level domain name registry' or 'TLD name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

(22) 'entity providing domain name registration services' means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

(23) 'digital service' means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council ([30]);

(24) 'trust service' means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;

(25) 'trust service provider' means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;

(26) 'qualified trust service' means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;

(27) 'qualified trust service provider' means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;

(28) 'online marketplace' means an online marketplace as defined in Article 2, point (n), of Directive 2005/29/EC of the European Parliament and of the Council ([31]);

(29) 'online search engine' means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council ([32]);

(30) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

([30]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

([31]) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

([32]) Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

(31) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(32) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(33) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

(34) 'representative' means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;

(35) 'public administration entity' means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

(36) 'public electronic communications network' means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972;

(37) 'electronic communications service' means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972;

(38) 'entity' means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(39) 'managed service provider' means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;

(40) 'managed security service provider' means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

(41) 'research organisation' means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

CHAPTER II

COORDINATED CYBERSECURITY FRAMEWORKS

Article 7

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:

(a) objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;

(b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;

(c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

(d) a mechanism to identify relevant assets and an assessment of the risks in that Member State;

(e) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;

(f) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

(g) a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

(f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;

(j) promoting active cyber protection.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.

4. Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.

Article 8

Competent authorities and single points of contact

1. Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).

2. The competent authorities referred to in paragraph 1 shall monitor the implementation of this Directive at national level.

3. Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.

4. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State.

5. Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive.

6. Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto. Each Member State shall make public the identity of its competent authority. The Commission shall make a list of the single points of contact publicly available.

Article 9

National cyber crisis management frameworks

1. Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

2. Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.

3. Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive.

4. Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:

(a) the objectives of national preparedness measures and activities;

(b) the tasks and responsibilities of the cyber crisis management authorities;

(c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;

(d) national preparedness measures, including exercises and training activities;

(e) the relevant public and private stakeholders and infrastructure involved;

(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

5. Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.

Article 10

Computer security incident response teams (CSIRTs)

1. Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.

2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).

3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.

4. The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.

5. The CSIRTs shall participate in peer reviews organised in accordance with Article 19.

6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network.

7. The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.

8. The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

9. Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.

10. Member States may request the assistance of ENISA in developing their CSIRTs.

Article 11

Requirements, technical capabilities and tasks of CSIRTs

1. The CSIRTs shall comply with the following requirements:

(a) the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;

(b) the CSIRTs' premises and the supporting information systems shall be located at secure sites;

(c) the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;

(d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;

(e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately;

(f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services.

The CSIRTs may participate in international cooperation networks.

2. Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.

3. The CSIRTs shall have the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services.

When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.

4. The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.

5. In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:

(a) incident-handling procedures;

(b) crisis management; and

(c) coordinated vulnerability disclosure under Article 12(1).

Article 12

Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

(a) identifying and contacting the entities concerned;

(b) assisting the natural or legal persons reporting a vulnerability; and

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:

(a) information describing the vulnerability;

(b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;

(c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.

Article 13

Cooperation at national level

1. Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30.

3. Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive.

4. In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.

5. Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.

6. Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.

CHAPTER III

COOPERATION AT UNION AND INTERNATIONAL LEVEL

Article 14

Cooperation Group

1. In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.

2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation.

Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work.

The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

(a) to provide guidance to the competent authorities in relation to the transposition and implementation of this Directive;

(b) to provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure, as referred to in Article 7(2), point (c);

(c) to exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities pursuant to Article 2(2), points (b) to (e);

(d) to exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;

(e) to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive;

(f) to exchange best practices and information with relevant Union institutions, bodies, offices and agencies;

(g) to exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity;

(h) where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations;

(i) to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1);

(j) to discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions as referred to in Article 37;

(k) upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance as referred to in Article 37;

(l) to provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;

(m) to exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe;

(n) to contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;

(o) to organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges;

(p) to discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA;

(q) to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6);

(r) to prepare reports for the purpose of the review referred to in Article 40 on the experience gained at a strategic level and from peer reviews;

(s) to discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware.

The Cooperation Group shall submit the reports referred to in the first subparagraph, point (r), to the Commission, to the European Parliament and to the Council.

5. Member States shall ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group.

6. The Cooperation Group may request from the CSIRTs network a technical report on selected topics.

7. By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.

8. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4), point (e).

9. The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.

Article 15

CSIRTs network

1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.

2. The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) to exchange information about the CSIRTs' capabilities;

(b) to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;

(c) to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

(d) to exchange information with regard to cybersecurity publications and recommendations;

(e) to ensure interoperability with regard to information-sharing specifications and protocols;

(f) at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;

(g) at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State;

(h) to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive;

(i) to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;

(j) to discuss and identify further forms of operational cooperation, including in relation to:

  (i) categories of cyber threats and incidents;

  (ii) early warnings;

  (iii) mutual assistance;

  (iv) principles and arrangements for coordination in response to cross-border risks and incidents;

  (v) contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State;

(k) to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard;

(l) to take stock of cybersecurity exercises, including those organised by ENISA;

(m) at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT;

(n) to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union;

(o) where relevant, to discuss the peer-review reports referred to in Article 19(9);

(p) to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report. The report shall, in particular, draw up conclusions and recommendations on the basis of the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.

5. The CSIRTs network shall adopt its rules of procedure.

6. The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.

Article 16

European cyber crisis liaison organisation network (EU-CyCLONe)

1. EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

2. EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.

ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information.

Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.

3. EU-CyCLONe shall have the following tasks:

(a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;

(b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;

(c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;

(d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;

(e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).

4. EU-CyCLONe shall adopt its rules of procedure.

5. EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities.

6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6).

7. By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.

Article 17

International cooperation

The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.

Article 18

Report on the state of cybersecurity in the Union

1. ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following:

(a) a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape;

(b) an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;

(c) an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises;

(d) an aggregated assessment of the outcome of the peer reviews referred to in Article 19;

(e) an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.

2. The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

3. ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).

Article 19

Peer reviews

1. The Cooperation Group shall, on 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed.

The peer reviews shall cover at least one of the following:

(a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23;

(b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;

(c) the operational capabilities of the CSIRTs;

(d) the level of implementation of mutual assistance referred to in Article 37;

(e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29;

(f) specific issues of cross-border or cross-sector nature.

2. The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews.

3. Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review.

4. Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3.

5. Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment.

6. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties.

7. Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group.

8. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State.

9. Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.

CHAPTER IV

CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

5. By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph.

When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 22

Union level coordinated security risk assessments of critical supply chains

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

2. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.

Article 23

Reporting obligations

1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

3. An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

5. The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.

6. Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

7. Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.

8. At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.

10. The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.

11. The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article.

By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities.

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 24

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period.

Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881.

3. Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.

Article 25

Standardisation

1. In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

CHAPTER V

JURISDICTION AND REGISTRATION

Article 26

Jurisdiction and territoriality

1. Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:

(a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;

(b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;

(c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.

2. For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

3. If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.

4. The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.

5. Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.

Article 27

Registry of entities

1. ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.

2. Member States shall require entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025:

(a) the name of the entity;

(b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;

(c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);

(d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3);

(e) the Member States where the entity provides services; and

(f) the entity's IP ranges.

3. Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.

4. Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

5. Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.

Article 28

Database of domain name registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.

2. For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:

(a) the domain name;

(b) the date of registration;

(c) the registrant's name, contact email address and telephone number;

(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

3. Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.

4. Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

5. Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.

6. Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.

CHAPTER VI

INFORMATION SHARING

Article 29

Cybersecurity information-sharing arrangements

1. Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

3. Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).

4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.

Article 30

Voluntary notification of relevant information

1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by:

(a) essential and important entities with regard to incidents, cyber threats and near misses;

(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.

2. Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

CHAPTER VII

SUPERVISION AND ENFORCEMENT

Article 31

General aspects concerning supervision and enforcement

1. Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.

2. Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.

4. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

Article 32

Supervisory and enforcement measures in relation to essential entities

1. Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

(b) regular and targeted security audits carried out by an independent body or a competent authority;

(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(f) requests to access data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to:

(a) issue warnings about infringements of this Directive by the entities concerned;

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;

(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;

(h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;

(i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.

5. Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to:

(a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;

(b) request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.

Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such enforcement measures were applied. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Directive.

6. Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive.

As regards public administration entities, this paragraph shall be without prejudice to national law as regards the liability of public servants and elected or appointed officials.

7. When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:

  (i) repeated violations;

  (ii) a failure to notify or remedy significant incidents;

  (iii) a failure to remedy deficiencies following binding instructions from competent authorities;

  (iv) the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement;

  (v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23;

(b) the duration of the infringement;

(c) any relevant previous infringements by the entity concerned;

(d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;

(e) any intent or negligence on the part of the perpetrator of the infringement;

(f) any measures taken by the entity to prevent or mitigate the material or non-material damage;

(g) any adherence to approved codes of conduct or approved certification mechanisms;

(h) the level of cooperation of the natural or legal persons held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement measures. Before adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

9. Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive. Where appropriate, the competent authorities under Directive (EU) 2022/2557 may request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557.

10. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

Article 33

Supervisory and enforcement measures in relation to important entities

1. When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site *ex post* supervision conducted by trained professionals;

(b) targeted security audits carried out by an independent body or a competent authority;

(c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(d) requests for information necessary to assess, *ex post*, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to:

(a) issue warnings about infringements of this Directive by the entities concerned;

(b) adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive;

(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;

(h) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.

5. Article 32(6), (7) and (8) shall apply *mutatis mutandis* to the supervisory and enforcement measures provided for in this Article for important entities.

6. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

Article 34

General conditions for imposing administrative fines on essential and important entities

1. Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).

3. When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).

4. Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

5. Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

6. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.

7. Without prejudice to the powers of the competent authorities pursuant to Articles 32 and 33, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities.

8. Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. The Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024 and, without delay, any subsequent amendment law or amendment affecting them.

Article 35

Infringements entailing a personal data breach

1. Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.

2. Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an administrative fine pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive.

3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.

Article 36

Penalties

Member States shall lay down rules on penalties applicable to infringements of national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay of any subsequent amendment affecting them.

Article 37

Mutual assistance

1. Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:

(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;

(b) a competent authority may request another competent authority to take supervisory or enforcement measures;

(c) a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.

2. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.

CHAPTER VIII

DELEGATED AND IMPLEMENTING ACTS

Article 38

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 Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. The delegation of power referred to in Article 24(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 Article 24(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 two months of notification of that act to the European Parliament and to 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 two months at the initiative of the European Parliament or of the Council.

Article 39

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

CHAPTER IX

FINAL PROVISIONS

Article 40

Review

By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The report shall be accompanied, where necessary, by a legislative proposal.

Article 41

Transposition

1. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 18 October 2024.

2. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 42

Amendment of Regulation (EU) No 910/2014

In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024.

Article 43

Amendment of Directive (EU) 2018/1972

In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024.

Article 44

Repeal

Directive (EU) 2016/1148 is repealed with effect from 18 October 2024.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III.

