European Parliament
2019-2024

Committee on Economic and Monetary Affairs

24.6.2022

PROVISIONAL AGREEMENT RESULTING FROM INTERINSTITUTIONAL NEGOTIATIONS

Subject: **Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014**
(COM2020(0595) – C9-0304/2020 – 2020/0266(COD))

The interinstitutional negotiations on the aforementioned proposal for a regulation have led to a compromise. In accordance with Rule 74(4) of the Rules of Procedure, the provisional agreement, reproduced below, is submitted as a whole to the Committee on Economic and Monetary Affairs for decision by way of a single vote.

REGULATION (EU)…/…
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on
digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

(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,

Whereas:

[1] [add reference] OJ C , , p. .
[2] [add reference] OJ C , , p. .

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks 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 nowadays core features of all activities of Union financial entities, digital resilience has yet to be sufficiently built in their operational frameworks.

(2) The use of ICT has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance intermediaries offering their services online operating with InsurTech, to digital insurance underwriting. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.

(3) The European Systemic Risk Board (ESRB) has reaffirmed in a 2020 report addressing systemic cyber risk[3] how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities[4] to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches occurring in finance 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, generating liquidity runs and an overall loss of confidence and trust in financial markets.

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

---

[3] ESRB report Systemic Cyber Risk from February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[4] According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are around 5,665 credit institutions, 5,934 investment firms, 2,666 insurance undertakings, 1,573 IORPS, 2,500 investment management companies, 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs), 45 CRAs and 2,500 authorised payment institutions and electronic money institutions. This sums up to approx. 21.233 entities and does not include crowd funding entities, statutory auditors and audit firms, crypto assets service providers and benchmark administrators.

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

(6) The Commission's 2018 Fintech action plan[5] highlighted the paramount importance of making the Union financial sector more resilient also from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling financial services to be effectively and smoothly delivered 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, the European Supervisory Authority (European Securities and Markets Authority) ('ESMA') established by Regulation (EU) No 1095/2010, and the European Supervisory Authority (European Investment and Occupational Pensions Authority) ('EIOPA') established by Regulation (EU) No 1094/2010 (hereinafter collectively referred to as "European Supervisory Authorities" or "ESAs") jointly issued two pieces of 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 Union sector-specific initiative.

---

5 Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, 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 this component, by strengthening the mandates of competent authorities to supervise the management of ICT risks in the financial sector, and thus to protect the integrity and efficiency of the single market, and to facilitate its orderly functioning.

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

(10) The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to 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, every single one issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risks 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 ICT capabilities and overall resilience which financial entities, based on such key requirements, would develop with a view to withstand operational outages, would help preserving 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 at contributing to the smooth functioning of the single market it should be based on the provisions of Article 114 TFEU as interpreted in accordance with the consistent case law of the Court of Justice of the European Union.

(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements as part of the operational risk requirements addressed so far separately in the different Regulations and Directives. While those Union legal acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they could not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk requirements, when further developed in these Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through requirements aiming at the protection, detection, containment, recovery and repair capabilities against ICT-related incidents or through setting out reporting and digital testing capabilities. Those Directives and Regulations were primarily meant to cover essential rules on prudential supervision, market integrity or conduct.

Through this exercise, which consolidates and updates rules on ICT risk, all provisions addressing digital risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This Regulation should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via targeted rules on ICT risk management capabilities, incident reporting, operational resilience testing and third party risk monitoring. This Regulation also intends to raise awareness of ICT risks and acknowledges that ICT incidents and a lack of operational resilience might jeopardise the financial soundness of financial entities.

(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk according to their size, the nature, scale and complexity of their services, activities and operations, and their overall risk profile. 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. The respect of a basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.

(14) The use of a regulation helps reducing regulatory complexity, fosters supervisory convergence, increases legal certainty, while also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions. The choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities appears therefore the most appropriate way to guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.

(15) Directive (EU) 2016/1148 of the European Parliament and of the Council[6] was the first horizontal cybersecurity framework enacted at Union level. Among the seven critical sectors, that Directive also applied 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 identified by the Member States were in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements laid down in it.

Directive xx (for OPOCE: add reference to NIS2) repealing Directive (EU) 2016/1148 sets a uniform criterion to determine the entities falling within its scope of application (size-cap rule) while also keeping the three types financial entities in its remit.

(16) However, as this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in respect to those laid down in the current Union financial services legislation, this level constitutes an increased harmonisation also by comparison to requirements laid down in Directive (for OPOCE: add reference to NIS2) XX . Consequently, this Regulation constitutes lex specialis to Directive (EU) XX for OPOCE: add reference to NIS2.
In the same time it is crucial to maintain a strong relation between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive XX (for OPOCE: add reference to NIS2) 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 Directive (EU) 2016/1148.

[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).

(16a) In accordance with Article 4(2) of the Treaty on the European Union and without prejudice to the judicial review of the European Court of Justice, this Regulation should not affect the responsibility of Member States regarding 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.

(17) To enable a cross-sector learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (for OPOCE: add reference to NIS2) should remain part of the 'ecosystem' of that Directive (e.g. NIS Cooperation Group and CSIRTs).
The ESAs and national competent authorities, respectively, should be able to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, exchange information and further cooperate with the single points of contact designated under that Directive. The competent authorities under this Regulation should also consult and cooperate with the national CSIRTs designated in accordance with Article 9 of Directive (EU) 2016/1148. The competent authorities may also request technical advice from the authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 and establish cooperation arrangements that should ensure effective and fast-response coordination mechanisms.

(18) Strong interlinkages between the digital resilience and the physical resilience of financial entities call for a coherent approach by this Regulation and the Directive (EU) XXX/XXX of the European Parliament and the Council on the resilience of critical entities [CER Directive[7]]. 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 [CER Directive] should not apply to financial entities in the remit of that Directive.

---

7 Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities [Please insert full reference].

(19) Cloud computing service providers are one category of digital infrastructures covered by Directive (for OPOCE: add reference to NIS2). The Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities and should be considered complementary to the supervision under Directive (add reference to NIS2). Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority.

(20) To remain in full control of ICT risk, financial entities need to have in place comprehensive capabilities enabling a strong and effective ICT risk management, alongside specific mechanisms and policies for handling all ICT-related incidents and reporting major ones. Likewise, financial entities should have policies for the testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. The digital operational resilience baseline of financial entities should be raised while also allowing for a proportionate application of requirements for certain financial entities, particularly those which are 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 duly takes into account both the application the principle of proportionality, as well as the need to reduce administrative burdens for the competent authorities, the relevant national supervisory arrangements in respect to such entities should fully take into account the specific nature, scale, complexity of the services, activities and operations and the overall risk profile of these entities even when exceeding relevant thresholds established in Article 5 of Directive 2016/2341. In particular, supervisory activities could primarily focus on the need to address serious risks associated with the ICT risk management of a particular entity. 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 2016/2341, outsource a significant part of core business, such as asset management, actuarial calculations, accounting and data management, to service providers operating on their behalf, in result of which the proportionate application is considered appropriate.

(21) 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)[8] and the NIS Cooperation Group for the financial entities under Directive(add reference to NIS2) , divergent approaches on thresholds and taxonomies still exist or can emerge for the remainder of financial entities. This diversity entails multiple requirements which financial entities must abide to, especially when operating across several Union jurisdictions and when part of a financial group. Moreover, such divergences may hinder the creation of further Union uniform or centralised mechanisms speeding up the reporting process and supporting a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risks in case of large scale attacks with potentially systemic consequences.

(21a) To reduce the administrative burden and potentially duplicative reporting obligations, for payment service providers that fall within the scope of this regulation, the incident reporting under Directive (EU) 2015/2366 should cease to apply. As such, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of Directive (EU) 2015/2366, should report under this Regulation all operational or security payment-related incidents previously reported under Directive (EU) 2015/2366, irrespective of whether such incidents are ICT-related or not.

(22) 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 relevant requirements would address current gaps in the financial services legislation, 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

[8] ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

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 the [Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)], financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority, when they deem the cyber threat to be of relevance to the financial system, service users or clients.

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

(24) In addition, where no ICT testing is required, vulnerabilities remain undetected thus exposing a financial entity to ICT risk and ultimately creating higher risk to the financial sector's stability and integrity. Without Union intervention, digital operational resilience testing would continue to be inconsistent across jurisdictions and lacking a system of mutual recognition of ICT testing results across different jurisdictions. Also, 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, testing the defence capabilities and the business continuity, which and thus contributes to increase the trust of customers,suppliers and business partners.

To remedy these overlaps, divergences and gaps, it is necessary to lay down rules aiming at coordinated testing regime thus facilitating the mutual recognition of advanced testing for significant financial entities.

(25) Financial entities' reliance on 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 the past 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.

(26) This 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 they are subject to, or otherwise in enforcing specific rights, such as access or audit rights, when the latter are enshrined in the agreements. Moreover, many such contracts do not provide for sufficient safeguards allowing for a fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess these associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors.

(27) Even though the Union financial services legislation contains certain general rules on outsourcing, the monitoring of the contractual dimension is not fully anchored into Union legislation. 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 a particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. These principles should be accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level. These principles are complementary to sectorial legislation applicable to outsourcing.

(28) A certain lack of homogeneity and convergence regarding the monitoring of ICT third party risk and ICT third-party dependencies can be noticed today.
Despite efforts to address outsourcing, such as the 2017 recommendations on outsourcing to cloud service providers,[9] 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 barely addressed by Union legislation.
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 adequately monitor risks arising from concentration of ICT third-party dependencies.

(29) 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 risks occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Union Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities, while ensuring that the confidentiality or security of customers other than financial entities is preserved.
While the intragroup provision of ICT services has its specific risks and benefits, it should not be considered less risky than the provision of ICT services by providers outside of the financial group, and should be thus subject to the same regulatory framework.

However, when ICT services are provided from within the same financial group, financial entities may have a higher level of control over intra-group providers which is duly to be taken into account in the overall risk assessment.

[9] Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), now repealed by the EBA Guidelines on outsourcing (EBA/GL/2019/02) and ESMA Guidelines on outsourcing to cloud service providers (ESMA/50/164/4285)

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

(31) 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. The extent and quality of information sharing remains limited and fragmented, with relevant exchanges being done mostly locally (via 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.

(32) 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 enhance their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements which, when conducted in trusted environments, would help the financial community to prevent and collectively respond to threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels.

Those mechanisms should be conducted in full compliance with the applicable competition law rules of the Union as well as in a way that guarantees the full respect of Union data protection rules, mainly Regulation (EU) 2016/679 of the European Parliament and of the Council, based on one or more of the legal basis 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 point (f) of Article 6(1) 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 points (c) and (e) respectively, of Article 6(1) of that Regulation.

(32a) In order to maintain a high level of digital operational resilience for all the financial sector, and at the same time keep pace with technological developments, this Regulation should address risk stemming from all types of ICT services. To that effect, the definition of ICT services in this Regulation should be defined broadly, encompassing digital and data services provided through the ICT systems to one or more internal or external users, on an ongoing basis. This should include for instance so called 'over the top' services, falling as such into the category of electronic communications services. It should only exclude 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 telephones telephone services.