Article 45

Entry into force

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

Article 46

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

ANNEX I

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2]) — Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 — Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])
	(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council ([5])
		— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission

Sector	Subsector	Type of entity
2. Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council ([10]), not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council ([11]), including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([12])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 ([13]) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([14])
3. Banking		Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council ([15])
4. Financial market infrastructures		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council ([16])
		— Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([17])

Sector	Subsector	Type of entity
5. Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([18])
		— EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([19])
		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([20]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([21])
6. Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([22]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([23]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers, excluding operators of root name servers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers
		— Providers of public electronic communications networks
		— Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		— Managed service providers — Managed security service providers

Sector	Subsector	Type of entity
10. Public administration		— Public administration entities of central governments as defined by a Member State in accordance with national law
		— Public administration entities at regional level as defined by a Member State in accordance with national law
11. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

(1) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).
(2) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
(3) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).
(4) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).
(5) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).
(6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).
(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).
(8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).
(9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).
(10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).
(11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).
(12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
(13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).
(14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).
(15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).
(16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).
(17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).
(18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).
(20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).
(21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).
(22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).
(23) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

ANNEX II

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council ([1]), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council ([2]) and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council ([3]) which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices	Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council ([4]), and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council ([5]) with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2

Sector	Subsector	Type of entity
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platforms
7. Research		Research organisations

([1]) Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

([2]) Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

([3]) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

([4]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

([5]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

ANNEX III

CORRELATION TABLE

Directive (EU) 2016/1148	This Directive
Article 1(1)	Article 1(1)
Article 1(2)	Article 1(2)
Article 1(3)	-
Article 1(4)	Article 2(12)
Article 1(5)	Article 2(13)
Article 1(6)	Article 2(6) and (11)
Article 1(7)	Article 4
Article 2	Article 2(14)
Article 3	Article 5
Article 4	Article 6
Article 5	–
Article 6	–
Article 7(1)	Article 7(1) and (2)
Article 7(2)	Article 7(4)
Article 7(3)	Article 7(3)
Article 8(1) to (5)	Article 8(1) to (5)
Article 8(6)	Article 13(4)
Article 8(7)	Article 8(6)
Article 9(1), (2) and (3)	Article 10(1), (2) and (3)
Article 9(4)	Article 10(9)
Article 9(5)	Article 10(10)
Article 10(1), (2) and (3), first subparagraph	Article 13(1), (2) and (3)
Article 10(3), second subparagraph	Article 23(9)
Article 11(1)	Article 14(1) and (2)
Article 11(2)	Article 14(3)
Article 11(3)	Article 14(4), first subparagraph, points (a) to (q) and (s), and paragraph (7)
Article 11(4)	Article 14(4), first subparagraph, point (r), and second subparagraph
Article 11(5)	Article 14(8)
Article 12(1) to (5)	Article 15(1) to (5)
Article 13	Article 17
Article 14(1) and (2)	Article 21(1) to (4)
Article 14(3)	Article 23(1)
Article 14(4)	Article 23(3)
Article 14(5)	Article 23(5), (6) and (8)

Directive (EU) 2016/1148	This Directive
Article 14(6)	Article 23(7)
Article 14(7)	Article 23(11)
Article 15(1)	Article 31(1)
Article 15(2), first subparagraph, point (a)	Article 32(2), point (e)
Article 15(2), first subparagraph, point (b)	Article 32(2), point (g)
Article 15(2), second subparagraph	Article 32(3)
Article 15(3)	Article 32(4), point (b)
Article 15(4)	Article 31(3)
Article 16(1) and (2)	Article 21(1) to (4)
Article 16(3)	Article 23(1)
Article 16(4)	Article 23(3)
Article 16(5)	–
Article 16(6)	Article 23(6)
Article 16(7)	Article 23(7)
Article 16(8) and (9)	Article 21(5) and Article 23(11)
Article 16(10)	–
Article 16(11)	Article 2(1), (2) and (3)
Article 17(1)	Article 33(1)
Article 17(2), point (a)	Article 32(2), point (e)
Article 17(2), point (b)	Article 32(4), point (b)
Article 17(3)	Article 37(1), points (a) and (b)
Article 18(1)	Article 26(1), point (b), and paragraph (2)
Article 18(2)	Article 26(3)
Article 18(3)	Article 26(4)
Article 19	Article 25
Article 20	Article 30
Article 21	Article 36
Article 22	Article 39
Article 23	Article 40
Article 24	–
Article 25	Article 41
Article 26	Article 45
Article 27	Article 46
Annex I, point (1)	Article 11(1)
Annex I, points (2)(a)(i) to (iv)	Article 11(2), points (a) to (d)

Directive (EU) 2016/1148	This Directive
Annex I, point (2)(a)(v)	Article 11(2), point (f)
Annex I, point (2)(b)	Article 11(4)
Annex I, points (2)(c)(i) and (ii)	Article 11(5), point (a)
Annex II	Annex I
Annex III, points (1) and (2)	Annex II, point (6)
Annex III, point (3)	Annex I, point (8)

DIRECTIVE (EU) 2022/2556 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 53(1) and 114 thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The Union needs to adequately and comprehensively address digital risks to all financial entities stemming from an increased use of information and communication technology (ICT) in the provision and consumption of financial services, thereby contributing to the realisation of the potential of digital finance, in terms of boosting innovation and promoting competition in a secure digital environment.

(2) Financial entities are heavily reliant on the use of digital technologies in their daily business. It is therefore of utmost importance to ensure the operational resilience of their digital operations against ICT risk. This need has become even more pressing due to the growth of breakthrough technologies in the market, in particular technologies enabling digital representations of value or of rights to be transferred and stored electronically, using distributed ledger or similar technology (crypto-assets), and of services related to those assets.

([1]) OJ C 343, 26.8.2021, p. 1.
([2]) OJ C 155, 30.4.2021, p. 38.
([3]) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.

(3) At Union level, the requirements related to the management of ICT risk in the financial sector are currently provided for in Directives 2009/65/EC ([4]), 2009/138/EC ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) and (EU) 2016/2341 ([11]) of the European Parliament and of the Council.

Those requirements are diverse and occasionally incomplete. In some cases, ICT risk has been addressed only implicitly as part of operational risk, and in other cases it has not been addressed at all. Those issues are remedied by the adoption of Regulation (EU) 2022/2554 of the European Parliament and of the Council ([12]). Those Directives should therefore be amended to ensure consistency with that Regulation. This Directive enacts a set of amendments that are necessary to bring legal clarity and consistency in relation to the application, by financial entities authorised and supervised in accordance with those Directives, of various digital operational resilience requirements that are necessary in the pursuit of their activities and in the provision of services, thereby guaranteeing the smooth functioning of the internal market. It is necessary to ensure the adequacy of those requirements in relation to market developments, while encouraging proportionality in particular with regard to the size of financial entities and the specific regimes to which they are subject, with the aim of reducing compliance costs.

(4) In the area of banking services, Directive 2013/36/EU currently sets out only general internal governance rules and operational risk provisions containing requirements for contingency and business continuity plans which implicitly serve as a basis for addressing ICT risk. However, in order to address ICT risk explicitly and clearly, the requirements for contingency and business continuity plans should be amended to also include business continuity plans and response and recovery plans concerning ICT risk, in accordance with the requirements laid down in Regulation (EU) 2022/2554. Furthermore, ICT risk is only implicitly included, as part of operational risk, in the supervisory review and evaluation process (SREP) performed by competent authorities and the criteria for its assessment are currently defined in the Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP), issued by the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([13]). In order to provide legal clarity and ensure that bank supervisors effectively identify ICT risk, and monitor its management by financial entities, in

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

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

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

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

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

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

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

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

([12]) 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 (See page1 of this Official Journal).

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

line with the new framework on digital operational resilience, the scope of the SREP should also be amended to explicitly refer to the requirements laid down in Regulation (EU) 2022/2554 and to cover in particular the risks revealed by major ICT-related incident reports and by the results of the digital operational resilience testing performed by financial entities in accordance with that Regulation.

(5) Digital operational resilience is essential to preserve the critical functions and core business lines of a financial entity in the event of its resolution, and thereby to avoid disruption to the real economy and to the financial system. Major operational incidents can hamper the capacity of a financial entity to continue operating and can jeopardise resolution objectives. Certain contractual arrangements on the use of ICT services are essential to ensure operational continuity and to provide the necessary data in the event of resolution. In order to be aligned with the objectives of the Union framework for operational resilience, Directive 2014/59/EU should be amended accordingly, with a view to ensuring that information relating to operational resilience is taken into account in the context of resolution planning and the assessment of financial entities' resolvability.

(6) Directive 2014/65/EU sets out more stringent ICT risk rules for investment firms and trading venues that are engaging in algorithmic trading. Less detailed requirements apply to data reporting services and to trade repositories. Also, Directive 2014/65/EU contains only limited references to control and safeguard arrangements for information processing systems and to the use of appropriate systems, resources and procedures to ensure continuity and regularity of business services. Furthermore, that Directive should be aligned with Regulation (EU) 2022/2554 as regards continuity and regularity in the provision of investment services and in the performance of investment activities, operational resilience, the capacity of trading systems, and the effectiveness of business continuity arrangements and risk management.

(7) Directive (EU) 2015/2366 sets out specific rules on ICT security controls and mitigation elements for the purposes of obtaining an authorisation to provide payment services. Those authorisation rules should be amended to align them with Regulation (EU) 2022/2554. Furthermore, in order to reduce the administrative burden and to avoid complexity and duplicative reporting requirements, the incident reporting rules in that Directive should cease to apply to payment service providers which are regulated under that Directive and also subject to Regulation (EU) 2022/2554, thus allowing those payment service providers to benefit from a single, fully harmonised incident reporting mechanism with regard to all operational or security payment-related incidents, irrespective of whether such incidents are ICT-related.

(8) Directives 2009/138/EC and (EU) 2016/2341 partially capture ICT risk within their general provisions on governance and risk management, leaving certain requirements to be specified through delegated acts with or without specific references to ICT risk. Similarly, only very general rules apply to managers of alternative investment funds subject to Directive 2011/61/EU and management companies subject to Directive 2009/65/EC. Those Directives should therefore be aligned with the requirements laid down in Regulation (EU) 2022/2554 with regard to the management of ICT systems and tools.

(9) In many cases, further ICT risk requirements have already been laid down in delegated and implementing acts, adopted on the basis of draft regulatory technical standards and draft implementing technical standards developed by the competent European Supervisory Authority. Since the provisions of Regulation (EU) 2022/2554 henceforth constitute the legal framework for ICT risk in the financial sector, certain empowerments to adopt delegated and implementing acts in Directives 2009/65/EC, 2009/138/EC, 2011/61/EU and 2014/65/EU should be amended to remove the ICT risk provisions from the scope of those empowerments.

(10) To ensure a consistent implementation of the new framework on digital operational resilience for the financial sector, Member States should apply the provisions of national law transposing this Directive from the date of application of Regulation (EU) 2022/2554.

(11) Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 have been adopted on the basis of Article 53(1) or Article 114 of the Treaty on the Functioning of the European Union (TFEU) or both. The amendments in this Directive have been included in a single legislative act due to the interconnectedness of the subject matter and objectives of the amendments. Consequently, this Directive should be adopted on the basis of both Article 53(1) and Article 114 TFEU.

(12) Since the objectives of this Directive cannot be sufficiently achieved by the Member States as they entail the harmonisation of requirements already contained in Directives but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(13) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([14]), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Amendments to Directive 2009/65/EC

Article 12 of Directive 2009/65/EC is amended as follows:

(1) in the second subparagraph of paragraph 1, point (a) is replaced by the following:

'(a) has sound administrative and accounting procedures, control and safeguard arrangements for electronic data processing, including with regard to network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as adequate internal control mechanisms, including, in particular, rules for personal transactions by its employees or for the holding or management of investments in financial instruments in order to invest on its own account and ensuring, at least, that each transaction involving the UCITS may be reconstructed according to its origin, the parties to it, its nature, and the time and place at which it was effected and that the assets of the UCITS managed by the management company are invested according to the fund rules or the instruments of incorporation and the legal provisions in force;

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) paragraph 3 is replaced by the following:

'3. Without prejudice to Article 116, the Commission shall adopt, by means of delegated acts in accordance with Article 112a, measures specifying:

(a) the procedures and arrangements referred to in point (a) of the second subparagraph of paragraph 1, other than the procedures and arrangements concerning network and information systems;

(b) the structures and organisational requirements to minimise conflicts of interests referred to in point (b) of the second subparagraph of paragraph 1.'.

([14]) OJ C 369, 17.12.2011, p. 14.

Article 2

Amendments to Directive 2009/138/EC

Directive 2009/138/EC is amended as follows:

(1) in Article 41, paragraph 4 is replaced by the following:

'4. Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertakings shall employ appropriate and proportionate systems, resources and procedures, and shall, in particular, set up and manage network and information systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) in Article 50(1), points (a) and (b) are replaced by the following:

'(a) the elements of the systems referred to in Article 41, Article 44, in particular the areas listed in Article 44(2), and Articles 46 and 47, other than the elements concerning information and communication technology risk management;

(b) the functions referred to in Articles 44, 46, 47 and 48, other than functions related to information and communication technology risk management.'.

Article 3

Amendment to Directive 2011/61/EU

Article 18 of Directive 2011/61/EU is replaced by the following:

'*Article 18*

General principles

1. Member States shall require that AIFMs use, at all times, adequate and appropriate human and technical resources that are necessary for the proper management of AIFs.

In particular, the competent authorities of the home Member State of the AIFM, having regard also to the nature of the AIFs managed by the AIFM, shall require that the AIFM has sound administrative and accounting procedures, control and safeguard arrangements for electronic data processing, including with regard to network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as adequate internal control mechanisms, including, in particular, rules for personal transactions by its employees or for the holding or management of investments in order to invest on its own account and ensuring, at least, that each transaction involving the AIFs may be reconstructed according to its origin, the parties to it, its nature, and the time and place at which it was effected and that the assets of the AIFs managed by the AIFM are invested in accordance with the AIF rules or instruments of incorporation and the legal provisions in force.

2. The Commission shall, by means of delegated acts in accordance with Article 56 and subject to the conditions of Articles 57 and 58, adopt measures specifying the procedures and arrangements referred to in paragraph 1 of this Article, other than the procedures and arrangements concerning network and information systems.

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).'.

Article 4

Amendments to Directive 2013/36/EU

Directive 2013/36/EU is amended as follows:

(1) in Article 65(3), point (a)(vi) is replaced by the following:

'(vi) third parties to whom the entities referred to in points (i) to (iv) have outsourced functions or activities, including ICT third-party service providers referred to in Chapter V of Regulation (EU) 2022/2554 of the European Parliament and of the Council (*);

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(2) in Article 74(1), the first subparagraph is replaced by the following:

'Institutions shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554, and remuneration policies and practices that are consistent with and promote sound and effective risk management.';

(3) in Article 85, paragraph 2 is replaced by the following:

'2. Competent authorities shall ensure that institutions have adequate contingency and business continuity policies and plans, including ICT business continuity policies and plans and ICT response and recovery plans for the technology they use for the communication of information, and that those plans are established, managed and tested in accordance with Article 11 of Regulation (EU) 2022/2554, in order to allow institutions to keep operating in the event of severe business disruption and limit losses incurred as a consequence of such disruption.';

(4) in Article 97(1), the following point is added:

'(d) risks revealed by digital operational resilience testing in accordance with Chapter IV of Regulation (EU) 2022/2554.'.

Article 5

Amendments to Directive 2014/59/EU

Directive 2014/59/EU is amended as follows:

(1) Article 10 is amended as follows:

(a) in paragraph 7, point (c) is replaced by the following:

'(c) a demonstration of how critical functions and core business lines could be legally and economically separated, to the extent necessary, from other functions so as to ensure continuity and digital operational resilience upon the failure of the institution;';

(b) in paragraph 7, point (q) is replaced by the following:

'(q) a description of essential operations and systems for maintaining the continuous functioning of the institution's operational processes, including network and information systems as referred to in Regulation (EU) 2022/2554 of the European Parliament and of the Council (*);

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(c) in paragraph 9, the following subparagraph is added:

'In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards in order to, inter alia, take account of the provisions of Chapter II of Regulation (EU) 2022/2554.';

(2) the Annex is amended as follows:

(a) in Section A, point (16) is replaced by the following:

'(16) arrangements and measures necessary to maintain the continuous functioning of the institution's operational processes, including network and information systems that are set up and managed in accordance with Regulation (EU) 2022/2554;';

(b) Section B is amended as follows:

(i) point (14) is replaced by the following:

'(14) an identification of the owners of the systems identified in point (13), service level agreements related thereto, and any software and systems or licenses, including a mapping to their legal entities, critical operations and core business lines, as well as an identification of critical ICT third-party service providers as defined in Article 3, point (23), of Regulation (EU) 2022/2554;';

(ii) the following point is inserted:

'(14a) the results of institutions' digital operational resilience testing under Regulation (EU) 2022/2554;';

(c) Section C is amended as follows:

(i) point (4) is replaced by the following:

'(4) the extent to which the service agreements, including contractual arrangements on the use of ICT services, that the institution maintains are robust and fully enforceable in the event of resolution of the institution;';

(ii) the following point is inserted:

'(4a) the digital operational resilience of the network and information systems supporting critical functions and core business lines of the institution, taking into account major ICT-related incident reports and the results of digital operational resilience testing under Regulation (EU) 2022/2554;'.

Article 6

Amendments to Directive 2014/65/EU

Directive 2014/65/EU is amended as follows:

(1) Article 16 is amended as follows:

(a) paragraph 4 is replaced by the following:

'4. An investment firm shall take reasonable steps to ensure continuity and regularity in the performance of investment services and activities. To that end, the investment firm shall employ appropriate and proportionate systems, including information and communication technology ("ICT") systems that are set up and managed in accordance with Article 7 of Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), as well as appropriate and proportionate resources and procedures.

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(b) in paragraph 5, the second and third subparagraphs are replaced by the following:

'An investment firm shall have sound administrative and accounting procedures, internal control mechanisms and effective procedures for risk assessment.

Without prejudice to the ability of competent authorities to require access to communications in accordance with this Directive and Regulation (EU) No 600/2014, an investment firm shall have sound security mechanisms in place to ensure, in accordance with the requirements laid down in Regulation (EU) 2022/2554, the security and authentication of the means of transfer of information, to minimise the risk of data corruption and unauthorised access and to prevent information leakage, thereby maintaining the confidentiality of the data at all times.';

(2) Article 17 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. An investment firm that engages in algorithmic trading shall have in place effective systems and risk controls suitable to the business it operates to ensure that its trading systems are resilient and have sufficient capacity in accordance with the requirements laid down in Chapter II of Regulation (EU) 2022/2554, are subject to appropriate trading thresholds and limits and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market.

Such a firm shall also have in place effective systems and risk controls to ensure the trading systems cannot be used for any purpose that is contrary to Regulation (EU) No 596/2014 or to the rules of a trading venue to which it is connected.

The investment firm shall have in place effective business continuity arrangements to deal with any failure of its trading systems, including ICT business continuity policy and plans and ICT response and recovery plans established in accordance with Article 11 of Regulation (EU) 2022/2554, and shall ensure its systems are fully tested and properly monitored to ensure that they meet the general requirements laid down in this paragraph and any specific requirements laid down in Chapters II and IV of Regulation (EU) 2022/2554.';

(b) in paragraph 7, point (a) is replaced by the following:

'(a) the details of organisational requirements laid down in paragraphs 1 to 6, other than those related to ICT risk management, which are to be imposed on investment firms providing different investment services, investment activities, ancillary services or combinations thereof, whereby the specifications in relation to the organisational requirements laid down in paragraph 5 shall set out specific requirements for direct market access and for sponsored access in such a way as to ensure that the controls applied to sponsored access are at least equivalent to those applied to direct market access;';

(3) in Article 47, paragraph 1 is amended as follows:

(a) point (b) is replaced by the following:

'(b) to be adequately equipped to manage the risks to which it is exposed, including to manage ICT risk in accordance with Chapter II of Regulation (EU) 2022/2554, to implement appropriate arrangements and systems for identifying significant risks to its operation, and to put in place effective measures to mitigate those risks;';

(b) point (c) is deleted;

(4) Article 48 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Member States shall require a regulated market to establish and maintain its operational resilience in accordance with the requirements laid down in Chapter II of Regulation (EU) 2022/2554 to ensure its trading systems are resilient, have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, are fully tested to ensure such conditions are met and are subject to effective business continuity arrangements, including ICT business continuity policy and plans and ICT response and recovery plans established in accordance with Article 11 of Regulation (EU) 2022/2554, to ensure continuity of its services if there is any failure of its trading systems.';

(b) paragraph 6 is replaced by the following:

'6. Member States shall require a regulated market to have in place effective systems, procedures and arrangements, including requiring members or participants to carry out appropriate testing of algorithms and providing environments to facilitate such testing in accordance with the requirements laid down in Chapters II and IV of Regulation (EU) 2022/2554, to ensure that algorithmic trading systems cannot create or contribute to disorderly trading conditions on the market and to manage any disorderly trading conditions which do arise from such algorithmic trading systems, including systems to limit the ratio of unexecuted orders to transactions that may be entered into the system by a member or participant, to be able to slow down the flow of orders if there is a risk of its system capacity being reached and to limit and enforce the minimum tick size that may be executed on the market.';

(c) paragraph 12 is amended as follows:

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

'(a) the requirements to ensure trading systems of regulated markets are resilient and have adequate capacity, except the requirements related to digital operational resilience;';

(ii) point (g) is replaced by the following:

'(g) the requirements to ensure appropriate testing of algorithms, other than digital operational resilience testing, so as to ensure that algorithmic trading systems including high-frequency algorithmic trading systems cannot create or contribute to disorderly trading conditions on the market.'.

Article 7

Amendments to Directive (EU) 2015/2366

Directive (EU) 2015/2366 is amended as follows:

(1) in Article 3, point (j) is replaced by the following:

'(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information and communication technology (ICT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services;';

(2) Article 5(1) is amended as follows:

(a) the first subparagraph is amended as follows:

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

'(e) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures as well as arrangements for the use of ICT services in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), which demonstrates that those governance arrangements and internal control mechanisms are proportionate, appropriate, sound and adequate;

(*) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L333, 27.12.2022, p.1).';

(ii) point (f) is replaced by the following:

'(f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incident reporting mechanism which takes account of the notification obligations of the payment institution laid down in Chapter III of Regulation (EU) 2022/2554;';

(iii) point (h) is replaced by the following:

'(h) a description of business continuity arrangements including a clear identification of the critical operations, effective ICT business continuity policy and plans and ICT response and recovery plans and a procedure to regularly test and review the adequacy and efficiency of such plans in accordance with Regulation (EU) 2022/2554;';

(b) the third subparagraph is replaced by the following:

'The security control and mitigation measures referred to in point (j) of the first subparagraph shall indicate how they ensure a high level of digital operational resilience in accordance with Chapter II of Regulation (EU) 2022/2554, in particular in relation to technical security and data protection, including for the software and ICT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations. Those measures shall also include the security measures laid down in Article 95(1) of this Directive. Those measures shall take into account EBA's guidelines on security measures as referred to in Article 95(3) of this Directive, when in place.';

(3) in Article 19(6), the second subparagraph is replaced by the following:

'Outsourcing of important operational functions, including ICT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authorities to monitor and retrace the payment institution's compliance with all of the obligations laid down in this Directive.';

(4) in Article 95(1), the following subparagraph is added:

'The first subparagraph is without prejudice to the application of Chapter II of Regulation (EU) 2022/2554 to:

(a) payment service providers referred to in points (a), (b) and (d) of Article 1(1) of this Directive;

(b) account information service providers referred to in Article 33(1) of this Directive;

(c) payment institutions exempted pursuant to Article 32(1) of this Directive; and

(d) electronic money institutions benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC.';

(5) in Article 96, the following paragraph is added:

'7. Members States shall ensure that paragraphs 1 to 5 of this Article do not apply to:

(a) payment service providers referred to in points (a), (b) and (d) of Article 1(1) of this Directive;

(b) account information service providers referred to in Article 33(1) of this Directive;

(c) payment institutions exempted pursuant to Article 32(1) of this Directive; and

(d) electronic money institutions benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC.';

(6) in Article 98, paragraph 5 is replaced by the following:

'5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments, and of the provisions of Chapter II of Regulation (EU) 2022/2554.'.

Article 8

Amendment to Directive (EU) 2016/2341

Article 21(5) of Directive (EU) 2016/2341 is replaced by the following:

'5. Member States shall ensure that IORPs take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, IORPs shall employ

appropriate and proportionate systems, resources and procedures, and shall, in particular, set up and manage network and information systems in accordance with Regulation (EU) 2022/2554 of the European Parliament and of the Council (*), where applicable.