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

(33a) 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, payment institutions and e-money institutions exempted under Article 32(1) of Directive (EU) 2015/2366 and Article 9(1) of Directive 2009/110/EC, respectively, are included in the scope of this Regulation even if they have not been granted authorisation in accordance with Directive (EU) 2015/2366 to provide and execute payment services or if they have not been granted authorisation under Directive 2009/110/EC to issue electronic money, respectively.
On the contrary, post office giro institutions, referred to in Article 1(1), point (c) of Directive (EU) 2015/2366, are excluded from the scope of this Regulation.
The competent authority for payment institutions exempted under Directive (EU) 2015/2366, electronic money institutions exempted under Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, is the one designated in accordance with Article 22 of Directive (EU) 2015/2366.

(34) As larger financial entities may enjoy wider resources and could 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 an internal risk management and control model, and to submit their ICT risk management framework to internal audits.

(34a) Some financial entities benefit from exemptions or a very light framework under their respective sector specific Union legislation. Such financial entities include managers of alternative investment funds referred to in Article 3 (2) of Directive 2011/61/EU, insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC and institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total.

In light of these 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, small or medium-sized enterprises should not be subject to this Regulation.

(34b) As regard institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU, since they are excluded from the application of that Directive, Member States may consequently also choose to exempt such institutions located within their respective territory from the application of this Regulation.

(34c) In the same vein, in order to align this Regulation to the scope of Directive 2014/65/EU, it is also appropriate to exclude form the scope of this Regulation, natural and legal persons referred in Articles 2 and 3 of Directive 2014/65/EU 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 exempts 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 exemption from the scope of this Regulation of the persons and entities referred in Articles 2 and 3 of Directive 2014/65/EU should not encompass these central securities depositories, collective investment undertakings or insurance and reinsurance undertakings.

(34e) Under sector specific Union legislation some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. These categories include 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 under Directive 2013/36/EU. Therefore, in accordance with the principle of proportionality and to preserve the spirit of sector specific Union legislation, it is also appropriate to subject these financial entities to a simplified ICT- risk framework under this Regulation. The proportionate character of the ICT-risk management framework covering these 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 benefiting from exemptions in accordance with national transpositions of these Union legal acts to a proportionate ICT-risk framework under this Regulation, while payment institutions and electronic money institutions which have not been exempted in accordance with their respective transposition of sectorial Union legislation should comply with the general framework laid down by this Regulation.

(34f) In the same vein, financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework mentioned in the previous recital, should not be required to establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation, to assign the responsibility for managing and overseeing ICT risks 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 an 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 request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents, to maintain redundant ICT capacities, to communicate to national competent authorities implemented changes following post ICT-related incident reviews, to monitor on a continuous basis relevant technological developments, to establish a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework provided for in this Regulation, and 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.

As far as the digital operational resilience testing programme is concerned, microenterprises should benefit from a more flexible regime. When considering the type and frequency of testing to be performed they should properly balance the objective of maintaining a high digital operational resilience and the available resources and their overall risk profile. Microenterprises and financial entities subject to the proportionate ICT risk management framework mentioned in the previous recital, should be exempted from the requirement to perform advanced testing of ICT tools, systems and processes based on threat led penetration testing as such testing should be required only to significant financial entities.
In light of their limited capabilities, microenterprises may 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.

(35) Moreover, as solely those financial entities identified as significant 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 by the performance of such tests should be devolved to a small percentage of financial entities.

(36) 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 management body should be required to maintain a pivotal and active role in steering and adapting the ICT risk management framework and the overall digital resilience strategy. The approach to be taken by the management body should not only focus on the means to ensure 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 over cyber risks and a commitment to respect a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risks 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.

(37) Moreover, the principle of the management body's full and ultimate accountability for the management of 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 enable the latter to achieve a high level of digital operational resilience.

(38) Inspired by relevant international, national and industry-set best practices, guidelines, recommendations or approaches towards the management of cyber risk,[10] this Regulation promotes a set of principles facilitating the overall structuring of the ICT risk management.

Consequently, as long as the main capabilities which financial entities put in place answer the needs of the objectives foreseen by the respective 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.

(39) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and endowed with sufficient capacity not only to guarantee the processing of data as it is necessary for the provision of their services, but also to ensure the technological resilience allowing financial entities to adequately deal with additional processing needs which stressed market conditions or other adverse situations may generate.

(40) Efficient business continuity and recovery plans are required 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 the back-up policies.

However, such resumption should in no way jeopardise the integrity and security of

[10] CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf; G7 Fundamental Elements of Cybersecurity for the Financial Sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB CIRR toolkit, https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/

the network and information systems or the confidentiality, integrity or availability of data.

(41) While this Regulation allows financial entities to determine themselves the recovery time and recovery point objectives in a flexible manner and hence set such objectives by fully taking into account the nature and the criticality of the relevant function and any specific business needs, an assessment on the potential overall impact on market efficiency should also be required when determining such objectives.

(42) Financial entities are typically much more exposed to suffer cyber-attacks and hence to incur significant consequences since propagators are pursuing financial gains directly at the source.

To prevent ICT systems losing integrity or becoming unavailable, and hence to avoid data being breached or physical ICT infrastructure suffering damage, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined.

ICT-related incident reporting should be harmonised for all financial entities through 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 Regulation (EU) No 1024/2013 should submit such reporting to the national competent authorities which should subsequently transmit the reporting to the ECB.

While all financial entities should be subject to incident reporting, such requirement is not expected to affect them in the same manner. Indeed, relevant materiality thresholds, as well as reporting timelines, should be duly calibrated, in the context of delegated acts based on the regulatory technical standards to be developed by the ESAs, with a view to only capture major ICT-related incidents as well as to take into account financial entities' specificities for the purposes of setting timelines for reporting.

In addition, credit institutions, payment institutions, account information service providers and electronic money institutions will report under this Regulation all operational or security payment-related incidents - previously reported under Directive (EU) 2015/2366 - irrespective of the ICT nature of the incident.
Such direct reporting would enable financial supervisors' immediate access to information on major ICT-related incidents.
Financial supervisors should in turn pass on details of major ICT related incident to public non-financial authorities (such as NIS competent authorities, Single Points of Contact, national data protection authorities and law enforcement authorities for major ICT-related incidents of a criminal nature) to enable such authorities awareness on such incidents and in the case of CSIRTs to facilitate prompt assistance to financial entities, as appropriate.
Member States may additionally determine that financial entities themselves provide such information to the public non-financial authorities. This flow of information would allow financial entities to swiftly benefit from any relevant technical input, advice on 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 event, to aid wider collective defence.

(43) The ESAs should be mandated to assess the feasibility and conditions for a possible centralisation of ICT-related incident reports at Union level.
Such a centralisation could be envisaged by means of establishing a single EU Hub for major ICT-related incident reporting either receiving directly 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 to prepare in consultation with the ECB and ENISAa joint report exploring the feasibility of setting up a single EU Hub.

(44) In order to achieve a high digital operational resilience, and in line with both international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing) and with frameworks applied in the Union, such as the TIBER-EU, financial entities should regularly test their ICT systems and staff with 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 different financial subsectors as regards financial entities' preparedness on cybersecurity, 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 threat led penetration testing (TLPT) which should be only required to financial entities that are mature enough from an ICT perspective to carry out such tests.
The digital operational resilience testing set out by this Regulation should thus be more demanding for significant financial entities (such as large credit institutions, stock exchanges, central securities depositories, central counterparties, etc.).
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 (e.g. payments, banking, clearing and settlement), and less relevant for other subsectors (e.g. asset managers, credit rating agencies, etc.).
Financial entities involved in cross-border activities and exercising the freedom of establishment or provision of services within the Union should comply with a single set of advanced testing requirements (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.

To draw on the expertise already acquired by certain competent authorities, notably in the context of the implementation of Tiber -EU framework, this Regulation allows either Member States to designate a single public authority as responsible in the financial sector, at national level, for all threat led penetration testing matters or competent authorities, to delegate, in the absence of such designation, the exercise of TLPT related tasks to another national financial competent authority.
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 in scope of such test.
Pooled testing in the meaning of this Regulation - involving the participation of more financial entities in a threat led penetration testing and for which an ICT third-party service provider may directly enter into contractual arrangements with an external tester - should only be allowed where the quality, confidentiality or security of services delivered by the ICT third-party service provider to customers falling outside the scope of this Regulation are reasonably expected to be adversely impacted, and should 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 TLPT pursuant to this Regulation.

(44a) To allow financial entities to take advantage of internal resources available at corporate level, this Regulation allows the use of internal testers for the purposes of carrying out TLPT, upon supervisory approval, acknowledgment of lack of conflicts of interest, periodical alternation of TLPTs with external testers (every 3 years) while 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 on the level of ICT risk to which the financial entity is exposed nor be seen as an endorsement of its ICT risk management and mitigation capabilities.

(45) 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 the critical or important functions, as well as more generally in context of all ICT third-party dependencies.

(45a) To address the complexity posed by 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 centres services.
In the same vein, since financial entities should identify and manage effectively and coherently 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 equally 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 be equally deemed as ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and of public authorities when providing ICT related services in the context of fulfilling State functions.

(46) A financial entity should remain at all times fully responsible for complying with the obligations under 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.

(47) 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 such ICT third-party dependencies.

To enhance supervisory awareness over ICT third-party dependencies, and with a view to further support 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 on the use of ICT services provided by ICT third-party service providers.

Financial supervisors should be able to request the full register or ask for specific sections thereof, and thus obtain essential information for acquiring a broader understanding of the ICT dependencies of financial entities.

(48) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, notably by looking at elements such as the criticality or importance of the services supported by the envisaged ICT contract, needed supervisory approvals or conditions, 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 contracts could be prompted at least by a series of circumstances showing shortfalls at the ICT third-party service provider level, notably significant breaches of laws or contractual terms, circumstances revealing a potential alteration of the performance of the functions provided in the contract, evidenced weaknesses of the ICT third party service provider in its overall ICT risk management, or circumstances conducive to assert the inability of the competent authority to effectively supervise the financial entity.

(49) 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 on concentration risk since the imposition of any rigid caps or strict limitations may hinder the conduct of business and restrain the contractual freedom. Financial entities should thoroughly assess their envisaged contractual arrangements to identify the likelihood for such risk to emerge, including by means of in-depth analyses of subcontracting arrangements, notably when concluded with ICT third-party service providers established in a third country. At this stage, and with a view to strike a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to provide for strict caps and limits to ICT third-party exposures.

In the context of the Oversight Framework, the Lead Overseer 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 [11].

[11] In addition, should the risk of abuse by an ICT third-party service provider considered dominant arise, financial entities should also have the possibility to bring either a formal or an informal complaint with the European Commission or with the national competition law authorities.

(50) To evaluate and monitor on a regular basis the ability of the ICT third-party service provider to securely provide services to the financial entity without adverse effects on the latter's digital operational resilience, several key contractual elements throughout the performance of contracts with ICT third-party providers should be harmonised.

Such harmonisation should cover minimum areas which are considered crucial for enabling a full monitoring by the financial entity of the risks that may emerge from the ICT third-party service provider, from the perspective of a financial entity's need to secure its digital resilience because the latter is deeply dependent on the stability, functionality, availability and security of the ICT services received.
When renegotiating contracts 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 act.

(51) 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 locations where such functions are provided and where data is to be processed, as well as an indication of service level descriptions.
In the same vein, other elements deemed essential 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 the provisions requiring the ICT third-party service provider to provide assistance in case of ICT incidents in connection to the services provided, at no additional cost or at a cost determined ex-ante; the provisions on the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity and the provisions on termination rights and related minimum notices period for the termination of the contract, in accordance with competent and resolution authorities' expectations.

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

(53) Such contracts 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 latter's full cooperation during inspections.