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

Article 9

Transposition

1. By 17 January 2025, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 17 January 2025.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

Article 10

Entry into force

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

Article 11

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on the resilience of critical entities and repealing Council Directive 2008/114/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

(2) Council Directive 2008/114/EC ([4]) provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted

([1]) OJ C 286, 16.7.2021, p. 170.
([2]) OJ C 440, 29.10.2021, p. 99.
([3]) Position of the European Parliament of 22 November 2022 (not yet published in the Official Journal) and Council decision of 8 December 2022.
([4]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

to enhance the resilience of critical entities. Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services.

(3) While a number of measures at Union level, such as the European Programme for Critical Infrastructure Protection, and at national level aim to support the protection of critical infrastructure in the Union, more should be done to better equip the entities operating such infrastructure to address the risks to their operations that could result in the disruption of the provision of essential services. More should also be done to better equip such entities because there is a dynamic threat landscape, which includes evolving hybrid and terrorist threats, and growing interdependencies between infrastructure and sectors. Moreover, there is an increased physical risk due to natural disasters and climate change, which intensifies the frequency and scale of extreme weather events and brings long-term changes in average climate conditions that can reduce the capacity, efficiency and lifespan of certain infrastructure types if climate adaptation measures are not in place. In addition, the internal market is characterised by fragmentation in respect of the identification of critical entities because relevant sectors and categories of entities are not recognised consistently as critical in all Member States. This Directive should therefore achieve a solid level of harmonisation in terms of the sectors and categories of entities falling within its scope.

(4) While certain sectors of the economy, such as the energy and transport sectors, are already regulated by sector-specific Union legal acts, those legal acts contain provisions which relate only to certain aspects of resilience of entities operating in those sectors. In order to address in a comprehensive manner the resilience of those entities that are critical for the proper functioning of the internal market, this Directive creates an overarching framework that addresses the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional.

(5) The growing interdependencies between infrastructure and sectors are the result of an increasingly cross-border and interdependent network of service provision using key infrastructure across the Union in the energy, transport, banking, drinking water, waste water, production, processing and distribution of food, health, space, financial market infrastructure and digital infrastructure sectors and in certain aspects of the public administration sector. The space sector falls within the scope of this Directive with respect to the provision of certain services that depend on ground-based infrastructure owned, managed and operated either by Member States or by private parties; consequently, infrastructure owned, managed or operated by or on behalf of the Union as part of its space programme does not fall within the scope of this Directive.

In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that, where deemed appropriate, electricity generation can include electricity transmission parts of nuclear power plants but excludes the specifically nuclear elements covered by treaties and Union law, including relevant legal acts of the Union concerning nuclear power. The process for identifying critical entities in the food sector should adequately reflect the nature of the internal market in that sector and the extensive Union rules relating to the general principles and requirements of food law and food safety. Therefore, in order to ensure that there is a proportionate approach and to adequately reflect the role and importance of those entities at national level, critical entities should only be identified among food businesses, whether for profit or not and whether public or private, that are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing with a significant market share as observed at national level. Those interdependencies mean that any disruption of essential services, even one which is initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in a far-reaching and long-term negative impact on the delivery of services across the internal market. Major crises, such as the COVID-19 pandemic, have shown the vulnerability of our increasingly interdependent societies in the face of high-impact low-probability risks.

(6) The entities involved in the provision of essential services are increasingly subject to diverging requirements imposed under national law. The fact that some Member States have less stringent security requirements on those entities not only leads to various levels of resilience but also risks negatively impacting the maintenance of vital societal functions or economic activities across the Union and leads to obstacles to the proper functioning of the internal market. Investors and companies can rely on and trust critical entities that are resilient, and reliability and trust are the cornerstones of a well-functioning internal market. Similar types of entities are considered as critical in some Member States but not in others, and those which are identified as critical are subject to divergent requirements in different Member States. That results in an additional and unnecessary administrative burden for companies operating across borders, in particular for companies active in Member States with more stringent requirements. A Union framework would therefore also have the effect of levelling the playing field for critical entities across the Union.

(7) It is necessary to lay down harmonised minimum rules to ensure the provision of essential services in the internal market, to enhance the resilience of critical entities and to improve cross-border cooperation between competent authorities. It is important that those rules be future proof in terms of their design and implementation while allowing for necessary flexibility. It is also crucial to improve the capacity of critical entities to provide essential services in the face of a diverse set of risks.

(8) In order to achieve a high level of resilience, Member States should identify critical entities that will be subject to specific requirements and supervision and that will be provided with particular support and guidance in the face of all relevant risks.

(9) Given the importance of cybersecurity for the resilience of critical entities and in the interests of consistency, a coherent approach should be ensured, wherever possible, between this Directive and Directive (EU) 2022/2555 of the European Parliament and of the Council ([5]). In light of the higher frequency and particular characteristics of cyber risks, Directive (EU) 2022/2555 imposes comprehensive requirements on a large set of entities to ensure their cybersecurity. Given that cybersecurity is addressed sufficiently in Directive (EU) 2022/2555, the matters covered by that Directive should be excluded from the scope of this Directive, without prejudice to the particular regime for entities in the digital infrastructure sector.

(10) Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience, and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive should not apply, so as to avoid duplication and unnecessary burden. In that case, the relevant provisions of such Union legal acts should apply. Where the relevant provisions of this Directive do not apply, the provisions on supervision and enforcement laid down in this Directive should not apply either.

(11) This Directive does not affect the competence of Member States and their authorities in terms of administrative autonomy or their responsibility for safeguarding national security and defence or their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order. The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should fall within the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries.

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

Certain critical entities carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or provide services exclusively to public administration entities that carry out activities predominantly in those areas. In light of the Member States' responsibility for safeguarding national security and defence, Member States should be able to decide that the obligations on critical entities laid down in this Directive do not apply, in whole or in part, to those critical entities if the services they provide or the activities they perform are predominantly related to the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. Critical entities whose services or activities are only marginally related to those areas should fall within the scope of this Directive. No Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security. Union or national rules for the protection of classified information and non-disclosure agreements are of relevance.

(12) In order not to jeopardise national security or the security and commercial interests of critical entities, sensitive information should be accessed, exchanged and handled prudently and with particular attention to the transmission channels and storage capacities used.

(13) With a view to ensuring a comprehensive approach to the resilience of critical entities, each Member State should have in place a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy should set out the strategic objectives and policy measures to be implemented. In the interests of coherence and efficiency, the strategy should be designed to seamlessly integrate existing policies, building, wherever possible, upon relevant existing national and sectoral strategies, plans or similar documents. In order to achieve a comprehensive approach, Member States should ensure that their strategies provide for a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 in the context of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and in the context of the exercise of supervisory tasks. When putting in place their strategies, Member States should take due account of the hybrid nature of threats to critical entities.

(14) Member States should communicate their strategies and substantial updates thereto to the Commission, in particular to enable the Commission to assess the correct application of this Directive as regards policy approaches to the resilience of critical entities at national level. Where necessary, the strategies could be communicated as classified information. The Commission should draw up a summary report of the strategies communicated by Member States to serve as a basis for exchanges to identify best practices and issues of common interest in the framework of a Critical Entities Resilience Group. Due to the sensitive nature of the aggregated information included in the summary report, whether classified or not, the Commission should manage the summary report with the appropriate level of awareness with respect for the security of critical entities, Member States and the Union. The summary report and the strategies should be safeguarded against unlawful or malicious action and should be accessible only to authorised persons in order to fulfil the objectives of this Directive. The communication of the strategies and substantial updates thereto should also help the Commission to understand developments in approaches to the resilience of critical entities and feed into the monitoring of the impact and added value of this Directive, which the Commission is to review periodically.

(15) The actions of Member States to identify and help ensure the resilience of critical entities should follow a risk-based approach that focuses on the entities most relevant for the performance of vital societal functions or economic activities. In order to ensure such a targeted approach, each Member State should carry out, within a harmonised framework, an assessment of the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, that could affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics and hybrid threats or other antagonistic threats, including terrorist offences, criminal infiltration and sabotage ('Member State risk assessment'). When carrying out Member State risk assessments, Member States should take into account other general or sector-specific risk assessments carried out pursuant to other Union legal acts and should consider the extent to which sectors depend on one another, including on sectors in other Member States and third countries. The outcome of Member State risk assessments should be used for the purposes of identifying critical entities and assisting those entities in meeting their resilience requirements. This Directive applies only to Member States and critical entities that operate within the Union.

Nevertheless, the expertise and knowledge generated by competent authorities, in particular through risk assessments, and by the Commission, in particular through various forms of support and cooperation, could be used, where appropriate and in accordance with the applicable legal instruments, for the benefit of third countries, in particular those in the direct neighbourhood of the Union, by feeding into existing cooperation on resilience.

(16) In order to ensure that all relevant entities are subject to the resilience requirements of this Directive and to reduce divergences in that respect, it is important to lay down harmonised rules allowing for a consistent identification of critical entities across the Union, while also allowing Member States to adequately reflect the role and importance of those entities at national level. When applying the criteria laid down in this Directive, each Member State should identify entities that provide one or more essential services and that operate and have critical infrastructure located on its territory. An entity should be considered to operate on the territory of a Member State in which it carries out activities necessary for the essential service or services in question and in which that entity's critical infrastructure, which is used to provide that service or those services, is located. Where no entity meets those criteria in a Member State, that Member State should be under no obligation to identify a critical entity in the corresponding sector or subsector. In the interests of effectiveness, efficiency, consistency and legal certainty, appropriate rules should be established as regards notifying entities that they have been identified as critical entities.

(17) Member States should submit to the Commission, in a manner that fulfils the objectives of this Directive, a list of essential services, the number of critical entities identified for each of the sectors and subsectors set out in the Annex and for the essential service or services that each entity provides and, if applied, thresholds. It should be possible to present thresholds as such or in aggregated form, meaning that the information can be averaged by geographic area, by year, by sector, by subsector or by other means, and can include information on the range of the indicators provided.

(18) Criteria should be established to determine the significance of a disruptive effect produced by an incident. Those criteria should build on the criteria set out in Directive (EU) 2016/1148 of the European Parliament and of the Council ([6]) in order to capitalise on the efforts carried out by Member States to identify operators of essential services as defined in that Directive and the experience gained in that regard. Major crises, such as the COVID-19 pandemic, have shown the importance of ensuring the security of the supply chain and have demonstrated how its disruption can have a negative economic and societal impact across a large number of sectors and across borders. Therefore, Member States should also consider effects on the supply chain, to the extent possible, when determining the extent to which other sectors and subsectors depend on the essential service provided by a critical entity.

(19) In accordance with applicable Union and national law, including Regulation (EU) 2019/452 of the European Parliament and of the Council ([7]), which establishes a framework for the screening of foreign direct investments in the Union, the potential threat posed by foreign ownership of critical infrastructure within the Union is to be acknowledged because services, the economy and the free movement and safety of Union citizens depend on the proper functioning of critical infrastructure.

(20) Directive (EU) 2022/2555 requires entities belonging to the digital infrastructure sector, which might be identified as critical entities under this Directive, to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems and to notify significant incidents and cyber threats. Since threats to the security of network and information systems can have different origins, Directive (EU) 2022/2555 applies an all-hazards approach that includes the resilience of network and information systems, as well as the physical components and environment of those systems.

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

([7]) Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79 I, 21.3.2019, p. 1).