In the same vein, the competent authority of the financial entity should have those rights, based on notices, to inspect and audit the ICT third-party service provider, subject to confidentiality.

(54) Such contractual arrangements should also foresee 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 reduce the risk of disruptions at the level of the financial entity, or to allow the latter to effectively switch to the use of other ICT third-party service providers, or, alternatively resort to the use of in-house solutions, consistent with the complexity of the provided ICT service.

The definition of 'critical or important function' provided for in this Regulation should encompass the 'critical functions' as defined in point (35) of Article 2(1) of Directive 2014/59/EU. Accordingly, functions deemed to be critical pursuant to Directive (EU) 2014/59/EU should be included in the critical functions within the meaning of this

Regulation.

Moreover, credit institutions should ensure that the relevant contracts for ICT services are robust and fully enforceable in the event of resolution of the credit institutions. Thus, in line with the expectations of the resolution authorities, credit institutions should ensure that the relevant contracts for ICT services are resolution resilient. As long as the credit institutions continues meeting its payment obligations, those financial entities should ensure that the relevant contracts for ICT services contain, among other requirements, clauses for non-termination, non- suspension and non-modification on grounds of restructuring or resolution.

(55) Moreover, the voluntary use of standard contractual clauses developed by public authorities or Union institutions, notably the use of contractual clauses developed by the Commission for cloud computing services may provide further comfort to the financial entities and ICT third-party providers, by enhancing the level of legal certainty on the use of cloud computing services by the financial sector, in full alignment with requirements and expectations set out by the financial services regulation. This work builds on measures already envisaged in the 2018 Fintech Action Plan that announced 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.

(56) With a view to promote convergence and efficiency in relation to supervisory approaches when addressing ICT third-party risk in the financial sector, as well as with a view to strengthen the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the ICT services supporting the provision of services, and thus to contribute to preserving the Union's financial system stability, the integrity of the single 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 in the same time recalled that this solution appears suitable in the context of this Regulation, dealing with a specific subject-matter on digital operational resilience in the financial sector, and should not be deemed as a new model for the Union supervision in the areas of financial services and activities.

(57) Since only critical ICT third-party service providers warrant a special Union monitoring regime, a designation mechanism for the purposes of applying the Union Oversight Framework should be put in place to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers, which translates into a set of quantitative and qualitative criteria that would set the criticality parameters as a basis for inclusion into the Oversight Framework. In order to ensure the accuracy of this 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 the above-mentioned criteria should have the possibility to opt in to the Oversight Framework on a voluntary basis, while those ICT third-party service providers that are already subject to oversight mechanism frameworks supporting the fulfilment of the tasks of the Eurosystem as referred to in Article 127(2) of the Treaty on the Functioning of the European Union should, on the other hand, be exempted.

Similarly, financial entities which provide 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 already subject to supervisory mechanisms established by the respective Union financial services legislation. Where applicable, competent authorities should take into account in the context of their supervisory activities the ICT risks 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 group.
ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State should be also exempted from the designation mechanism by virtue of their limited activities and lack of cross-border impact.

(57a) The digital transformation experienced in financial services has brought about an unprecedented usage of, and reliance on, ICT services. Since the provision of financial services has become unconceivable 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 these companies, innovators in developing and applying ICT-based technologies, play a significant role in the delivery of financial services, or have become integrated in the financial services value chain. They have thus become critical to the stability and integrity of the Union financial system.
This widespread reliance on the services supplied by critical ICT third-party service providers, combined with the interdependence between the information systems of different market operators, create a direct, and potentially severe, risk to the Union financial services system to the continuity of delivery of financial services if critical ICT third-party service providers were to be confronted with 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 finance and can extend across sectors and beyond geographical borders. They may therefore 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 either is unable to withstand, or which requires the deployment of heavy shock absorption measures. To prevent these scenarios from materialising and endangering the financial stability and integrity of the Union, the convergence of supervisory practices relating to ICT third-party risk in finance is essential, in particular through new rules enabling the Union-wide oversight of critical ICT third-party service

providers.

The Oversight framework largely depends on the degree of collaboration between the Lead Overseer and critical ICT third-party service provider delivering to financial entities services affecting the supply of financial services.
The successful execution of the oversight is determined, among others, by 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 integrate the Lead Overseer's recommendations, concerns, perspectives and approaches.
Since a lack of cooperation by a critical ICT third-party service provider delivering services affecting the supply of financial services, such as the refusal to grant access to its premises or to submit information, ultimately deprives 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.

(57b) 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 set of 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, critical ICT third-party service providers, delivering to financial entities services affecting the supply of financial services, should 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.

Therefore, in order to continue its provision of ICT services to financial entities in the Union, an ICT third-party service provider 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 in the Union, by means of a establishing a subsidiary, as defined throughout the Union acquis, namely in Directive 2013/34/EU on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings.

(58) Such requirement to set up a subsidiary in the Union, does not prevent ICT services and related technical support to be provided from facilities and infrastructures located outside the Union. Neither does this Regulation impose data localisation since this Regulation does not entail any further requirement on data storage or processing to be undertaken in Union.

(58a) Critical ICT third-party service providers may provide ICT services from anywhere in the world, hence not necessarily or not only from premises located in the Union. Oversight objectives 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. These actions might however not be sufficient to allow the Lead Overseer to fully and effectively perform its duties under this Regulation. The Lead Overseer should therefore be empowered to exercise its relevant oversight powers in third countries as well. Exercising these powers in third countries would allow the Lead Overseer to examine facilities from where the ICT services or the technical support are actually provided, or managed, by the critical ICT third-party service provider, and, as such, would give the Lead Overseer a comprehensive and operational understanding of the ICT risk management of the critical ICT third-party service provider.

The possibility of the Lead Overseer, as a Union agency, to exercise powers outside the territory of the Union, should be duly framed by relevant conditions, notably the consent of the concerned critical ICT third-party service provider and the information and non-objection of the relevant authority of the third country of the exercise, on its own territory, of such powers of the Lead Overseer. At the same time, for reasons of ensuring efficient implementation, without prejudice to the respective competences of the Member States and the Union institutions such powers also need to be fully anchored in the establishment of administrative cooperation arrangements with the relevant authorities of the concerned third country. Hence, with a view to ease the practical implementation of the Lead Overseer's powers to carry-out inspections in third countries, this Regulation should enable the ESAs to conclude administrative cooperation arrangements with the relevant authorities of the third countries, which should not create legal obligations in respect of the Union and its Member States.

(58b) To ease the communication channels with the Lead Overseer and ensure adequate representation, critical ICT third-party service providers part of a group should designate one legal person as coordination point.

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

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

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

(62) Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the critical ICT third-party service providers premises and locations and to obtain complete and updated information. This set of 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 grasping and addressing the systemic dimension of ICT risk in finance. The Union footprint of critical ICT third-party service providers and the potential issues of attached ICT concentration risk call for taking a collective approach exercised at Union level.
A simultaneous conduct of multiple audits and access rights, performed separately by numerous competent authorities, with little or no coordination would prevent financial supervisors from obtaining a complete and comprehensive overview on 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.

(63) Due to the significant impact of being designated as critical, this Regulation should ensure the need to respect the rights of critical ICT third-party service providers throughout the entire oversight framework. Thus, they should be granted the right to be heard prior to the designation decision by means of 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, 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 be given the opportunity to provide, prior to the finalisation of the recommendations, explanations regarding the expected impact of the solutions envisaged in the recommendation upon customers falling outside this Regulation and formulating solutions to mitigate risks. Critical ICT third-party service providers disagreeing with the adopted recommendation should be given the right to submit a reasoned explanation of their intention not to endorse the recommendation.

Before issuing recommendations in accordance with paragraph 1, the Lead Overseer shall give the opportunity to the ICT third-party service provider to provide within 30 calendar days relevant information evidencing expected impact on customers not subject to this Regulation and where appropriate, formulating solutions to mitigate risks.

Where such explanations are deemed insufficient, the Lead Overseer should issue a public notice describing summarily the matter of non-compliance.

(63b) Competent authorities should duly integrate the task of verifying the substantive compliance with recommendations issued by the Lead Overseer in their functions of prudential supervision of financial entities. Competent authorities may require financial entities to take additional measures to duly tackle the risks identified in the Lead Overseer's recommendations, and should, in due course, issue notifications to that effect.

Where recommendations are addressed to critical ICT third-party service providers that are supervised under the NIS Directive, competent authorities may, on a voluntary basis, before adopting additional measures, consult the NIS competent authorities to

help foster a coordinated approach for the treatment of the respective critical ICT third-party service providers.

(63c) The exercise of the Oversight should be guided by three operational principles seeking to ensure (a) ESAs close coordination in their Lead Overseers roles (through the Joint Oversight Network), (b) consistency with the framework established by Directive [add NIS 2 reference] (though a voluntary consultation of authorities established by that Directive to avoid duplication of measures directed at critical ICT third-party service providers) and (c) diligence in minimising the potential risk of disruption to services provided by the critical ICT third-party service providers to customers not subject to this Regulation.

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

(64a) To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring 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 previously coordinated and agreed with the Lead Overseer in the context of the exercise of tasks in the Oversight Framework.

(65) To promote convergence at international level on best practices to be used 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 to facilitate the development of best practices addressing ICT third-party risk.

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

(66a) Whereas costs resulting from oversight tasks would be fully funded from fees levied on critical ICT third-party service providers, the ESAs would incur, in advance of the start of the oversight framework, also costs for the implementation of dedicated ICT systems supporting the Oversight, since such ICT systems would need to be developed and deployed beforehand. This Regulation consequently provides for a hybrid funding model, whereby the oversight framework, as such, is fully fee-funded, while the development of the ESAs' IT systems is funded from Union and national competent authorities' contributions.

(67) Competent authorities should possess all required supervisory, investigative and sanctioning powers to ensure the application of this Regulation. Administrative penalties should, in principle, be published. 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 close cooperation, on the one hand, between the relevant competent authorities including the ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013[12] 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.

---

[12] 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).

(68) 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 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of 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 supplies, 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, 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 provider 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.[13] 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.

(69) Since this Regulation, together with Directive (EU) 20xx/xx of the European Parliament and of the Council,[14] 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, 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.

---

13 OJ L 123, 12.5.2016, p. 1.

14 [Please insert full reference]

Regulatory technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. In their roles of bodies endowed with highly specialised expertise, the ESAs should be mandated to 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.

(70) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. 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, the nature, scale and complexity of their services, activities and operations, and their overall risk profile.

(71) To facilitate the comparability of major ICT-related incidents, major operational or security payment-related incidents reports as well as to ensure transparency on contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should be mandated to 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 standardized templates for the register of information. When developing those standards, the ESAs should take into account the size of the financial entities, the nature, scale and complexity of their services, activities and operations, and their overall risk profile. 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, respectively. 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, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, respectively, 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.

(72) This exercise will entail the subsequent amendments of existing delegated and implementing acts adopted in different areas of the financial services legislation. The scope of the relevant articles related to operational risk upon which empowerments laid down in those acts had mandated the adoption of delegated and implementing acts should consequently be modified with a view to carry over into this Regulation all provisions covering the digital operational resilience aspects which today are part of those Regulations.

(72a) 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 consider the need for enlarging the scope of this Regulation while aligning such review with the outcome of the comprehensive revision envisaged for the Payment Services Directive.
Numerous large-scale attacks over the past decade demonstrate how payment systems have become an entry point for cyber threats. Placed at the core of the payment services chain and evidencing strong interconnections with the overall financial system, payment systems and payment processing activities acquired a critical significance for the functioning of the European financial markets. Cyber-attacks on such systems can cause severe operational business disruptions with direct repercussions on a key economic function, such the facilitation of payments, and indirect reactions on related economic processes.
Until a harmonised regime and supervision of operators of payment systems and processing entities are put in place at Union level, Member States may, with a view to apply 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.

(73) 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 and different rules in Union acts or in the legislations of some Member States, but can rather, because 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.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

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

   (a) requirements applicable to financial entities in relation to:

   - Information and Communication Technology (ICT) risk management;
   - reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;

- 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 (c);
- digital operational resilience testing;
- information and intelligence sharing in relation to cyber threats and vulnerabilities;
- measures for the sound management of ICT third-party risk by financial entities;

(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) 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 operators of essential services pursuant to national rules transposing Article 5 of Directive (EU) 2016/1148, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 1(7) of that Directive.

2a. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

Article 2

Personal 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 in accordance with Article 32 (1) of Directive (EU) 2015/2366,

(ba) account information service providers,

(c) electronic money institutions, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC,

(d) investment firms,

(e) crypto-asset service providers as authorized under MiCA and issuers of asset-referenced tokens,

(f) central securities depositories,

(g) central counterparties,

(h) trading venues,

(i) trade repositories,

(j) managers of alternative investment funds,

(k) management companies,

(l) data reporting service providers,

(m) insurance and reinsurance undertakings,

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,

(o) institutions for occupational retirement provision,

(p) credit rating agencies,

(q)

(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 (a) to (t) shall collectively be referred to as 'financial entities'.

3. This Regulation shall not apply to:

(a) managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU;

(b) insurance and reinsurance undertakings 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 from the application of Directive 2014/65/EU pursuant to Articles 2 and 3 of that Directive;

(e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises, small or medium-sized enterprises;

(g) institutions referred to in point (3) of Article 2(5) of Directive 2013/36/EU.

4. Member States may exempt institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU that are located within their respective territory from the scope of this Regulation. In case such option is exercised, this Regulation shall not apply to the exempted institutions.

Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes. The Commission shall make the information public on a 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 of 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 makes use of, and which support the continued provision of financial services and their quality throughout disruptions;

(2) 'network and information system' means network and information system as defined in point (1) of Article 4 of Directive (EU) No 2016/1148;

(2a) “legacy ICT system” means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades and fixes, due to technological or commercial reasons, or is no longer supported by its supplier or an ICT third-party service provider, but that is still in use and supports the functions of the financial entity;

(3) ‘security of network and information systems’ means security of network and information systems as defined in point (2) of Article 4 of Directive (EU) No 2016/1148;

(4) ‘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;

(5) ‘information asset’ means a collection of information, either tangible or intangible, that is worth protecting;

(5a) ‘ICT asset’ means a software or hardware asset in the network and information systems used by the financial entity;

(6) ‘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 has an adverse impact on the availability, authenticity, integrity or confidentiality of data or of the services provided by the financial entity;

(6a) ‘operational or security payment-related incident’ means a single event or a series of linked events unplanned by the financial entities referred to in points (a) to (c) of Article 2(1), ICT-related or not, that has an adverse impact on the confidentiality, integrity or availability of data, or the continuity of payment-related services provided;

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

(7a) ‘major operational or security payment-related incident’ means an operational or security payment-related incident that has a high adverse impact on the confidentiality, integrity or availability of data, or the continuity of payment-related services provided;

(8) ‘cyber threat’ means ‘cyber threat’ as defined in point (8) of Article 2 Regulation (EU) 2019/881 of the European Parliament and of the Council[15];

(8a) ‘significant cyber threat’ means a cyber threat whose technical characteristics indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident*;*

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

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

(11) ‘defence-in-depth’ means an ICT-related strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the financial entity;

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

(13) ‘threat led penetration testing’ 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;

---

15 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).

(14) ‘ICT third-party risk’ means 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;

(15) ‘ICT third-party service provider’ means an undertaking providing ICT services;

(15a) ‘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;

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

(17) ‘critical or important function’ means a function whose disruption would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or whose discontinued, defective or failed performance 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 legislation;

(18) ‘critical ICT third-party service provider’ means an ICT third-party service provider designated in accordance with Article 28;

(19) ‘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 that has entered into a contractual arrangement with a financial entity for the provision of ICT services;

(19a) "subsidiary" means a subsidiary undertaking as defined in point (10) of Article 2 and Article 22 of Directive 2013/34/EU of the European Parliament and of the Council;

(19b) "group" means a group as defined in point (11) of Article 2 of Directive 2013/34/EU of the European Parliament and of the Council;

(19c) "parent undertaking" means a parent undertaking as defined in point (9) of Article 2 and Article 22 of Directive 2013/34/EU of the European Parliament and of the Council;

(20) 'ICT subcontractor established in a third country' means an ICT subcontractor that is a legal person established in a third-country 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;

(21) '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 the latter may potentially endanger the ability of a financial entity to deliver critical or important functions, or to suffer other type of adverse effects, including large losses, or endanger *the* financial stability of the Union as a whole;

(22) 'management body' means a management body as defined in point (36) of Article 4(1) of Directive 2014/65/EU, point (7) of Article 3(1) of Directive 2013/36/EU, point (s) of Article 2(1) of Directive 2009/65/EC, point (45) of Article 2(1) of Regulation (EU) No 909/2014, point (20) of Article 3(1) of Regulation (EU) 2016/1011 of the European Parliament and of the Council[16], point (18) of Article 3(1) of Regulation (EU) 20xx/xx of the European Parliament and of the Council[17] [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation.

---

16 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).

17 [please insert full title and OJ details]

(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[18];

(23b) ‘institution exempted pursuant to Directive 2013/36/EU’ means a institution as referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU;

(24) ‘investment firm’ means an investment firm as defined in point (1) of Article 4(1) of Directive 2014/65/EU;

(24a) ‘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;

(25) ‘payment institution’ means a payment institution as defined in point (4) of Article 4 of Directive (EU) 2015/2366;

(25a) ‘payment institution exempted pursuant to Directive (EU) 2015/2366’ means a payment institution benefitting from an exemption pursuant to Article 32 (1) of Directive (EU) 2015/2366;

(25b) ‘account information service providers’ means an account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;

(26) ‘electronic money institution’ means an electronic money institution as defined in point (1) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[19];

(26a) ‘electronic money institution exempted *pursuant to* Directive 2009/110/EC’ means an electronic money institution benefitting from a waiver under Article 9 of Directive 2009/110/EC;

---

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

19 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).

(27) ‘central counterparty’ means a central counterparty as defined in point (1) of Article 2 of Regulation (EU) No 648/2012;

(28) ‘trade repository’ means a trade repository’ as defined in point (2) of Article 2 of Regulation (EU) No 648/2012;

(29) ‘central securities depository’ means a central securities depository as defined in point (1) of Article 2(1) of Regulation 909/2014;

(30) ‘trading venue’ means a trading venue as defined in point (24) of Article 4(1) of Directive 2014/65/EU;

(31) ‘manager of alternative investment funds’ means a manager of alternative investment funds as defined in point (b) of Article 4(1) of Directive 2011/61/EU;

(32) ‘management company’ means a management company as defined in point (b) of Article 2(1) of Directive 2009/65/EC;

(33) ‘data reporting service provider’ means a data reporting service provider within the meaning of Regulation 600/2014, referred to in Article 2(1), points (34) to (36);

(34) ‘insurance undertaking’ means an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC;

(35) ‘reinsurance undertaking’ means a reinsurance undertaking as defined in point (4) of Article 13 of Directive 2009/138/EC;

(36) ‘insurance intermediary’ means insurance intermediary as defined in point (3) of Article 2 (1) of Directive (EU) 2016/97;

(37) ‘ancillary insurance intermediary’ means an ancillary insurance intermediary as defined in point (4) of Article 2 (1) of Directive (EU) 2016/97;

(38) ‘reinsurance intermediary’ means a reinsurance intermediary as defined in point (5) of Article 2(1) of Directive (EU) 2016/97;

(39) ‘institution for occupational retirement provision’ means an institution for occupational retirement provision as defined in point (1) of Article 6 of Directive 2016/2341;

(39a) ‘small institution for occupational retirement provision’ means an institution for occupational retirement provision as defined in point (39), which operates pension schemes which together have less than 100 members in total;

(40) ‘credit rating agency’ means a credit rating agency as defined in point (a) of Article 3(1) of Regulation (EC) No 1060/2009;

(41)

(42)

(43) ‘crypto-asset service provider’ means crypto-asset service provider as defined in point (8) of Article 3(1) of Regulation (EU) 202x/xx [PO: insert reference to MiCA Regulation];

(44)

(45) ‘issuer of asset-referenced tokens’ means an issuer of ‘asset-referenced tokens’ as defined in point (3) of Article 3 (1) of [OJ: insert reference to MiCA Regulation];

(46)

(47) ‘administrator of critical benchmarks’ means an administrator of “critical benchmarks” as defined in point (25) of Article 3 of Regulation 2016/1011 [OJ: insert reference to Benchmark Regulation];

(48) ‘crowdfunding service provider’ means a crowdfunding service provider as defined in point (e) Article 2(1)of Regulation (EU) 2020/1503;

(49) ‘securitisation repository’ means securitisation repository as defined in point (23) of Article 2 of Regulation (EU) 2017/2402;

(50) ‘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 whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million;

(51) Lead Overseer means the European Supervisory Authority appointed in accordance with Article 28;

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

(54) ‘small enterprise’ means a financial entity that employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million;

(50f) "medium-sized enterprise" means a financial entity that is not a small enterprise and employs fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million;

(55) ‘public authority’ means any government or other public administration entity, including national central banks.

Article 3a

Proportionality principle

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

2. In addition, the application by financial entities of Chapters III, IV and Section I of Chapter V shall be proportionate to their size, nature, scale and complexity of the services, activities and operations, and their overall risk profile, 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, if requested, on the basis of Article 5(6) and Article 14a(2).

CHAPTER II

ICT RISK MANAGEMENT

SECTION I

Article 4

Governance and organisation

1. Financial entities shall have in place an internal governance and a control framework that ensures an effective and prudent management of all ICT risks, in accordance with Article 5(5), 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 accountable for the implementation of all arrangements related to the ICT risk management framework referred to in Article 5(1).

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

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

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

(b) 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 them;

(c) bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 5(9) including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9);

(d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT response and recovery plans, 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, referred to in, respectively, paragraphs 1 and 3 of Article 10;

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

(f) allocate and periodically review appropriate budget to fulfil the financial entity’s digital operational resilience needs in respect of all types of resources, including relevant training on ICT security awareness and digital operational resilience referred to in Article 12(6) first subparagraph and ICT skills for all staff;

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

(h) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;

(i) be duly informed about at least major ICT-related incidents and their impact and about response, recovery and corrective measures.

3. Financial entities other than microenterprises shall establish a role 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 sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risks being managed.

SECTION II

Article 5

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 referred to in paragraph 1 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, relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all those information assets and ICT assets are adequately protected from risks including damage and unauthorized access or usage.

3. Financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, protocols and tools as determined in the ICT risk management framework. They shall provide complete and updated information on ICT risks and on their ICT risk management framework as requested by the competent authorities.

4.

5. Financial entities other than microenterprises shall assign the responsibility for managing and overseeing ICT risks 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 defense model, or an internal risk management and control model.