Given that the requirements laid down in Directive (EU) 2022/2555 in that regard are at least equivalent to the corresponding obligations laid down in this Directive, the obligations laid down in Article 11 and Chapters III, IV and VI of this Directive should not apply to entities belonging to the digital infrastructure sector in order to avoid duplication and unnecessary administrative burden. However, considering the importance of the services provided by entities belonging to the digital infrastructure sector to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive, entities belonging to the digital infrastructure sector as critical entities. Consequently, the strategies, the Member State risk assessments and the support measures set out in Chapter II of this Directive should apply. Member States should be able to adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

(21) Union financial services law establishes comprehensive requirements on financial entities to manage all risks they face, including operational risks, and to ensure business continuity. Such law includes Regulations (EU) No 648/2012 ([8]), (EU) No 575/2013 ([9]) and (EU) No 600/2014 ([10]) of the European Parliament and of the Council and Directives 2013/36/EU ([11]) and 2014/65/EU ([12]) of the European Parliament and of the Council. That legal framework is complemented by Regulation (EU) 2022/2554 of the European Parliament and of the Council ([13]), which lays down requirements applicable to financial entities to manage Information and Communication Technology (ICT) risks, including concerning the protection of physical ICT infrastructure. Since the resilience of those entities is therefore comprehensively covered, Article 11 and Chapters III, IV and VI of this Directive should not apply to those entities in order to avoid duplication and unnecessary administrative burden.

However, considering the importance of the services provided by entities in the financial sector to critical entities belonging to all other sectors, Member States should identify, based on the criteria and using the procedure provided for in this Directive, entities in the financial sector as critical entities. Consequently, the strategies, the Member State risk assessments and the support measures set out in Chapter II of this Directive should apply. Member States should be able to adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities provided that those provisions are consistent with applicable Union law.

(22) Member States should designate or establish authorities competent to supervise the application of and, where necessary, enforce the rules of this Directive and ensure that those authorities are adequately empowered and resourced. In light of the differences in national governance structures, in order to safeguard existing sectoral arrangements or Union supervisory and regulatory bodies, and in order to avoid duplication, Member States should be able to designate or establish more than one competent authority. Where Member States designate or establish more than one competent authority, they should clearly delineate the respective tasks of the authorities concerned and ensure that they cooperate smoothly and effectively. All competent authorities should also cooperate more generally with other relevant authorities, at both Union and national level.

([8]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

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

([10]) Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

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

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

([13]) 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 (see page 1 of this Official Journal).

(23) In order to facilitate cross-border cooperation and communication and to enable the effective implementation of this Directive, each Member State should, without prejudice to the requirements of sector-specific Union legal acts, designate one single point of contact responsible for coordinating issues related to the resilience of critical entities and cross-border cooperation at Union level ('single point of contact'), where relevant within a competent authority. Each single point of contact should liaise and coordinate communication, where relevant, with the competent authorities of its Member State, with the single points of contact of other Member States and with the Critical Entities Resilience Group.

(24) The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information in relation to cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities as well as in relation to relevant measures taken by competent authorities under this Directive and competent authorities under Directive (EU) 2022/2555. It is important that Member States ensure that the requirements provided for in this Directive and in Directive (EU) 2022/2555 are implemented in a complementary manner and that critical entities are not subject to an administrative burden beyond that which is necessary to achieve the objectives of this Directive and that Directive.

(25) Member States should support critical entities, including those that qualify as small or medium-sized enterprises, in strengthening their resilience, in compliance with Member State obligations laid down in this Directive, without prejudice to the critical entities' own legal responsibility to ensure such compliance and, in so doing, prevent excessive administrative burden. Member States could, in particular, develop guidance materials and methodologies, support the organisation of exercises to test the resilience of critical entities and provide advice and training to the personnel of critical entities. Where necessary and justified by public interest objectives, Member States could provide financial resources and should facilitate voluntary information sharing and the exchange of good practices between critical entities, without prejudice to the application of competition rules laid down in the Treaty on the Functioning of the European Union (TFEU).

(26) With the aim of enhancing the resilience of critical entities identified by Member States and in order to reduce the administrative burden on those critical entities, the competent authorities should consult one another, whenever appropriate, for the purpose of ensuring that this Directive is applied in a consistent manner. Those consultations should be entered into at the request of any interested competent authority and should focus on ensuring a convergent approach regarding interlinked critical entities that use critical infrastructure which is physically connected between two or more Member States, that belong to the same groups or corporate structures, or that have been identified in one Member State and that provide essential services to or in other Member States.

(27) Where provisions of Union or national law require critical entities to assess risks relevant for the purposes of this Directive and to take measures to ensure their own resilience, those requirements should be adequately considered for the purpose of supervising the compliance of critical entities with this Directive.

(28) Critical entities should have a comprehensive understanding of the relevant risks to which they are exposed and a duty to analyse those risks. To that end, they should carry out risk assessments whenever necessary in view of their particular circumstances and the evolution of those risks and, in any event, every four years, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment'). Where critical entities have carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for their critical entity risk assessment, they should be able to use those assessments and documents to meet the requirements set out in this Directive concerning critical entity risk assessments. A competent authority should be able to declare that an existing risk assessment carried out by a critical entity that addresses the relevant risks and the relevant extent of dependence is compliant, in whole or in part, with the obligations laid down in this Directive.

(29) Critical entities should take technical, security and organisational measures that are appropriate and proportionate to the risks they face so as to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident. While critical entities should take those measures in accordance with this Directive, the details and extent of such measures should reflect the different risks that each critical entity has identified as part of its critical entity risk assessment and the specificities of such entity in an appropriate and proportionate way. To promote a coherent Union approach, the Commission should, after consulting the Critical Entities Resilience Group, adopt non-binding guidelines to further specify those technical, security and organisational measures. Member States should ensure that each critical entity designate a liaison officer or equivalent as point of contact with the competent authorities.

(30) In the interests of effectiveness and accountability, critical entities should describe the measures they take, with a level of detail that sufficiently achieves the aims of effectiveness and accountability, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. Where a critical entity has already taken technical, security and organisational measures and drawn up documents pursuant to other legal acts that are relevant for resilience-enhancing measures under this Directive, it should be able, in order to avoid duplication, to use those measures and documents to meet the requirements as regards resilience measures under this Directive. In order to avoid duplication, a competent authority should be able to declare existing resilience measures taken by a critical entity that address its obligation to take technical, security and organisational measures pursuant to this Directive as compliant, in whole or in part, with the requirements of this Directive.

(31) Regulations (EC) No 725/2004 ([14]) and (EC) No 300/2008 ([15]) of the European Parliament and of the Council and Directive 2005/65/EC of the European Parliament and of the Council ([16]) establish requirements applicable to entities in the aviation and maritime transport sectors to prevent incidents caused by unlawful acts and to resist and mitigate the consequences of such incidents. While the measures required under this Directive are broader in terms of risks addressed and types of measures to be taken, critical entities in those sectors should reflect in their resilience plan or equivalent documents the measures taken pursuant to those other Union legal acts. Critical entities are also to take into consideration Directive 2008/96/EC of the European Parliament and of the Council ([17]), which introduces a network-wide road assessment to map the risk of accidents and a targeted road safety inspection to identify hazardous conditions, defects and problems that increase the risk of accidents and injuries, based on site visits of existing roads or sections of roads. Ensuring the protection and resilience of critical entities is of the utmost importance for the railway sector and, when implementing resilience measures under this Directive, critical entities are encouraged to refer to non-binding guidelines and good practices documents developed under sectorial workstreams, such as the EU Rail Passenger Security Platform set up by Commission Decision 2018/C 232/03 ([18]).

(32) The risk of employees of critical entities or their contractors misusing, for instance, their access rights within the critical entity's organisation to harm and cause damage is of increasing concern. Member States should therefore specify the conditions under which critical entities are permitted, in duly reasoned cases and taking into account Member State risk assessments, to submit requests for background checks on persons falling within specific categories of its personnel. It should be ensured that the relevant authorities assess such requests within a reasonable timeframe and process them in accordance with national law and procedures and relevant and applicable Union law, including on the protection of personal data. In order to corroborate the identity of a person who is the subject of a background check, it is appropriate for Member States to require proof of identity, such as a passport, a national identity card or a digital form of identification, in accordance with applicable law.

([14]) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

([15]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

([16]) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

([17]) Directive 2008/96/EC of the European Parliament and of the Council of 19 November 2008 on road infrastructure safety management (OJ L 319, 29.11.2008, p. 59).

([18]) Commission Decision of 29 June 2018 setting up the EU Rail Passenger Security Platform 2018/C 232/03 (OJ C 232, 3.7.2018, p. 10).

Background checks should include a check of the criminal records of the person concerned. Member States should use the European Criminal Records Information System in accordance with the procedures set out in Council Framework Decision 2009/315/JHA ([19]) and, where relevant and applicable, Regulation (EU) 2019/816 of the European Parliament and of the Council ([20]) for the purpose of obtaining information from criminal records held by other Member States. Member States might also, where relevant and applicable, draw on the Second Generation Schengen Information System (SIS II) established by Regulation (EU) 2018/1862 of the European Parliament and of the Council ([21]), intelligence and any other objective information available that might be necessary to determine the suitability of the person concerned to work in the position in relation to which the critical entity has requested a background check.

(33) A mechanism for the notification of certain incidents should be established to allow the competent authorities to respond to incidents rapidly and adequately and to have a comprehensive overview of the impact, nature, cause and possible consequences of incidents with which the critical entities deal. Critical entities should notify, without undue delay, the competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Unless operationally unable to do so, critical entities should submit an initial notification no later than 24 hours after becoming aware of an incident. The initial notification should only include the information strictly necessary to make the competent authority aware of the incident and allow the critical entity to seek assistance, if required. Such a notification should indicate, where possible, the presumed cause of the incident. Member States should ensure that the requirement to submit that initial notification does not divert the critical entity's resources from activities related to incident handling, which should be prioritised. The initial notification should be followed, where relevant, by a detailed report no later than one month after the incident. The detailed report should complement the initial notification and provide a more complete overview of the incident.

(34) Standardisation should remain primarily a market-driven process. However, there might still be situations in which it is appropriate to require compliance with specific standards. Member States should, where useful, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.

(35) While critical entities generally operate as part of an increasingly interconnected network of service provision and infrastructure and often provide essential services in more than one Member State, some of those critical entities are of particular significance for the Union and its internal market because they provide essential services to or in six or more Member States and, therefore, could benefit from specific support at Union level. Rules on advisory missions in respect of such critical entities of particular European significance should therefore be established. Those rules are without prejudice to the rules on supervision and enforcement set out in this Directive.

(36) On a reasoned request from the Commission or from one or more Member States to or in which the essential service is provided, where additional information is necessary to be able to advise a critical entity in meeting its obligations under this Directive or to assess the compliance of a critical entity of particular European significance with those obligations, the Member State that has identified a critical entity of particular European significance as a critical entity should provide the Commission with certain information as set out in this Directive. In agreement with the Member State that has identified the critical entity of particular European significance as a critical entity, the Commission should be able to organise an advisory mission to assess the measures put in place by that entity. In order to ensure that such advisory missions are carried out properly, complementary rules should be established, in particular on the organisation and conduct of the advisory missions, the follow-up actions to be taken and the obligations for the critical entities of particular European significance concerned. The advisory mission should,

([19]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

([20]) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

([21]) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

without prejudice to the need for the Member State in which the advisory mission is conducted and the critical entity concerned to comply with the rules laid down in this Directive, be conducted subject to the detailed rules of the law of that Member State, for instance on the precise conditions to be fulfilled in order to obtain access to relevant premises or documents and on judicial redress. Specific expertise required for such advisory missions could, where relevant, be requested through the Emergency Response Coordination Centre established by Decision No 1313/2013/EU of the European Parliament and of the Council ([22]).

(37) In order to support the Commission and facilitate cooperation among Member States and the exchange of information, including best practices, on issues relating to this Directive, a Critical Entities Resilience Group should be established as a Commission expert group. Member States should endeavour to ensure that the designated representatives of their competent authorities in the Critical Entities Resilience Group effectively and efficiently cooperate, including by designating representatives who hold security clearance, where appropriate. The Critical Entities Resilience Group should begin to perform its tasks as soon as possible, so as to provide additional means for appropriate cooperation during the transposition period of this Directive. The Critical Entities Resilience Group should interact with other relevant sector-specific expert working groups.