6. The ICT risk management framework referred to in paragraph 1 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.

7. As regards financial entities other than microenterprises, the ICT risk management framework referred to in paragraph 1 shall be subject to internal audit on a regular basis in line with the financial entities' audit plan by auditors possessing 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 risks of the financial entity.

8. A formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings, shall be established, taking into consideration the conclusions from the audit review.

9. The ICT risk management framework referred to in paragraph 1 shall include a digital operational resilience strategy setting out how the framework is implemented. To that effect the digital operational resilience strategy shall include the 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 limit 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, protect and prevent impacts of ICT-related incidents;

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

(g)

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

(i) outlining a communication strategy in case of ICT-related incidents required to be disclosed in accordance with Article 13.

9a. Financial entities may, in the context of the strategy referred to in paragraph 9, 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 national and European sectoral legislation, outsource the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings. In case of such outsourcing, the financial entity remains fully accountable for the verification of compliance with the ICT risk management requirements.

Article 6

ICT systems, protocols and tools

1. Financial entities shall use and maintain updated ICT systems, protocols and tools, in order to address and manage ICT risk, that are:

(a) appropriate to the magnitude of operations supporting the conduct of their activities, as referred to in Article 3a;

(b) reliable;

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

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

Article 7

Identification

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting these functions, and their roles and dependencies with 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 functions, supporting processes or information 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 support critical or important functions.

6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories which must be updated periodically and every time any major change as referred to in Article 7(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.

Annual ICT risk assessments shall be conducted on legacy ICT systems especially before and after connecting technologies, applications or systems.

Article 8

Protection and Prevention

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

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

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

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

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

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

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

4. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:

(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of the 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 using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in case of cyber-attacks;

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

(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls 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, system or security changes, that are based on a risk-assessment approach and as 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 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 point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.

Article 9

Detection

1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, 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 22.

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, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

4. Financial entities referred to in points (34) and (36) of Article 2 (1) of Regulation 600/2014 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 any such erroneous reports.

Article 10

Response and recovery

1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place 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 referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:

   (a)

   (b) ensuring the continuity of the financial entity's critical or important functions;

   (c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in a way that limits damage and prioritises resumption of activities and recovery actions;

   (d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;

   (e) estimating preliminary impacts, damages and losses;

   (f) setting 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 13, and reported to competent authorities in accordance with Article 17.

3. As part of the ICT risk management framework referred to in Article 5(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.

4a. As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions.

Financial entities shall assess under the BIA 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, supporting processes, third-party dependencies and information assets, and their interdependencies.

Financial entities shall foresee a design and usage of ICT assets and ICT services in full alignment with the BIA notably with regard to adequately ensuring the redundancy of all critical components.

5. 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 upon any substantive changes to ICT systems supporting critical or important functions;

(b) test the crisis communication plans established in accordance with Article 13.

For the purposes of 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 11.

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.

6. Financial entities other than microenterprises shall have a crisis management function, which, in case 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 13.

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

8. Financial entities referred to in point (f) of Article 2(1) shall provide to the competent authorities copies of the results of the ICT business continuity tests or similar exercises performed during the period under review.

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

9a. The ESAs shall, through the Joint Committee, develop common guidelines on the estimation of aggregated annual costs and losses referred to in paragraph 9 by [OJ: insert date 18 months after the date of entry into force].

Article 11

Backup policies, restoration and recovery 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) recovery methods.

2. Financial entities shall set up backup-systems that can be activated for processing in accordance with the backup policies, procedures and recovery methods referred to in paragraph 1.
   The activation of backup systems shall not jeopardize the security of the network and information systems or the confidentiality, integrity or availability of data.
   Testing of the backup and restoration procedures shall be undertaken on a periodic basis.

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 unauthorized access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.

For financial entities referred to in point (g) of Article 2(1), 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 functionalities that are sufficient and adequate to ensure business needs. Microenterprises shall assess the need to maintain such redundant ICT capacities based on their risk profile.

5. Financial entities referred to in point (f) of Article 2(1) shall maintain at least one secondary processing site endowed with resources, capabilities, functionalities and staffing arrangements sufficient and appropriate 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 case the primary processing site has become unavailable.

6. In determining the recovery time and 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 level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

Article 12

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 their likely impacts on their digital operational resilience.

2. Financial entities shall put in place post ICT-related incident reviews after major ICT-related incidents disrupting 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 10.

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

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:

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

(b) the quality and speed in performing 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 operation resilience testing carried out in accordance with Articles 23 and 24 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 counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework referred to in Article 5(1).

4. Financial entities shall monitor the effectiveness of the implementation of their digital resilience strategy set out in Article 5(9). They shall map the evolution of ICT risks over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understand the level of ICT risk exposure, notably 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 programs and digital operational resilience trainings as compulsory modules in their staff training schemes. These shall be applicable to all employees and to senior management staff, and 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 27(2) point (kd).

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

Article 13

Communication

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place 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 referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.

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

Article 14

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 for the following purposes:

(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the confidentiality, integrity and availability of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays;

(b)

(c)

(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;

(e) develop further the elements specified in Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;

(f) specify further the components of the ICT business continuity policy referred to in Article 10(1);

(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to ensure that it 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;

(h) specify further the components of the ICT response and recovery plans referred to in Article 10(3).

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

When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities, 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 [OJ: insert date 12 months after the date of entry into force].

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, respectively.

Article 14a

Simplified ICT risk management framework

1. Articles 4 to 14 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), electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision.

   These financial entities shall nevertheless:

   (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 all ICT risks, including for the protection of relevant physical components and infrastructures;

(b) continuously monitor the security and functioning of all ICT systems;

(c) minimize the impact of ICT risks 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 confidentiality, integrity and availability of data 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 and important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restore 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 according to points (a) and (c) above;

(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 training and awareness programs for staff and management.

2. The ICT risk management framework referred to in point (a) of paragraph 1 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 European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards for the following purposes:

(a) specify further the elements to be included in the ICT risk management framework referred to in point (a) of paragraph 1;

(b) specify further the elements in relation to systems, protocols and tools to minimize the impact of ICT risks referred to in point (c) of paragraph 1, with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse and preserve the confidentiality, integrity and availability of data;

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

(d) specify further the rules on the testing of business continuity plans and of the effectiveness of the controls implemented referred to in point (g) of paragraph 1 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.

(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, nature, scale, complexity and overall risk profile of the financial entities.

The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 12 months after the date of entry into force].

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, respectively.

CHAPTER III

ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING

Article 15

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 make sure 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

   (a) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and to the severity and criticality of the services impacted, in accordance with the criteria referred to in Article 16(1);

   (b) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;

   (c) set out plans for communication to staff, external stakeholders and media in accordance with Article 13, and for notification to clients, 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;

(d) ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body on at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents;

(e) establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.

Article 16

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, such as confidentiality, integrity or availability loss;

(e)

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

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

1a. 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.

2. The ESAs shall, through the Joint Committee and in consultation with the European Central Bank (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 17(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 for major ICT-related incidents or, as applicable, major operational or security payment-related incidents to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.

(c) the criteria set out in paragraph 1a, including high materiality thresholds for determining significant cyber threats.

3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account the criteria referred to in Article 3a(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 referred to in Article 3a(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 [PO: insert date 12 months after the date of entry into force].

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.

Article 17

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 41 in accordance to paragraph 3.

Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 41, 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 relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU that shall systematically and immediately, transmit the 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 3 using the template referred to in Article 18 and submit it to the competent authority. In case of technical impossibility of submitting the template, financial entities shall submit the initial notification to the competent authority via alternative communication channels.

The initial notification and reports referred to in paragraph 3 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 by the financial entity to the relevant competent authority, pursuant to the first subparagraph, Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report referred to in paragraph 3 using the template referred to in Article 18 to the national competent authorities or the national Computer Security Incident Response Teams designated in accordance with Articles 8 and 9 of Directive (EU) 2016/1148.

1a. 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 5.

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 that shall systemically and immediately transmit the notification to the ECB.

Member States may determine that those financial entities that on a voluntary basis notify in accordance to paragraph 1 may also transmit that notification to the national Computer Security Incident Response Teams designated in accordance with Articles 8 and 9 of Directive (EU) 2016/1148.

2. Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay after having 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.

3. Financial entities shall submit to the relevant competent authority within the time-limits to be set out in accordance with Article 18(1a):

(a) an initial notification;

(b) an intermediate report, 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, after the initial notification referred to in point (a), 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 or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.

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

5. Upon receipt of the initial notification and each report referred to in paragraph 3, 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 points (a), (b) and (c) of Article 2(1); and

(c) the national competent authorities, single point of contact or Computer Security Incident Response Teams designated, respectively, in accordance with Articles 8 and 9 of Directive (EU) 2016/1148;

(ca) the resolution authorities, as referred to in Article 3 of Directive (EU) No 2014/59, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014, 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 concerns incidents that pose a risk to ensuring critical functions within the meaning of Article 2(1) of the Directive 2014/59/EU;

(d) other relevant public authorities under national law.

6. Following receipt of information in accordance with paragraph 5, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess the relevance of the major ICT-related incident to other relevant competent authorities in other Member States. Following this assessment, EBA, ESMA or EIOPA shall notify relevant competent authorities in other Member States accordingly as soon as possible. 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.

(7) The notification to be done by ESMA pursuant to paragraph 6 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 financial entity referred to in Article 2 (1) (f) has significant cross-border activity in the host Member State, the major ICT-related incident is likely to entail 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 18

Harmonisation of reporting content and templates

1. 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:

      (1) establish the content of the reporting for major ICT-related incidents in order to reflect the criteria laid out in the first paragraph of Article 16 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;

      (2) determine the time-limits for the initial notification and each report referred to in Article 17(3).

      (3) 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, nature, scale, complexity and overall risk profile of the financial entities, and notably with a view to ensure, that, for the purposes of point (2), different time-limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach on ICT-related incident reporting across this Regulation and the Directive…(reference to NIS2). The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of the NIS 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 notify a significant cyber threat.

The ESAs shall submit the common draft regulatory technical standards referred to in point (a) of the first subparagraph and the common draft implementing technical standards referred to in point (b) of the first subparagraph to the Commission by xx 202x [PO: insert date 18 months after the date of entry into orce].

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

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

Article 19

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 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 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;

(ba) the needed capability to ensure interoperability with regard to other relevant reporting schemes;

(c) elements of operational management;

(d) conditions of membership;

(e) modalities for financial entities and national competent authorities to access the single EU Hub;

(f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the single EU Hub, including the required expertise

3. The ESAs shall submit the report referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [OJ: insert date 24 months after the date of entry into force].

Article 20

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 national Computer Security Incident Response Teams pursuant to the tasks foreseen in Article 9 of Directive (EU) 2016/1148, the competent authority shall, upon receipt of each initial notification and reports as referred to in Article 17(3), acknowledge receipt of notification and may, where feasible, provide in a timely manner relevant and proportionate feedback or high-level guidance to the financial entity, in particular to make available any relevant anonymised information and intelligence on similar threats, discuss remedies applied at the level of the entity and ways to minimise and mitigate adverse impact across financial sectors.

Without prejudice to the supervisory feedback received, financial entities shall remain fully accountable for the handling and consequences of the ICT-related incidents reported pursuant to Article 17(1).

2. The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the major ICT-related incidents, the details of which are provided by competent authorities in accordance with Article 17(5), setting out at least the number of major ICT-related incidents, their nature, impact on the operations of financial entities or clients, costs and remedial actions taken.

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

Article 20a

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 21

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 or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities other than microenterprises shall, taking into account the criteria referred to in Article 3a(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 5.

2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.

3. Financial entities referred to in paragraph 1 shall follow a risk-based approach taking into account the criteria referred to in Article 3a(2) when conducting the digital operational resilience testing programme referred to in paragraph 1, duly considering the evolving landscape of ICT risks, any specific risks to which the financial entity 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 referred to in paragraph 1 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 referred to in paragraph 1 shall establish procedures and policies to prioritise, classify and remedy all issues acknowledged 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 referred to in paragraph 1 shall ensure that appropriate tests are conducted on all critical ICT systems and applications at least yearly.

Article 22

Testing of ICT tools and systems

1. The digital operational resilience testing programme referred to in Article 21 shall provide, in accordance with the criteria referred to in Article 3a(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 or penetration testing.

2. Financial entities referred to in points (f) and (g) of Article 2(1) shall perform vulnerability assessments before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.

3. Microenterprises shall perform the tests referred to in paragraph 1 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 time to be allocated to the ICT testing foreseen 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 23

Advanced testing of ICT tools, systems and processes based on threat led penetration testing

1. Financial entities other than financial entities referred to in Article 14a and other than microenterprises identified in accordance with the second subparagraph of paragraph 3 shall carry out at least every 3 years advanced testing by means of threat led penetration testing.
   Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where needed, request the financial entity to reduce or extend this frequency.

2. Each threat led penetration test shall cover several or all critical or important functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical or important functions and services, shall be determined by financial entities and shall be validated by the competent authorities.

   For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical or important functions and ICT services, including critical or important functions and services outsourced or contracted to ICT third-party service providers.

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

Without prejudice to the first subparagraph, where the participation of an ICT third-party service provider in the threat led penetration testing, as referred to in the third subparagraph, is reasonably expected to have an adverse impact on the quality, confidentiality or security of services delivered by the ICT third-party service provider to customers that fall outside the scope of this Regulation, 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 threat led penetration testing involving several financial entities ("pooled testing") to which the ICT third-party service provider provides ICT services.

The pooled testing referred to in subparagraph 4 shall cover the relevant range of services supporting the critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing referred to in subparagraph 4 shall be considered as threat led penetration testing carried out by respective pooled financial entities referred to in paragraph 1.

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

Financial entities shall, with the cooperation of ICT third-party service providers and other involved parties, 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 counterparties or to the financial sector.

At the end of the test, after reports and remediation plans have been agreed, the financial entity and the external testers shall provide to the authorities, designated in accordance with paragraph 3a or 3b, a summary of the relevant findings, the remediation plans and the documentation demonstrating that the threat led penetration testing has been conducted in accordance with the requirements.

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

Without prejudice of such attestation, financial entities shall remain at all times fully responsible for the impacts of the tests referred to in the fourth subparagraph of Article 23(2).

3. Financial entities shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.
When financial entities employ internal testers for the purposes of undertaking threat led penetration testing, they shall contract an external tester every three tests.
Financial entities referred to in point a) of Article 2(1) that are classified as significant in accordance with Article 6 paragraph 4 of Regulation (EU) 1024/2013, shall only use external testers in accordance with points (a)-(e) of paragraph 1 of Article 24.

Competent authorities shall identify financial entities required to perform threat led penetration testing taking into account the criteria referred to in Article 3a(2), based on the assessment of the following:

(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;

(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;

(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved.

3a. Member States may designate a single public authority in the financial sector to be responsible for threat led penetration testing related matters at national level in the financial sector and shall entrust it with all competences and tasks to that effect.

3b. In the absence of a designation in accordance with paragraph 3a and without prejudice to the power to identify the financial entities to perform threat led penetration testing, a competent authority may delegate the exercise of some or all of the tasks referred to in Articles 23 and 24 to other national authority in the financial sector.

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

(a) the criteria used for the purpose of the application of the second subparagraph of paragraph 3 of this Article;

(aa) the requirements and standards governing the use of internal testers;

(b) the requirements in relation to:

(i) the scope of threat led penetration testing referred to in paragraph 2 of this Article;

(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;

(c) the type of supervisory and other relevant cooperation needed for the implementation of threat led penetration testing, 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 [OJ: insert date 18 months after the date of entry into force].

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

Article 24

Requirements for testers for the deployment of threat led penetration testing

1. Financial entities shall only use testers for the deployment of threat led penetration testing, which:

   (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 execution of threat led penetration testing, including the proper 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.

1a. The use of internal testers shall be subject to the following conditions:
i) their use has been approved by the relevant competent authority or respectively by the single public authority designated in accordance with Article 23(3a);
ii) the relevant competent authorities have 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;
iii) the threat intelligence provider is external to the financial entity

2. Financial entities shall ensure that contracts concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, 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 25

General principles

Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:

1. 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 complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.

2. Financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account:

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

   (b) 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 to the potential impact on the continuity and availability of financial services and activities, at individual and at group level.

3. As part of their ICT risk management framework, financial entities other than financial entities referred to in Article 14a 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 point (g) of Article 5(9) if applicable. That strategy shall include a policy on the use of ICT services concerning critical or important functions provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services shall regularly review the risks identified in respect to contractual arrangements on the use of ICT services concerning critical or important functions.

4. 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 critical or important functions and those that do not.

Financial entities shall report at least yearly to the competent authorities information 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 services and functions which are being provided.

Financial entities shall make available to the competent authority, upon 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 concerning critical or important functions and when a function has become critical or important.

5. 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 concerning 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 arrangements may contribute to reinforcing ICT related concentration risk as referred to in Article 26;

(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.

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

7. In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall on a risk-based approach pre-determine the frequency of audits and inspections and 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 auditors or a pool of auditors, possess appropriate skills and knowledge to effectively perform relevant audits and assessments.

8. Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated at least under 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 the overall ICT risk management and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information;

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

9. For ICT services related to 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 of the latter, a deterioration of the quality of the functions provided, any business disruption due to inappropriate or failed provision of services or material risk arising in relation to the appropriate and continuous deployment of the function, or in the event of termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 8.

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 their provision of services to clients.

Exit plans shall be comprehensive, documented and in accordance with the criteria referred to in Article 3a(2), sufficiently tested and reviewed periodically.

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

Financial entities shall take appropriate contingency measures to maintain business continuity under all of the circumstances referred to in the first subparagraph.

10. 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 4, 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 [OJ: insert date 12 months after the date of entry into force of this Regulation].

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 1095/2010 and (EU) No 1094/2010, respectively.

11. 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 3 in relation to the contractual arrangements on the use of ICT services concerning 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, nature, scale, complexity and overall risk profile of the financial entities.

The ESAs shall submit those draft regulatory technical standards to the Commission by [PO: insert date 12 months after the date of entry into force].

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

Power is delegated to the Commission to adopt implementing technical standards referred to in paragraph 10 in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.

Article 26

Preliminary assessment of ICT concentration risk

1. When performing the identification and assessment of ICT concentration risk referred to in point (c) of Article 25(5), financial entities shall take into account whether the conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:

   (a) contracting with 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 arrangement on the use of ICT services supporting critical or important functions includes the possibility that an ICT third-party service provider further subcontracts 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 possible subcontracting, in particular in the case of an ICT subcontractor established in a third-country.

Where contractual arrangements on the use of ICT services concerning critical or important functions are concluded with an ICT third-party service provider, 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 respect of Union data protection rules and the effective enforcement of the law.

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 27

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 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:

   (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 a critical or important function, or material parts thereof, is permitted and, if so, 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 in advance the financial entity if it envisages changing such locations;

   (c) provisions on accessibility, availability, integrity, security, confidentiality and protection of data, including personal data;

   (ca) 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 case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the case of termination of the contractual arrangements;

   (d) service level descriptions, including updates and revisions thereof;

   (e)

(f) the obligation of the ICT third-party service provider to provide assistance in case of an ICT-related incident related to the service provided at no additional cost or at a cost that is determined ex-ante;

(g)

(h)

(i) the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them;

(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent and resolution authorities' expectations;

(k)

(kd) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programs and digital operational resilience trainings in accordance with Article 12(6).

2a. The contractual arrangements for the provision of critical or important functions shall, in addition to paragraph 2, include 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 an effective monitoring by the financial entity and enable without undue delay appropriate corrective actions to be taken 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 carry out 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 secure 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 a threat led penetration test of the financial entity as referred to in Article 23 and 24;

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

(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 commitment by the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, lead overseer, financial entity or an appointed third party, and details on the scope, modalities 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 reduce the risk of disruptions at the financial entity or to ensure its effective resolution and restructuring;

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

By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that 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.

3. 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.

4. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when subcontracting critical or important functions to properly give effect to the provisions of point (a) of paragraph 2.

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

The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 18 months after the date of entry into force].

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 1095/2010 and (EU) No 1094/2010, respectively.

SECTION II

OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS

Article 28

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 29(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 point (a) of paragraph 1 shall be based on all of the following criteria in relation to ICT services provided by an ICT third-party service provider:

   (a) the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant ICT third-party 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 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, by means or 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 to partially or fully migrate the relevant data and workloads from the relevant to another ICT third-party service provider, due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration.

2a. 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.

2b. Critical ICT third-party service providers which are part of a group shall designate one legal person as coordination point to ensure adequate representation and communication with the Lead Overseer.

2c. The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment leading to designation referred in point (a) of paragraph 1.
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.

After designating a 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 be effective subject to oversight activities. Such date shall be established 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.

3. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 and in point (iii) of paragraph 5 by [OJ: insert date 18 months after the date of entry into force].

4. The designation mechanism referred to in point (a) of paragraph 1 shall not be used until the Commission has adopted a delegated act in accordance with paragraph 3.

5. The designation mechanism referred to in point (a) of paragraph 1 shall not apply in relation to:

(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.

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

7. For the purposes of point (a) of paragraph 1, competent authorities shall transmit, on a yearly and aggregated basis, the reports referred to in Article 25(4), third subparagraph, to the Oversight Forum established pursuant to Article 29. The Oversight Forum shall assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.

8. The ICT third-party service providers that are not included in the list referred to in paragraph 6 may request to be designated as critical in accordance with point a of paragraph 1.

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 point (a) of paragraph 1.

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.

9. Financial entities shall only make use of the services of an ICT third-party service provider established in a third country which has been designated as critical pursuant to paragraph 1 if the latter has established a subsidiary in the Union within 12 months following the designation.

9a. The critical ICT third-party service provider referred to in paragraph 9 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.

Article 29

Structure of the Oversight Framework

1. The Joint Committee, in accordance with Article 57(1) of Regulation (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 the Lead Overseer referred to in point (b) of Article 28(1) in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and common acts of the Joint Committee in that area.

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

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 of critical ICT third-party service providers to be adopted by the Joint Committee as joint positions of the ESAs in accordance with Articles 56(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

3. 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 41 from each Member State;

(c) the Executive Directors of each ESA and one representative from the European 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 41 from each Member State as observer;

(e) where applicable, one representative of the national competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or a digital service provider listed in Annex III of that Directive, respectively, 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 3b.

3a. Each Member State shall designate the relevant competent authority whose staff member shall be the high-level representative referred in point (b) of paragraph 3 and shall inform the Lead Overseer thereof.

The ESAs shall publish on their website the list of high-level representatives designated by Member States.

3b. The independent experts referred to in paragraph 3 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 on financial stability, digital operational resilience and ICT security matters.

The independent expert 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.