(38) The Critical Entities Resilience Group should cooperate with the Cooperation Group established under Directive (EU) 2022/2555 with a view to supporting a comprehensive framework for cyber and non-cyber resilience of critical entities. The Critical Entities Resilience Group and the Cooperation Group established under Directive (EU) 2022/2555 should engage in a regular dialogue to promote cooperation between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 and to facilitate the exchange of information, in particular on topics of relevance to both groups.

(39) In order to achieve the objectives of this Directive and without prejudice to the legal responsibility of Member States and critical entities to ensure compliance with their respective obligations laid down therein, the Commission should, where it considers it appropriate, support competent authorities and critical entities with the aim of facilitating their compliance with their respective obligations. When providing support to Member States and critical entities in the implementation of obligations under this Directive, the Commission should build on existing structures and tools, such as those under the Union Civil Protection Mechanism, established by Decision No 1313/2013/EU, and the European Reference Network for Critical Infrastructure Protection. In addition, it should inform Member States about resources available at Union level, such as within the Internal Security Fund, established by Regulation (EU) 2021/1149 of the European Parliament and of the Council ([23]), Horizon Europe, established by Regulation (EU) 2021/695 of the European Parliament and of the Council ([24]), or other instruments relevant for the resilience of critical entities.

(40) Member States should ensure that their competent authorities have certain specific powers for the proper application and enforcement of this Directive in relation to critical entities, where those entities fall under their jurisdiction as specified in this Directive. Those powers should include, in particular, the power to conduct inspections and audits, the power to supervise, the power to require critical entities to provide information and evidence relating to the measures they have taken to comply with their obligations and, where necessary, the power to issue orders to remedy identified infringements. When issuing such orders, Member States should not require measures which go beyond what is necessary and proportionate to ensure the compliance of the critical entity concerned, taking account of, in particular, the seriousness of the infringement and the economic capacity of the critical entity concerned. More generally, those powers should be accompanied by appropriate and effective safeguards to be specified in national law in accordance with the Charter of Fundamental Rights of the European

([22]) Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

([23]) Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

([24]) Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

Union. When assessing the compliance of a critical entity with its obligations as laid down in this Directive, the competent authorities under this Directive should be able to request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. The competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2555 should cooperate and exchange information for that purpose.

(41) In order to apply this Directive in an effective and consistent manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to supplement this Directive by drawing up a list of essential services. That list should be used by competent authorities for the purpose of conducting Member State risk assessments and identifying critical entities pursuant to this Directive. In light of the minimum harmonisation approach of this Directive, that list is non-exhaustive, and Member States could complement it with additional essential services at national level in order to take into account national specificities in the provision of essential services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([25]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(42) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([26]).

(43) Since the objectives of this Directive, namely to ensure that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market and to enhance the resilience of critical entities providing such services, cannot be sufficiently achieved by the Member States, but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union. In accordance with the principle of proportionality as set out in that Article 5, this Directive does not go beyond what is necessary in order to achieve those objectives.

(44) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([27]) and delivered an opinion on 11 August 2021.

(45) Directive 2008/114/EC should therefore be repealed,

([25]) OJ L 123, 12.5.2016, p. 1.

([26]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

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

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive:

(a) lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities within the scope of Article 114 TFEU are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them;

(b) lays down obligations for critical entities aimed at enhancing their resilience and ability to provide services as referred to in point (a) in the internal market;

(c) establishes rules:

(i) on the supervision of critical entities;

(ii) on enforcement;

(iii) for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have put in place to meet their obligations under Chapter III;

(d) establishes common procedures for cooperation and reporting on the application of this Directive;

(e) lays down measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market.

2. This Directive shall not apply to matters covered by Directive (EU) 2022/2555, without prejudice to Article 8 of this Directive. In light of the relationship between the physical security and cybersecurity of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner.

3. Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience and where those requirements are recognised by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply.

4. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and the security and commercial interests of critical entities, while respecting the security of Member States.

5. This Directive is without prejudice to the Member States' responsibility for safeguarding national security and defence and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

6. This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences.

7. Member States may decide that Article 11 and Chapters III, IV and VI, in whole or in part, do not apply to specific critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 6 of this Article.

8. The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

9. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council ([28]) and Directive 2002/58/EC of the European Parliament and of the Council ([29]).

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'critical entity' means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex;

(2) 'resilience' means a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident;

(3) 'incident' means an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law;

(4) 'critical infrastructure' means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service;

(5) 'essential service' means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment;

(6) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

(7) 'risk assessment ' means the overall process for determining the nature and extent of a risk by identifying and analysing potential relevant threats, vulnerabilities and hazards which could lead to an incident and by evaluating the potential loss or disruption of the provision of an essential service caused by that incident;

(8) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([30]);

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

([29]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

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

(9) 'technical specification' means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

(10) 'public administration entity' means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State authorities or by other central-level bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State authorities or by other central-level bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

Article 3

Minimum harmonisation

This Directive shall not preclude Member States from adopting or maintaining provisions of national law with a view to achieving a higher level of resilience of critical entities, provided that such provisions are consistent with Member States' obligations laid down in Union law.

CHAPTER II

NATIONAL FRAMEWORKS ON THE RESILIENCE OF CRITICAL ENTITIES

Article 4

Strategy on the resilience of critical entities

1. Following a consultation that is, to the extent practically possible, open to relevant stakeholders, each Member State shall adopt by 17 January 2026 a strategy for enhancing the resilience of critical entities (the 'strategy'). The strategy shall set out strategic objectives and policy measures, building upon relevant existing national and sectoral strategies, plans or similar documents, with a view to achieving and maintaining a high level of resilience on the part of critical entities and covering at least the sectors set out in the Annex.

2. Each strategy shall contain at least the following elements:

(a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities, taking into account cross-border and cross-sectoral dependencies and interdependencies;

(b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties involved in the implementation of the strategy;

(c) a description of measures necessary to enhance the overall resilience of critical entities, including a description of the risk assessment referred to in Article 5;

(d) a description of the process by which critical entities are identified;

(e) a description of the process supporting critical entities in accordance with this Chapter, including measures to enhance cooperation between the public sector, on the one hand, and the private sector and public and private entities, on the other hand;

(f) a list of the main authorities and relevant stakeholders, other than critical entities, involved in the implementation of the strategy;

(g) a policy framework for coordination between the competent authorities under this Directive ('competent authorities') and the competent authorities under Directive (EU) 2022/2555 for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks;

(h) a description of measures already in place which aim to facilitate the implementation of obligations under Chapter III of this Directive by small and medium-sized enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC ([31]) that the Member State in question has identified as critical entities.

Following a consultation that is, to the extent practically possible, open to relevant stakeholders, Member States shall update their strategies at least every four years.

3. Member States shall communicate their strategies, and substantial updates thereto, to the Commission within three months of their adoption.

Article 5

Risk assessment by Member States

1. The Commission is empowered to adopt a delegated act, in accordance with Article 23, by 17 November 2023 to supplement this Directive by establishing a non-exhaustive list of essential services in the sectors and subsectors set out in the Annex. The competent authorities shall use that list of essential services for the purpose of carrying out a risk assessment ('Member State risk assessment') by 17 January 2026, whenever necessary subsequently, and at least every four years. The competent authorities shall use Member State risk assessments for the purpose of identifying critical entities in accordance with Article 6 and assisting those critical entities to take measures pursuant to Article 13.

Member State risk assessments shall account for the relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541 of the European Parliament and of the Council ([32]).

2. In carrying out Member State risk assessments, Member States shall take into account at least the following:

(a) the general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU;

(b) other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific Union legal acts, including Regulations (EU) 2017/1938 ([33]) and (EU) 2019/941 ([34]) of the European Parliament and of the Council and Directives 2007/60/EC ([35]) and 2012/18/EU ([36]) of the European Parliament and of the Council;

([31]) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).
([32]) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).
([33]) Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (OJ L 280, 28.10.2017, p. 1).
([34]) Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).
([35]) Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks (OJ L 288, 6.11.2007, p. 27).
([36]) Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC (OJ L 197, 24.7.2012, p. 1).

(c) the relevant risks arising from the extent to which the sectors set out in the Annex depend on one another, including from the extent to which they depend on entities located within other Member States and third countries, and the impact that a significant disruption in one sector may have on other sectors, including any significant risks to citizens and the internal market;

(d) any information on incidents notified in accordance with Article 15.

For the purposes of the first subparagraph, point (c), Member States shall cooperate with the competent authorities of other Member States and the competent authorities of third countries, as appropriate.

3. Member States shall make the relevant elements of Member State risk assessments available, where relevant through their single points of contact, to the critical entities that they have identified in accordance with Article 6. Member States shall ensure that the information provided to critical entities assists them in carrying out their risk assessments pursuant to Article 12 and in taking measures to ensure their resilience pursuant to Article 13.

4. Within three months of carrying out a Member State risk assessment, a Member State shall provide the Commission with relevant information on the types of risks identified following, and the outcomes of, that Member State risk assessment, per sector and subsector set out in the Annex.

5. The Commission shall, in cooperation with the Member States, develop a voluntary common reporting template for the purpose of complying with paragraph 4.

Article 6

Identification of critical entities

1. By 17 July 2026, each Member State shall identify the critical entities for the sectors and subsectors set out in the Annex.

2. When a Member State identifies critical entities pursuant to paragraph 1, it shall take into account the outcomes of its Member State risk assessment and its strategy and shall apply all of the following criteria:

(a) the entity provides one or more essential services;

(b) the entity operates, and its critical infrastructure is located, on the territory of that Member State; and

(c) an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services.

3. Each Member State shall establish a list of the critical entities identified pursuant to paragraph 2 and ensure that those critical entities are notified that they have been identified as critical entities within one month of that identification. Member States shall inform those critical entities of their obligations under Chapters III and IV and the date from which those obligations apply to them, without prejudice to Article 8. Member States shall inform critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex that they have no obligations under Chapters III and IV, unless national measures provide otherwise.

For the critical entities concerned, Chapter III shall apply from 10 months after the date of the notification referred to in the first subparagraph of this paragraph.

4. Member States shall ensure that their competent authorities under this Directive notify the competent authorities under Directive (EU) 2022/2555 of the identity of the critical entities that they have identified under this Article within one month of that identification. That notification shall specify, where applicable, that the critical entities concerned are entities in the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive and have no obligations under Chapters III and IV thereof.

5. Member States shall, where necessary and in any event at least every four years, review and, where appropriate, update the list of identified critical entities referred to in paragraph 3. Where those updates lead to the identification of additional critical entities, paragraphs 3 and 4 shall apply to those additional critical entities. In addition, Member States shall ensure that entities that are no longer identified as critical entities following any such update are notified in due time of that fact and the fact that they are no longer subject to the obligations under Chapter III from the date of receipt of that notification.

6. The Commission shall, in cooperation with the Member States, develop recommendations and non-binding guidelines to support Member States in identifying critical entities.

Article 7

Significant disruptive effect

1. When determining the significance of a disruptive effect as referred to in Article 6(2), point (c), Member States shall take into account the following criteria:

(a) the number of users relying on the essential service provided by the entity concerned;

(b) the extent to which other sectors and subsectors as set out in the Annex depend on the essential service in question;

(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population;

(d) the entity's market share in the market for the essential service or essential services concerned;

(e) the geographic area that could be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas;

(f) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service.

2. After the identification of the critical entities under Article 6(1), each Member State shall submit the following information to the Commission without undue delay:

(a) a list of essential services in that Member State where there are any additional essential services as compared to the list of essential services referred to in Article 5(1);

(b) the number of critical entities identified for each sector and subsector set out in the Annex and for each essential service;

(c) any thresholds applied to specify one or more of the criteria in paragraph 1.

Thresholds as referred to in the first subparagraph, point (c), may be presented as such or in aggregated form.

Member States shall subsequently submit information referred to in the first subparagraph whenever necessary and at least every four years.