4. In accordance with Article 16 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs shall by [OJ: insert date 18 months after the date of entry into force] issue guidelines on the cooperation between the ESAs and the competent authorities for the purposes of this Section on the detailed procedures and conditions relating to the execution of tasks between competent authorities and the ESAs and details on exchanges of information needed by competent authorities to ensure the follow-up of recommendations addressed by Lead Overseer pursuant to point (d) of Article 31(1) to critical ICT third-party providers.

5. The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2016/1148 and of other Union rules on oversight applicable to providers of cloud computing services.

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

Article 30

Tasks of the Lead Overseer

1. The Lead Overseer, appointed under Article 28(1), point (b), shall conduct the oversight of the assigned critical ICT third-party service providers and shall be the primary point of contact for those critical ICT third-party service providers.

1a. For the purposes of the first subparagraph, 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 risks which it may pose to financial entities.
That assessment shall mainly focus on ICT services provided by the critical ICT third-party service provider which support the critical or important functions of financial entities and where needed to address all relevant risks, the assessment shall extend to ICT services supporting functions other than critical or important ones.

2. The assessment referred to in paragraph 1a shall include:

(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 confidentiality, integrity and availability of data;

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

(c) the risk management processes, including ICT risk management policies, ICT business continuity 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 an effective ICT risk management;

(e) the identification, monitoring and prompt reporting of major ICT-related incidents to the 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.

3. Based on the assessment referred to in paragraph 1a, and following coordination with the Joint Oversight Network, the Lead Overseer shall adopt a clear, detailed and reasoned individual Oversight plan describing the annual oversight objectives and the main oversight actions foreseen for each critical ICT third-party service provider. That plan shall be communicated each year to the critical ICT third-party service provider.

Prior to 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 expected impact on customers not subject to this Regulation and where appropriate, formulating solutions to mitigate risks.

4. Once the annual Oversight plans referred to in paragraph 3 have been adopted and notified to the critical ICT third-party service providers, competent authorities may only take measures concerning critical ICT third-party service providers in agreement with the Lead Overseer.

Article 30a

Operational coordination between Lead Overseers

1. To ensure a consistent approach to oversight, the three Lead Overseers designated in accordance with point (b) of Article 28(1) shall set up a Joint Oversight Network (JON) to coordinate among themselves in the preparatory stages and the conduct of Oversight activities over their respective overseen critical ICT third-party service providers, as well as on any course of action that may be needed pursuant to Article 37, with a view to enable coordinated general oversight strategies and cohesive operational approaches and work methodologies.

2. For the purpose of the first paragraph, the Lead Overseers shall draw up a common Oversight protocol specifying the detailed modalities 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, notably the evolving oversight practical 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 Joint Oversight Network.

Article 31

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:

   (a) to request all relevant information and documentation in accordance with Article 32;

   (b) to conduct general investigations and inspections in accordance with Articles 33 and 34;

   (c) to request reports after the completion of the Oversight activities 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 address recommendations on the areas referred to in Article 30(2), in particular concerning the following:

      (i) the use of specific ICT security and quality requirements or processes, notably 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 services to financial entities, which the Lead Overseer deems relevant for preventing the generation of single points of failure, or the amplification thereof, or for minimising possible systemic impact across the Union's financial sector in case of ICT concentration risk;

(iii) upon the examination undertaken in accordance with Articles 32 and 33 of subcontracting arrangements, including subcontracting arrangements which the critical ICT third-party service providers plan to undertake with other ICT third-party service providers or with ICT subcontractors established in a third country, any planned subcontracting, including subcontracting, where the Lead Overseer deems that further subcontracting may trigger risks for the provision of services by the financial entity, or risks to the financial stability;

(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 a critical or important function of the financial entity;
- 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 the latter to comply with supervisory requirements.

For the purpose of point (iv), ICT third-party service providers shall transmit to the Lead Overseer the information regarding subcontracting using the template referred to in Article 36 (1)c).

1a. When exercising the powers referred to in this Article, the Lead Overseer shall:
(a) ensure regular coordination with the Joint Oversight Network, and in particular seek as appropriate consistent approaches with regard to the oversight of critical ICT third-party service providers;
(b) take due account of the framework established by Directive (EU) 2016/1148 and, where necessary, consult the relevant competent authorities established by 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 the critical ICT third-party service providers to customers not subject to this Regulation.

2. 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, the Lead Overseer shall give the opportunity to the ICT third-party service provider to provide within 30 calendar days relevant information evidencing expected impact on customers not subject to this Regulation and where appropriate, formulating solutions to mitigate risks.

2a. The Lead Overseer shall inform the Joint Oversight Network of the outcome of the exercise of the powers referred to points (a) and (b) of paragraph 1.
The Lead Overseer shall, without undue delay, transmit the reports referred in point (c) of paragraph 1 to the Joint Oversight Network and the competent authorities of the financial entities using that critical ICT third-party service provider.

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

3a. Where the Lead Overseer is not able to exercise oversight activities on premises located in a third-country, as referred to in Article 31a, it shall:
(a) exercise its powers on the basis of all facts and documents available,

(b) document and explain any consequence of its inability to conduct the envisaged oversight activities as referred to in Article 31a.
These potential consequences shall be considered in the Lead Overseer's recommendations issued pursuant to Article 31 (1) (d).

4. In the case of whole or partial non-compliance with the measures required to be taken in accordance with points (a) to (c) of paragraph 1, 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.

5. The periodic penalty payment referred to in paragraph 4 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification to the critical ICT third-party service provider.

6. 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 the non-compliance with the measures referred in paragraph 4:
(i) the gravity and the duration
(ii) whether it has been committed intentionally or negligently;
(iii) the level of cooperation of the ICT third-party service provider with the Lead Overseer;
To ensure a consistant approach, the Lead Overseer shall engage in consultation within the Joint Oversight Network for the purposes of subparagraph 1.

7. 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.

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

9. Before imposing a periodic penalty payment under paragraph 4, 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 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. They shall be entitled to have access to 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 Lead Overseer's internal preparatory documents.

Article 31a

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 28(9) or by exercising oversight activities on premises located in the Union, the Lead Overseer may exercise 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, services, including any administrative, business, operational offices, premises, lands, buildings or other properties, the powers referred to in:

(a) Article 31(1)(a); and
(b) Article 31(1)(b) pursuant to the conditions foreseen in points (a), (b) and (d) of Article 33(2) and, respectively, in Article 34(1) and point (a) of Article 34(2).

Those powers referred to in subparagraph 1 may be exercised subject to all of the following conditions:
(i) the conduction 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 conduction 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.

3. Without prejudice to the respective competences of the Member States and the Union institutions, for the purposes of paragraph 1, EBA, ESMA or EIOPA, respectively, shall conclude with the relevant authority of the third-country concerned administrative cooperation arrangements enabling the smooth conduct of inspections in a third-country by the Lead Overseer and its designated team for its mission in the third country. Those 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. The cooperation arrangements referred to in the first subparagraph shall specify at least the following elements:

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

(b) the mechanism for the transmission of any relevant information between EBA, ESMA or EIOPA, respectively, 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 32;

(c) the mechanisms for the prompt notification by the relevant authority of the third-country concerned to EBA, ESMA or EIOPA, respectively, of cases where an ICT third-party service provider established in a third-country and designated as critical in accordance with point (a) of Article 28(1) is deemed to have infringed requirements to which is obliged to adhere pursuant to the applicable law of a third-country when providing services to financial institutions in the respective third-country, as well as the remedies and sanctions 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 to the inspections conducted by the Lead Overseer and the designation team.

Article 32

Request for information

1. The Lead Overseer may by simple request or by decision require the 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 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 that in case 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 31(4) 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);

   (f) indicate the right to appeal the decision before 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 respectively.

4. Representatives of 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 critical ICT third-party providers' services and to the Joint Oversight Network.

Article 33

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 35(1), may conduct the necessary investigations of critical ICT third-party service providers:

2. The Lead Overseer shall be empowered 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, procedures and 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 31(4) where the production of the required records, data, 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 31(4), 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 investigation, the Lead Overseer shall inform competent authorities of the financial entities using that critical ICT third-party service provider of the investigation and of the identity of the authorised persons.
The Lead Overseer shall communicate to the Joint Oversight Network all information received pursuant to paragraph 5.

Article 34

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 35(1), may enter and conduct all necessary on-site 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-line inspections.
For the purposes of exercising the powers referred to in the first subparagraph, the Lead Overseer shall consult the Joint Oversight Network.

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.

They 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 31(4) where the representatives of the critical ICT third-party service providers concerned do not submit to the inspection.

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

5. Before any planned on-site inspection, the Lead Overseer shall give a 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, appoint the date on which it is to begin and indicate the periodic penalty payments provided for in Article 31(4), 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 terminate the contractual arrangements concluded with that critical ICT third-party service provider.

Article 35

Ongoing Oversight

1. Where conducting oversight activities notably 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 services;

   (c) the national competent authority referred to in Article 29(3)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 and operational risk. The joint examination team shall work under the coordination of a designated Lead Overseer staff member (the 'Lead Overseer coordinator').

3.

4. Within 3 months after the completion of an investigation or inspection, the Lead Overseer, after consultation of the Oversight Forum, shall adopt recommendations to be addressed by the Lead Overseer to the critical ICT third-party service provider pursuant to the powers referred to in Article 31.

5. The recommendations referred to in paragraph 4 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 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 36

Harmonisation of conditions enabling the conduct of the Oversight

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

(a) the information to be provided by a critical ICT third-party service provider in the application for a voluntary opt-in set out in Article 28(8);

(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 31(1), including the template to provide information on subcontracting arrangements;

(c)

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

(d) the details of the competent authorities' assessment of measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer pursuant to Article 37(2).

2. The ESAs shall submit those draft regulatory technical standards to the Commission by 1 January 20xx [OJ: insert date 18 months after the date of entry into force].

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 the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.

Article 37

Follow-up by competent authorities

1. Within 60 calendar days after the receipt of the recommendations issued by the Lead Overseer pursuant to point (d) of Article 31(1), critical ICT third-party service providers shall either notify the Lead Overseer on 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 competent authorities of the financial entities concerned.

1a. 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 in case the explanation provided by the critical ICT third-party service provider is not deemed as 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. It shall be limited to what is relevant and proportionate for the purpose of ensuring public awareness, unless such publication causes 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 the envisaged public disclosure pursuant the first subparagraph.

2. Competent authorities shall inform relevant financial entities of the risks identified in the recommendations addressed to critical ICT third-party service in accordance with point (d) of Article 31(1).
When managing ICT third-party risk, financial entities shall take into account the risks referred to in the first subparagraph.

2a. 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, pursuant to paragraph 3, in the absence of appropriate contractual arrangements aimed at addressing such risks.

2b. Upon receiving the reports referred to in point (c) of Article 31(1), and prior to taking any of the decisions referred to in paragraph 3, competent authorities may, on a voluntary basis, consult the national competent authorities designated under Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or digital service provider listed in Annex III of that Directive which has been designated as a critical ICT third-party service provider.

3. Competent authorities may, as a measure of last resort, following the notification and, if appropriate, the consultation as set out in paragraph 2a and 2b, in accordance with Article 44, require financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party 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.

3a. Where a refusal by a critical ICT third-party provider to endorse recommendations is grounded on a divergent approach from the one advised by the Lead Overseer, and this may adversely impact a large number of financial entities, or a significant part of a financial sector providing critical or important functions, 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 to promote consistent and convergent supervisory follow-up measures, as appropriate.

4. Upon receiving the reports referred to in point (c) of Article 31(1), competent authorities, when taking the decisions referred to in paragraph 3, 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 financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;

(d) whether the non-compliance has been committed intentionally or negligently.

(da) whether the suspension or termination introduces a continuity risk for the business operations of the financial entity nothwistanding the latter's efforts to avoid disruption in the provision of its services;

(e) where applicable, the opinion of the national competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or a digital service provider listed in Annex III of that Directive, respectively, which has been designated as a critical ICT third-party service provider, requested on a voluntary basis in accordance with paragraph 2b.

Competent authorities shall grant financial entities the necessary period of time for the latter to adjust the contractual arrangements with critical ICT third-party

service providers to avoid detrimental effects on their digital operational resilience and to allow them to deploy exit strategies and transition plans referred to in Article 25.

4b. The decision referred in paragraph 3 shall be notified to the members of the Oversight Forum referred in letters (a) to (c) of Article 29(3) and the Joint Oversight Network.

The critical ICT third-party service providers impacted by the decisions provided for in paragraph 3 shall fully cooperate with the affected financial entities in particular in the context of the process of suspension or termination of their contractual arrangements.

5. 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 taken by the latter where critical ICT third-party service providers have not endorsed in part or entirely recommendations addressed by the Lead Overseer.

5a. The Lead Overseer may, upon request, provide further clarifications on the recommendations to guide the competent authorities on the follow up measures.

Article 38

Oversight fees

1. The Lead Overseer shall, in accordance with the delegated act referred to in paragraph 2, 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 35, as well as including the cost of advice provided by the independent experts as referred to in the second subparagraph of Article 29(3) 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 foreseen in this Section and shall be proportionate to their turnover.

2. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid [OJ: insert date 18 months after the date of entry into force].

Article 39

International cooperation

1. Without prejudice to Article 31a, EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, notably 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, focussing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection or the functioning of the single market.

CHAPTER VI

INFORMATION SHARING ARRANGEMENTS

Article 40

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 at enhancing 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 defensive 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[20] and guidelines on competition policy[21].

---

[20] In accordance with 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).

[21] Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01.

2. For the purpose of point (c) of paragraph 1, 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 the latter 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 the latter takes effect.

CHAPTER VII

COMPETENT AUTHORITIES

Article 41

Competent authorities

Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Section II of Chapter V of this Regulation, compliance with the obligations set out in 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, the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, including for institutions exempted under Directive 2013/36/EU 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)

(d) for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034;

(e) for crypto-asset service providers as authorized under MiCA and issuers of asset-referenced tokens, the competent authority designated in accordance with Article 81 of [Regulation (EU) 20xx MICA Regulation];

(f) for central securities depositories, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;

(g) for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;

(h) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU; respectively the competent authority as defined in point (18) of Article 2(1) of Regulation (EU) No 600/2014;

(i) for trade repositories, the competent authority designated in accordance with Article 55 of Regulation (EU) No 648/2012;

(j) for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;

(k) for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;

(l) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;

(m) for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;

(n) for institutions for occupational retirement provision, the competent authority designated in accordance with Article 47 of Directive 2016/2341;

(o) for credit rating agencies, the competent authority designated in accordance Article 21 of Regulation (EC) No 1060/2009;

(p)

(q) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of Regulation (EU) 2016/1011;

(r) for crowdfunding service providers, the competent authority designated in accordance with Article 29 of Regulation(EU) 2020/1503;

(s) for securitisation repositories, the competent authority designated in accordance with Article 10 and 14 (1) of Regulation (EU) 2017/2402.

Article 42

Cooperation with structures and authorities established by Directive (EU) 2016/1148

1. To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs and the competent authorities may participate in the work 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 work of the Cooperation Group for matters in relation to entities listed under point (7) of Annex II to Directive (EU) 2016/1148 that have also been designated as critical ICT third-party service providers pursuant to Article 28 of this Regulation.

2. Where appropriate, competent authorities may consult and share information with the single point of contact and the national Computer Security Incident Response Teams referred to respectively in Articles 8 and 9 of Directive (EU) 2016/1148.

3. Where appropriate competent authorities may request any relevant technical advice and assistance from the competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 and establish cooperation arrangements to allow the set-up of effective and fast-response coordination mechanisms.

3a. The arrangements referred to in paragraph 3 may, amongst other, specify the procedures for the coordination of supervisory and oversight activities, respectively, in relation to operators of essential services listed under point (7) of Annex II or digital service providers listed in Annex III of the Directive (EU) 2016/1148 which have been designated as critical ICT third-party service providers pursuant to Article 28, including for the conduct, in accordance with national law, of investigations and on-site inspections, as well as mechanisms for the exchange of information between competent authorities and authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 which include access to information requested by the latter authorities.

Article 42a

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 the respective duties resulting from this Regulation, notably in relation to identified risks, approaches and measures taken as part of the Lead Overseer's oversight tasks.

Article 43

Financial cross-sector exercises, communication and cooperation

1. The ESAs, through the Joint Committee and in collaboration with competent authorities*, national resolution authorities as referred to in Article 3 of Directive (EU) No 2014/59*, the ECB, the Single Resolution Board in respect of 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 develop communication channels and gradually enable an effective EU-level coordinated response 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.

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

2. Competent authorities, EBA, ESMA or EIOPA and the ECB shall cooperate closely with each other and exchange information to carry out their duties pursuant to Articles 42 to 48. 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 44

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 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;

(ba) For the purpose of point b, in particular but not limited to:
i) summon 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) 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;

(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 according to Article 46, 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 the conduct 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 a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;

(d) require, in so far 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 the provisions referred to in point (c) of paragraph 2 and in 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 point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.

Article 45

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 44 in accordance with their national legal frameworks, as appropriate:

   (a) directly;

   (b) in collaboration with other authorities;

   (c) under their responsibility by delegation to other authorities;

   (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 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, 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 person;

(g) previous breaches by the responsible natural or legal person.

Article 46

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 47

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 [OJ: insert date 24 months after the date of entry into force]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.

Article 48

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 sanction 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 of individuals, jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt either of the following solutions in respect to the decision imposing an administrative sanction:

   (a) defer its publication until the moment where 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 proportional with the leniency of the imposed sanction.

4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with point (b) of paragraph 3, 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 49

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 under 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 and competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148, 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 under 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 49a

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 under 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 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 case of pending court proceedings requiring further retention of such data.

CHAPTER VIII

DELEGATED ACTS

Article 50

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 28(3) and 38(2) shall be conferred on the Commission for a period of five years from [PO: insert date 12 months after the date of entry into force of this Regulation]. 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 28(3) and 38(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 28(3) and 38(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 51

Review clause

By [PO: insert date 5 years after the date of entry into force of this Regulation], the Commission shall, after consulting EBA, ESMA, EIOPA, and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council, accompanied, if appropriate, by a legislative proposal. The report shall review at least the following:

(a) the criteria for the designation of critical ICT third-party service providers in Article 28(2);

(b) the voluntary nature of the notification of significant cyber threats;

(c) the regime referred to in Article 28(9) of this Regulation and the powers of the Lead Overseer provided for in the first indent of Article 31(1) d) (iv), with a view to evaluating the effectiveness of these provisions in ensuring effective oversight of critical third-country ICT third-party service providers, and the necessity to establish a subsidiary in the Union.

This review shall entail an analysis of this regime, including in terms of access for European financial entities to services from third countries and availability of services on the European 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 the application and, respectively, supervision of this regime, and any relevant regulatory and supervisory developments taking place at international level.

(d) in light of future market developments on the use of automated sales systems, the appropriateness of including in the scope of this Regulation financial entities referred to in point (e) of Article 2(3) making use of such systems;

(e) the functioning and effectiveness of the Joint Oversight Network in supporting consistency of the oversight and the efficiency of the exchange of information within the oversight framework.

In the context of the review of Directive 2015/2366 (PSD2), the Commission shall assess the need for increased cyber resilience of payment systems and payment-processing activities and the appropriateness of extending of 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 the Directive 2015/2366, a report to the Council and the EP no later than [PO: insert date 6 months after the date of entry into force].

Based on this review report and after consulting EBA, ESMA, EIOPA, ECB and the ESRB, the Commission may submit, if appropriate and as part of the legislative proposal that it may adopt to revise PSD2, 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 central bank oversight.

No later than [PO: 3 years after the date of entry into force], after consultation of the European Supervisory Authorities and the Committee of European Auditing Oversight Bodies, the Commission shall report to the European Parliament and the Council about the appropriateness of strengthened requirements as regards the digital operational resilience for statutory auditors and audit firms, by means of inclusion into the scope of this Regulation or through amendments to Directive 2006/43/EC, together with a legislative proposal if appropriate.

SECTION II

AMENDMENTS

Article 52

Amendments to Regulation (EC) No 1060/2009

In Annex I to Regulation (EC) No 1060/2009, the first subparagraph of point 4 of Section A 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) 2021/xx of the European Parliament and of the Council* [DORA].

* Regulation (EU) 2021/xx of the European Parliament and of the Council […] (OJ L XX, DD.MM.YYYY, p. X).

In Annex III to Regulation (EC) No 1060/2009, 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) 2021/xx of the European Parliament and of the Council* [DORA]*;* or by not implementing or maintaining decision-making procedures or organisational structures as required by that point.‘

Article 53

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) 2021/xx of the European Parliament and of the Council* [DORA].

* Regulation (EU) 2021/xx of the European Parliament and of the Council […](OJ L XX, DD.MM.YYYY, p. X).;‘

(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 response and recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring 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:

‘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, the first subparagraph of paragraph 3 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) 2021/xx [DORA].

2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity policy and response and recovery plans established in accordance with Regulation (EU) 2021/xx[DORA], aiming at ensuring 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.

(5a) In Annex I to Regulation (EC) No 648/2012, Section II is amended as follows:

(a) Points (a) and (b) are replaced as follows:

"(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) 2021/xx of the European Parliament and of the Council*;

(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) 2021/xx [DORA], aimed at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations;"

(b) Point (c) is deleted.

(5b) Annex III to Regulation (EC) No 648/2012 is amended as follows*:*

(a) In Section II, 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) 2021/xx (DORA) of the European Parliament and of the Council*;

(b) In Section II, point (f) is deleted.

(c) 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) 2021/xx [DORA], aimed at ensuring 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 54

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) 2021/xx of the European Parliament and of the Council*[DORA], 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) 2021/xx of the European Parliament and of the Council […](OJ L XX, DD.MM.YYYY, p. X).;‘

(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 and disaster recovery plan, including ICT business continuity policy and ICT response and recovery plans established in accordance with Regulation (EU) 2021/xx [DORA], 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 of 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 paragraphs (5) and (7) of Article 11 of Regulation (EU) 2021/xx [DORA].;'

(4) paragraph 6 is replaced by the following:

'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:

'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 risks, 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 55

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 as follows:

4. ‘An APA shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].‘’.

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

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

(2) Article 27h is amended as follows:

(a) paragraph 5 is replaced as follows:

‘A CTP shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].’.

(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 as follows:

‘An ARM shall comply with the requirements concerning the security of network and information systems set out in Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].’.

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

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

Article 55a

Amendments to Regulation (EU) No 2016/1011

In Article 6 of Regulation (EU) No 2016/1011, a new paragraph is added as follows:

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) 2021/xx of the European Parliament and of the Council* [DORA].

Article 56

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 [PO: insert date 24 months after the date of entry into force].

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*