3. The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to facilitate the application of the criteria referred to in paragraph 1 of this Article, taking into account the information referred to in paragraph 2 of this Article.

Article 8

Critical entities in the banking, financial market infrastructure and digital infrastructure sectors

Member States shall ensure that Article 11 and Chapters III, IV and VI do not apply to critical entities that they have identified in the sectors set out in points 3, 4 and 8 of the table in the Annex. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

Article 9

Competent authorities and single point of contact

1. Each Member State shall designate or establish one or more competent authorities responsible for the correct application and, where necessary, enforcement of the rules set out in this Directive at national level.

As regards the critical entities in the sectors set out in points 3 and 4 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities referred to in Article 46 of Regulation (EU) 2022/2554. As regards the critical entities in the sector set out in point 8 of the table in the Annex to this Directive, the competent authorities shall, in principle, be the competent authorities under Directive (EU) 2022/2555. Member States may designate a different competent authority for the sectors set out in points 3, 4 and 8 of the table in the Annex to this Directive in accordance with existing national frameworks.

Where Member States designate or establish more than one competent authority, they shall clearly set out the tasks of each of the authorities concerned and ensure that they cooperate effectively to fulfil their tasks under this Directive, including with regard to the designation and activities of the single point of contact referred to in paragraph 2.

2. Each Member State shall designate or establish one single point of contact to exercise a liaison function for the purpose of ensuring cross-border cooperation with the single points of contact of other Member States and the Critical Entities Resilience Group referred to in Article 19 ('single point of contact'). Where relevant, a Member State shall designate its single point of contact within a competent authority. Where relevant, a Member State may provide that its single point of contact also exercise a liaison function with the Commission and ensure cooperation with third countries.

3. By 17 July 2028, and every two years thereafter, the single points of contact shall submit a summary report to the Commission and to the Critical Entities Resilience Group referred to in Article 19 on the notifications they have received, including the number of notifications, the nature of notified incidents and the actions taken in accordance with Article 15(3).

The Commission shall, in cooperation with the Critical Entities Resilience Group, develop a common reporting template. The competent authorities may use, on a voluntary basis, that common reporting template for the purpose of submitting summary reports as referred to in the first subparagraph.

4. Each Member State shall ensure that its competent authority and single point of contact have the powers and the adequate financial, human and technical resources to carry out, in an effective and efficient manner, the tasks assigned to them.

5. Each Member State shall ensure that its competent authority, whenever appropriate, and in accordance with Union and national law, consults and cooperates with other relevant national authorities, including those in charge of civil protection, law enforcement and the protection of personal data, and with critical entities and relevant interested parties.

6. Each Member State shall ensure that its competent authority under this Directive cooperates and exchanges information with competent authorities under Directive (EU) 2022/2555 on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents affecting critical entities, including with regard to relevant measures its competent authority and competent authorities under Directive (EU) 2022/2555 have taken.

7. Within three months of the designation or establishment of the competent authority and the single point of contact, each Member State shall notify the Commission of their identity and their tasks and responsibilities under this Directive, their contact details and any subsequent change thereto. Member States shall inform the Commission where they decide to designate an authority other than the competent authorities referred to in paragraph 1, second subparagraph, as the competent authorities in respect of the critical entities in the sectors set out in points 3, 4 and 8 of the table in the Annex. Each Member State shall make public the identity of its competent authority and single point of contact.

8. The Commission shall make a list of the single points of contact publicly available.

Article 10

Member States' support to critical entities

1. Member States shall support critical entities in enhancing their resilience. That support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their resilience and providing advice and training to the personnel of critical entities. Without prejudice to applicable rules on State aid, Member States may provide financial resources to critical entities, where necessary and justified by public interest objectives.

2. Each Member State shall ensure that its competent authority cooperates and exchanges information and good practices with critical entities of the sectors set out in the Annex.

3. Member States shall facilitate voluntary information sharing between critical entities in relation to matters covered by this Directive, in accordance with Union and national law on, in particular, classified and sensitive information, competition and protection of personal data.

Article 11

Cooperation between Member States

1. Whenever appropriate, Member States shall consult one another regarding critical entities for the purpose of ensuring that this Directive is applied in a consistent manner. Such consultations shall take place, in particular, regarding critical entities that:

(a) use critical infrastructure which is physically connected between two or more Member States;

(b) are part of corporate structures that are connected with, or linked to, critical entities in other Member States;

(c) have been identified as critical entities in one Member State and provide essential services to or in other Member States.

2. The consultations referred to in paragraph 1 shall aim at enhancing the resilience of critical entities and, where possible, reducing the administrative burden on them.

CHAPTER III

RESILIENCE OF CRITICAL ENTITIES

Article 12

Risk assessment by critical entities

1. Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment').

2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

Where a critical entity has carried out other risk assessments or drawn up documents pursuant to obligations laid down in other legal acts that are relevant for its critical entity risk assessment, it may use those assessments and documents to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority may declare an existing risk assessment carried out by a critical entity that addresses the risks and extent of dependence referred to in the first subparagraph of this paragraph as compliant, in whole or in part, with the obligations under this Article.

Article 13

Resilience measures of critical entities

1. Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

(c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

(d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;

(e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;

(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.

For the purposes of the first subparagraph, point (e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

2. Member States shall ensure that critical entities have in place and apply a resilience plan or equivalent document or documents which describe the measures taken pursuant to paragraph 1. Where critical entities have drawn up documents or taken measures pursuant to obligations laid down in other legal acts that are relevant for the measures referred to in paragraph 1, they may use those documents and measures to meet the requirements set out in this Article. When exercising its supervisory functions, the competent authority may declare existing resilience-enhancing measures taken by a critical entity that address, in an appropriate and proportionate manner, the technical, security and organisational measures referred to in paragraph 1 as compliant, in whole or in part, with the obligations under this Article.

3. Member States shall ensure that each critical entity designates a liaison officer or equivalent as the point of contact with the competent authorities.

4. At the request of the Member State that has identified the critical entity and with the agreement of the critical entity concerned, the Commission shall organise advisory missions, in accordance with the arrangements set out in Article 18(6), (8) and (9), to provide advice to the critical entity concerned in meeting its obligations under Chapter III. The advisory mission shall report its findings to the Commission, that Member State and the critical entity concerned.

5. The Commission shall, after consulting the Critical Entities Resilience Group referred to in Article 19, adopt non-binding guidelines to further specify the technical, security and organisational measures that may be taken pursuant to paragraph 1 of this Article.

6. The Commission shall adopt implementing acts in order to set out the necessary technical and methodological specifications relating to the application of the measures referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

Article 14

Background checks

1. Member States shall specify the conditions under which a critical entity is permitted, in duly reasoned cases and taking into account the Member State risk assessment, to submit requests for background checks on persons who:

(a) hold sensitive roles in or for the benefit of the critical entity, in particular in relation to the resilience of the critical entity;

(b) are authorised to directly or remotely access its premises, information or control systems, including in connection with the security of the critical entity;

(c) are under consideration for recruitment to positions that fall under the criteria set out in point (a) or (b).

2. Requests as referred to in paragraph 1 of this Article shall be assessed within a reasonable timeframe and processed in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council ([37]). Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the critical entity concerned.

3. A background check as referred to in paragraph 1 shall, at least:

(a) corroborate the identity of the person who is the subject of the background check;

(b) check the criminal records of that person with regards to offences which would be relevant for a specific position.

When carrying out background checks, Member States shall use the European Criminal Records Information System in accordance with the procedures set out in Framework Decision 2009/315/JHA and, where relevant and applicable, Regulation (EU) 2019/816 for the purpose of obtaining information from criminal records held by other Member States. The central authorities referred to in Article 3(1) of Framework Decision 2009/315/JHA and in Article 3, point (5), of Regulation (EU) 2019/816 shall provide replies to requests for such information within 10 working days from the date on which the request was received in accordance with Article 8(1) of Framework Decision 2009/315/JHA.

([37]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

Article 15

Incident notification

1. Member States shall ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Member States shall ensure that, unless operationally unable to do so, critical entities submit an initial notification no later than 24 hours after becoming aware of an incident, followed, where relevant, by a detailed report no later than one month thereafter. In order to determine the significance of a disruption, the following parameters shall, in particular, be taken into account:

(a) the number and proportion of users affected by the disruption;

(b) the duration of the disruption;

(c) the geographical area affected by the disruption, taking into account whether the area is geographically isolated.

Where an incident has or might have a significant impact on the continuity of the provision of essential services to or in six or more Member States, the competent authorities of the Member States affected by the incident shall notify the Commission of that incident.

2. Notifications as referred to in paragraph 1, first subparagraph, shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including any available information necessary to determine any cross-border impact of the incident. Such notifications shall not subject critical entities to increased liability.

3. On the basis of the information provided by a critical entity in a notification as referred to in paragraph 1, the relevant competent authority, via the single point of contact, shall inform the single point of contact of other affected Member States where the incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States.

Single points of contact sending and receiving information pursuant to the first subparagraph shall, in accordance with Union or national law, treat that information in a way that respects its confidentiality and protects the security and commercial interest of the critical entity concerned.

4. As soon as possible following a notification as referred to in paragraph 1, the competent authority concerned shall provide the critical entity concerned with relevant follow-up information, including information that could support that critical entity's effective response to the incident in question. Member States shall inform the public where they determine that it would be in the public interest to do so.

Article 16

Standards

In order to promote the convergent implementation of this Directive, Member States shall, where useful and without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.

CHAPTER IV

CRITICAL ENTITIES OF PARTICULAR EUROPEAN SIGNIFICANCE

Article 17

Identification of critical entities of particular European significance

1. An entity shall be considered a critical entity of particular European significance where it:

(a) has been identified as a critical entity pursuant to Article 6(1);

(b) provides the same or similar essential services to or in six or more Member States; and

(c) has been notified pursuant to paragraph 3 of this Article.

2. Member States shall ensure that a critical entity, following the notification referred to in Article 6(3), informs its competent authority where it provides essential services to or in six or more Member States. In such a case, Member States shall ensure that the critical entity informs its competent authority of the essential services it provides to or in those Member States and of the Member States to which or in which it provides such essential services. Member States shall notify the Commission, without undue delay, of the identity of such critical entities and of the information they provide under this paragraph.

The Commission shall consult the competent authority of the Member State which identified a critical entity as referred to in the first subparagraph, the competent authority of other Member States concerned and the critical entity in question. During those consultations, each Member State shall inform the Commission where it deems that the services provided to that Member State by the critical entity are essential services.

3. Where the Commission establishes, on the basis of the consultations referred to in paragraph 2 of this Article, that the critical entity concerned provides essential services to or in six or more Member States, the Commission shall notify that critical entity, through its competent authority, that it is considered a critical entity of particular European significance and inform that critical entity of its obligations under this Chapter and the date from which those obligations apply to it. Once the Commission informs the competent authority of its decision to consider a critical entity as a critical entity of particular European significance, the competent authority shall forward that notification to that critical entity without undue delay.

4. This Chapter shall apply to the critical entity of particular European significance concerned from the date of receipt of the notification referred to in paragraph 3 of this Article.

Article 18

Advisory missions

1. At the request of the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), the Commission shall organise an advisory mission to assess the measures that that critical entity has put in place to meet its obligations under Chapter III.

2. On its own initiative or at the request of one or more Member States to or in which the essential service is provided, and provided that the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) so agrees, the Commission shall organise an advisory mission as referred to in paragraph 1 of this Article.

3. On a reasoned request from the Commission or from one or more Member States to or in which the essential service is provided, the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall provide the following to the Commission:

(a) the relevant parts of the critical entity risk assessment;

(b) a list of relevant measures taken in accordance with Article 13;

(c) supervisory or enforcement actions, including assessments of compliance or orders issued, that its competent authority has undertaken pursuant to Articles 21 and 22 in respect of that critical entity.

4. The advisory mission shall report its findings to the Commission, to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to the critical entity concerned within three months of the conclusion of the advisory mission.

The Member States to or in which the essential service is provided shall analyse the report referred to in the first subparagraph and, where necessary, shall advise the Commission as to whether the critical entity of particular European significance concerned complies with its obligations under Chapter III and, where appropriate, as to the measures which could be taken to improve the resilience of that critical entity.

The Commission shall, based on the advice referred to in the second subparagraph of this paragraph, communicate its opinion to the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), to the Member States to or in which the essential service is provided and to that critical entity as to whether that critical entity complies with its obligations under Chapter III and, where appropriate, as to the measures which could be taken to improve the resilience of that critical entity.

The Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1) shall ensure that its competent authority and the critical entity concerned take into account the opinion referred to in the third subparagraph of this paragraph and provide information to the Commission and the Member States to or in which the essential service is provided on the measures it has taken pursuant to that opinion.

5. Each advisory mission shall consist of experts from the Member State in which the critical entity of particular European significance is located, experts from the Member States to or in which the essential service is provided, and Commission representatives. Those Member States may propose candidates to be part of an advisory mission. The Commission shall, following a consultation with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1), select and appoint the members of each advisory mission in accordance with their professional capacity and ensuring, where possible, a geographically balanced representation from all those Member States. Whenever necessary, members of the advisory mission shall have valid and appropriate security clearance. The Commission shall bear the costs related to participation in advisory missions.

The Commission shall organise the programme of each advisory mission, in consultation with the members of the advisory mission in question and in agreement with the Member State that has identified a critical entity of particular European significance as a critical entity pursuant to Article 6(1).

6. The Commission shall adopt an implementing act laying down rules on the procedural arrangements for requests to organise advisory missions, for handling such requests, for the conduct and reports of advisory missions and for handling the communication of the Commission's opinion referred to in paragraph 4, third subparagraph, of this Article and of the measures taken, duly taking into account the confidentiality and commercial sensitivity of the information concerned. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. Member States shall ensure that critical entities of particular European significance provide advisory missions with access to information, systems and facilities relating to the provision of their essential services necessary for carrying out the advisory mission concerned.

8. Advisory missions shall be carried out in compliance with the applicable national law of the Member State in which they take place, with respect for that Member State's responsibility for national security and the protection of its security interests.

9. When organising advisory missions, the Commission shall take into account the reports of any inspections carried out by the Commission under Regulations (EC) No 725/2004 and (EC) No 300/2008 and the reports of any monitoring carried out by the Commission under Directive 2005/65/EC in respect of the critical entity concerned.

10. The Commission shall inform the Critical Entities Resilience Group referred to in Article 19 whenever an advisory mission is organised. The Member State in which the advisory mission took place and the Commission shall also inform the Critical Entities Resilience Group of the main findings of the advisory mission and the lessons learned with a view to promoting mutual learning.

CHAPTER V

COOPERATION AND REPORTING

Article 19

Critical Entities Resilience Group

1. A Critical Entities Resilience Group is hereby established. The Critical Entities Resilience Group shall support the Commission and facilitate cooperation among Member States and the exchange of information on issues relating to this Directive.

2. The Critical Entities Resilience Group shall be composed of representatives of the Member States and the Commission who hold security clearance, where appropriate. Where relevant for the performance of its tasks, the Critical Entities Resilience Group may invite relevant stakeholders to participate in its work. Where requested by the European Parliament, the Commission may invite experts from the European Parliament to attend meetings of the Critical Entities Resilience Group.

The Commission's representative shall chair the Critical Entities Resilience Group.

3. The Critical Entities Resilience Group shall have the following tasks:

(a) supporting the Commission in assisting Member States in reinforcing their capacity to contribute to ensuring the resilience of critical entities in accordance with this Directive;

(b) analysing the strategies in order to identify best practices in respect of the strategies;

(c) facilitating the exchange of best practices with regard to the identification of critical entities by the Member States pursuant to Article 6(1), including in relation to cross-border and cross-sectoral dependencies and regarding risks and incidents;

(d) where appropriate, contributing on issues relating to this Directive to documents concerning resilience at Union level;

(e) contributing to the preparation of the guidelines referred to in Article 7(3) and Article 13(5) and, upon request, any delegated or implementing acts adopted pursuant to this Directive;

(f) analysing the summary reports referred to in Article 9(3) with a view to promoting the sharing of best practices on the action taken in accordance with Article 15(3);

(g) exchanging best practices related to the notification of incidents referred to in Article 15;

(h) discussing the summary reports of advisory missions and the lessons learned in accordance with Article 18(10);

(i) exchanging information and best practices on innovation, research and development relating to the resilience of critical entities in accordance with this Directive;

(j) where relevant, exchanging information on matters concerning the resilience of critical entities with relevant Union institutions, bodies, offices and agencies.

4. By 17 January 2025 and every two years thereafter, the Critical Entities Resilience Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. That work programme shall be consistent with the requirements and objectives of this Directive.

5. The Critical Entities Resilience Group shall meet on a regular basis and in any event at least once a year with the Cooperation Group established under Directive (EU) 2022/2555 to promote and facilitate cooperation and the exchange of information.

6. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Critical Entities Resilience Group, respecting Article 1(4). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).

7. The Commission shall provide the Critical Entities Resilience Group with a summary report of the information provided by the Member States pursuant to Article 4(3) and Article 5(4) by 17 January 2027, whenever necessary subsequently, and at least every four years.

Article 20

Commission support to competent authorities and critical entities

1. The Commission shall, where appropriate, support Member States and critical entities in complying with their obligations under this Directive. The Commission shall prepare a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, organise advisory missions as referred to in Article 13(4) and Article 18 and facilitate information exchange among Member States and experts across the Union.

2. The Commission shall complement Member States' activities as referred to in Article 10 by developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test the resilience of critical entities.

3. The Commission shall inform Member States about financial resources at Union level available to Member States for enhancing the resilience of critical entities.

CHAPTER VI

SUPERVISION AND ENFORCEMENT

Article 21

Supervision and enforcement

1. In order to assess the compliance of the entities identified by Member States as critical entities pursuant to Article 6(1) with the obligations laid down in this Directive, Member States shall ensure that the competent authorities have the powers and means to:

(a) conduct on-site inspections of the critical infrastructure and the premises that the critical entity uses to provide its essential services, and off-site supervision of measures taken by critical entities in accordance with Article 13;

(b) conduct or order audits in respect of critical entities.

2. Member States shall ensure that the competent authorities have the powers and means to require, where necessary for the performance of their tasks under this Directive, that the entities under Directive (EU) 2022/2555 that Member States have identified as critical entities under this Directive provide, within a reasonable time limit set by those authorities:

(a) the information necessary to assess whether the measures taken by those entities to ensure their resilience meet the requirements set out in Article 13;

(b) evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified auditor selected by that entity and conducted at its expense.

When requiring that information, the competent authorities shall state the purpose of the requirement and specify the information required.

3. Without prejudice to the possibility to impose penalties in accordance with Article 22, the competent authorities may, following the supervisory actions referred to in paragraph 1 of this Article or the assessment of the information referred to in paragraph 2 of this Article, order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement of this Directive, within a reasonable time limit set by those authorities, and to provide those authorities with information on the measures taken. Those orders shall take into account, in particular, the seriousness of the infringement.

4. Member State shall ensure that the powers provided for in paragraphs 1, 2 and 3 can only be exercised subject to appropriate safeguards. Those safeguards shall guarantee, in particular, that such exercise takes place in an objective, transparent and proportionate manner, and that the rights and legitimate interests of the critical entities affected, such as the protection of trade and business secrets, are duly safeguarded, including the right to be heard, the right of defence and the right to an effective remedy before an independent court.

5. Member States shall ensure that, where a competent authority under this Directive assesses the compliance of a critical entity pursuant to this Article, that competent authority informs the competent authorities of the Member States concerned under Directive (EU) 2022/2555. For that purpose, Member States shall ensure that competent authorities under this Directive can request the competent authorities under Directive (EU) 2022/2555 to exercise their supervisory and enforcement powers in relation to an entity under that Directive that has been identified as a critical entity under this Directive. For that purpose, Member States shall ensure that competent authorities under this Directive cooperate and exchange information with the competent authorities under Directive (EU) 2022/2555.

Article 22

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 October 2024, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

CHAPTER VII

DELEGATED AND IMPLEMENTING ACTS

Article 23

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 Article 5(1) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. The delegation of power referred to in Article 5(1) 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 Article 5(1) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two 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 two months at the initiative of the European Parliament or of the Council.

Article 24

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VIII

FINAL PROVISIONS

Article 25

Reporting and review

By 17 July 2027, the Commission shall submit to the European Parliament and to the Council a report assessing the extent to which each Member State has taken the necessary measures to comply with this Directive.

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. That report shall, in particular, assess the added value of this Directive, its impact on ensuring the resilience of critical entities and whether the Annex to this Directive should be modified. The Commission shall submit the first such report by 17 June 2029. For the purpose of reporting under this Article, the Commission shall take into account relevant documents of the Critical Entities Resilience Group.

Article 26

Transposition

1. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 18 October 2024.

2. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 27

Repeal of Directive 2008/114/EC

Directive 2008/114/EC is repealed with effect from 18 October 2024.

References to the repealed Directive shall be construed as references to this Directive.

Article 28

Entry into force

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

Article 29

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

ANNEX

SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES

Sectors	Subsectors	Categories of entities
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2])
		— Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])

Sectors	Subsectors	Categories of entities
	(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council ([5])
		— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC
		— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])

Sectors	Subsectors	Categories of entities
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU and operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004, not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC, including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([10])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 ([11]) responsible for traffic management control, excluding public entities for whom traffic-management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([12])
	(e) public transport	— Public service operators as defined in Article 2, point (d), of Regulation (EC) No 1370/2007 of the European Parliament and of the Council ([13])
3. Banking		— Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013
4. Financial market infrastructure		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU
		— Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012

Sectors	Subsectors	Categories of entities
5. Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([14])
		— EU reference laboratories as referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([15])
		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([16])
		— Entities manufacturing basic pharmaceutical products and pharmaceutical preparations as referred to in Section C division 21 of NACE Rev. 2
		— Entities manufacturing medical devices considered as critical during a public health emergency ('public health emergency critical devices list') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([17])
		— Entities holding a distribution authorisation as referred to in Article 79 of Directive 2001/83/EC
6. Drinking water		— Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([18]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		— Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([19]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity

Sectors	Subsectors	Categories of entities
8. Digital infrastructure		— Providers of internet exchange points as defined in Article 6, point (18), of Directive (EU) 2022/2555
		— DNS service providers as defined in Article 6, point (20), of Directive (EU) 2022/2555, excluding operators of root name servers
		— top-level-domain name registries as defined in Article 6, point (21), of Directive (EU) 2022/2555
		— Providers of cloud computing services as defined in Article 6, point (30), of Directive (EU) 2022/2555
		— Providers of data centre services as defined in Article 6, point (31), of Directive (EU) 2022/2555
		— Providers of content delivery networks as defined in Article 6, point (32), of Directive (EU) 2022/2555
		— Trust service providers as defined in Article 3, point (19), of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([20])
		— Providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972 of the European Parliament and of the Council ([21])
		— Providers of electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972 insofar as their services are publicly available
9. Public administration		— Public administration entities of central governments as defined by Member States in accordance with national law
10. Space		— Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks as defined in Article 2, point (8), of Directive (EU) 2018/1972

Sectors	Subsectors	Categories of entities
11. Production, processing and distribution of food		— Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council ([22]) which are engaged exclusively in logistics and wholesale distribution and large scale industrial production and processing

([1]) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).
([2]) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
([3]) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).
([4]) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).
([5]) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).
([6]) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).
([7]) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).
([8]) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).
([9]) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).
([10]) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
([11]) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).
([12]) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).
([13]) Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70 (OJ L 315, 3.12.2007, p. 1).
([14]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).
([15]) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).
([16]) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).
([17]) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).
([18]) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).
([19]) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).
([20]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).
([21]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).
([22]) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)

Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN