EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- Reasons for and objectives of the proposal

This proposal is part of the Digital finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. It is in line with the Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. The digital finance package includes a new Strategy on digital finance for the EU financial sector with the aim to ensure that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to European consumers and businesses. In addition to this proposal, the package also includes a proposal for a pilot regime on distributed ledger technology (DLT) market infrastructure, a proposal for digital operational resilience, and a proposal to clarify or amend certain related EU financial services rules.

Digitalisation and operational resilience in the financial sector are two sides of the same coin. Digital, or Information Communication Technologies (ICT), gives rise to opportunities as well as risks. These need to be well understood and managed, especially in times of stress.

Policymakers and supervisors have therefore increasingly focused on risks stemming from reliance on ICT. They have notably tried to enhance firms' resilience through the setting of standards and through the coordination of regulatory or supervisory work. This work has been carried out at both international and European level, and both across industries and for a number of specific sectors, including financial services.

ICT risks nevertheless continue to pose a challenge to the operational resilience, performance and stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience[1] of the EU financial sector, only addressing ICT risks indirectly in some areas, as part of measures to address operational risks more broadly.

While the post-crisis changes to the EU financial services legislation put in place a Single Rulebook governing large parts of the risks associated with financial services they did not fully address digital operational resilience. The measures taken were associated with a number of features limiting their effectiveness. For example, they often remain subject to minimum harmonisation, leaving substantial room for diverging approaches across the Single Market. Furthermore, there has been only some limited or incomplete focus on ICT risks in the context of the operational risk coverage. Finally, these measures vary across the sectoral financial services legislation. Thus the intervention at Union level did not fully match what European financial entities needed also in terms of legal requirements on specific ICT operational risks to be able to withstand, respond and recover from impacts of ICT incidents, nor did it provide financial supervisors with the most adequate tools to fulfil their mandates to contain financial instability stemming from the materialization of those ICT risks.

The absence of comprehensive rules on digital operational resilience at EU level has led to the proliferation of national initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies). Action at Member

[1] The different measures adopted aimed to increase the capital position, liquidity, reduce market and credit risk for financial entities, etc.

State level only has a limited effect, given the cross-border nature of ICT risks. Moreover, the uncoordinated nature of the national initiatives has resulted in overlaps or inconsistencies, duplicative requirements, high administrative and compliance costs - especially for cross-border financial entities - or in ICT risks remaining undetected and hence unaddressed. This may fragment the single market and so undermine the stability and integrity of the EU financial sector, as well as the protection of consumers and investors.

It is therefore necessary to put in place a comprehensive framework on digital operational resilience for EU financial entities. This framework will deepen the management of the digital risk dimension of the Single Rulebook, in particular by enhancing and streamlining the financial entities' conduct of ICT risk management, by mandating a thorough testing of ICT systems, by increasing supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as by introducing powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers. The proposal will create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities, and strengthen supervisory effectiveness.

- Consistency with existing provisions in the policy area

This proposal is part of wider work ongoing at European and international level to strengthen the cybersecurity in financial services and address broader operational risks.[2]

It also responds to the 2019 Joint technical advice[3] of the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance and recommended the Commission to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through an EU sector-specific initiative. The ESAs advice was a response to the Commission's 2018 Fintech action plan.[4]

- Consistency with other Union policies

As stated by President von der Leyen in her Political Guidelines,[5] and set-out in the Communication 'Shaping Europe's digital future',[6] it is crucial for Europe to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries. The European strategy for data[7] sets out four pillars - data protection, fundamental rights, safety and cybersecurity - as essential pre-requisites for a society empowered by the use of data. A legislative framework strengthening the digital operational resilience of EU financial entities is consistent with these policy objectives. The proposal would also support policies aimed at recovering from the coronavirus, as it would ensure that increased reliance on digital finance goes hand in hand with operational resilience.

The initiative would maintain the benefits associated with the horizontal framework on cybersecurity (e.g. the Directive on Security of Networks and Information Systems, NIS

---

2 Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices*, December 2018 and *Principles for sound management of operational risk (PSMOR)*, October 2014.

3 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019).

4 European Commission, *Fintech Action Plan*, COM/2018/0109 final.

5 President Ursula Von Der Leyen, Political Guidelines for the next European Commission, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, *Shaping Europe's Digital Future*, COM(2020) 67 final.

7 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, *A European strategy for data*, COM(2020) 66 final.

Directive) by keeping the financial sector within its scope. The financial sector would remain associated to the NIS cooperation body and financial supervisors would be able to exchange relevant information within the existing NIS ecosystem. The initiative would be consistent with the European Critical Infrastructure (ECI) Directive, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructures against non-cyber related threats.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- Legal basis

The proposal for regulation is based on Article 114 TFEU and is accompanied by a proposal for directive based on Article 53(1) TFEU.

It removes obstacles to, and improves the establishment and functioning of the internal market for financial services by harmonising the applicable rules. The current disparities in the area of ICT risk management, reporting, testing and ICT third-party risk, both at legislative and supervisory levels, as well as national and EU levels, act as obstacles to the single market in financial services. Financial entities engaging in cross-border activities face different, at times overlapping, regulatory requirements or supervisory expectations with the potential to impede their exercise of freedom of establishment and provision of services. Different rules also distort competition between the same type of financial entities in different Member States. Moreover, in areas where harmonisation is absent, partial or limited (notably digital operational testing frameworks, oversight of activities of critical ICT third-party service providers), the development of divergent national rules or approaches, either already in force or in the process of adoption and implementation at national level, could act as deterrents to the single market freedoms for financial services.

- Subsidiarity

A high degree of interconnection across financial services, a significant cross-border activity of financial entities and an extensive dependency of the financial sector as a whole on ICT third-party service providers call for enabling a strong digital operational resilience as a matter of common interest to uphold the soundness of EU financial markets. Disparities resulting from uneven or partial regimes, overlaps and/or multiple requirements applying to the same financial entities operating cross-border and/or holding several authorisations[8] across the Single Market can only be tackled efficiently at Union level.

The initiative would harmonise the digital operational component of a deeply integrated and interconnected sector that already benefits from a single set of rules and supervision in most other key areas. For matters such as ICT-related incident reporting, only Union harmonised rules could reduce the level of administrative burdens and financial costs associated with the reporting of the same ICT-related incident to different Union and/or national authorities. EU action is needed to also facilitate the mutual recognition of advanced digital operational resilience testing results for entities operating cross-border, which are or may be subject to different frameworks in different Member States. The differences in testing approaches may also distort competition, as ICT risks are only properly mitigated in Member States that have introduced specific testing obligations. EU-wide action is also needed to address the lack of

[8] The same financial entity may have a banking, an investment firm, and payment institution licence, each issued by a different supervisor in one or several Member States.

appropriate oversight powers to monitor risks stemming from ICT third-party service providers, including concentration and contagion risks for the EU financial sector.

- Proportionality

The proposed rules will not go beyond what is necessary in order to achieve the objectives of the proposal. They will cover only the aspects that Member States cannot achieve on their own and where the administrative burden and costs are commensurate with the specific and general objectives to be achieved.

Proportionality is designed in terms of scope and intensity, through the use of qualitative and quantitative assessment criteria. These aim to ensure that, while the new rules cover all financial entities, they are at the same time tailored to risks and needs of specific entities, as well as to their size and business profiles. Proportionality will be embedded to different degrees in the rules on ICT risk management, digital resilience testing, reporting of major ICT-related incidents and oversight of CTPPs.

- Choice of the instrument

The measures are implemented through a Regulation and a Directive. The regulation lays down key rules governing ICT risk management, ICT-related incident reporting, testing and oversight. As the proposal amends several Directives of the European Parliament and of the Council adopted on the basis of Article 53(1) of the TFEU, a proposal for a Directive is therefore required to amend these Directives.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- Ex-post evaluations/fitness checks of existing legislation

No EU financial services legislation has until now focussed on operational resilience and none comprehensively tackled risks emerging from digitalisation, not even those rules which addressed more generally the operational risk dimension with ICT risk as a sub-component.

EU action greatly delivered on its objectives to ensure financial stability and establish a single set of harmonised prudential and market conduct rules which financial entities throughout the EU today respect. Those targets have largely been met.

Therefore, an evaluation exercise is difficult to carry out when factors driving progress did not include comprehensive rules preparing for, monitoring and dealing with operational disruptions based on a widespread use of technology.

- Stakeholder consultations

The Commission has consulted stakeholders throughout the process of preparing this proposal, in particular:

i) The Commission carried out a dedicated open public consultation (19 December 2019 - 19 March 2020);[9]

[9] [*Add reference*] Public consultation and the IIA

ii) The Commission consulted the public via an inception impact assessment (19 December 2019 - 16 January 2020);[10]

iii) The Commission services consulted Member State experts in the Expert Group on Banking, Payments and Insurance (EGBPI) on two occasions (18 May 2020 and 16 July 2020);[11]

iv) The Commission services held a dedicated webinar on digital operational resilience, as part of the Digital Finance Outreach 2020 series of events (19 May 2020).

The purpose of the public consultation was to inform the Commission on the development of a potential EU cross-sectoral digital operational resilience framework in the area of financial services. Responses showed a broad support for introducing a dedicated framework with actions focused on the four areas subject to the consultation, while stressing the need to ensure proportionality and to carefully address and explain the interaction with the horizontal rules of the NIS Directive. The Commission received two responses on the inception impact assessment, where respondents addressed specific aspects related to their area of activity.

Member States expressed in the EGBPI meeting organized on 18 May 2020 high support for strengthening the digital operational resilience of the financial sector through the actions envisaged along the four elements outlined by the Commission. Member States also stressed the need for clear articulation of the new rules with those on operational risk (inside the EU financial services legislation) and with the horizontal rules on cybersecurity (NIS Directive). During the second meeting, some Member States stressed the need to ensure proportionality and consider the specific situation of small companies or subsidiaries of larger groups, as well as the need to have a strong mandate for NCAs involved in the oversight.

The proposal also builds on and integrates the feedback drawn from meetings held with stakeholders and EU authorities and institutions. Stakeholders, including ICT third-party service providers, have been overall supportive. An analysis of the received feedback shows a focus on preserving proportionality and following a principle and risk-based approach in the design of all future rules. On the institutional side, main input came from the European Systemic Risk Board (ESRB), the ESAs, the European Union Agency on Cybersecurity (ENISA) and the European Central Bank (ECB), as well as from Member States' competent authorities.

- Collection and use of expertise

In preparing this proposal, the Commission relied on qualitative and quantitative evidence collected from recognised sources, including the two joint technical advices by the ESAs. This has been complemented with confidential input, and publicly available reports from supervisory authorities, international standard-setting bodies and leading research institutes, as well as quantitative and qualitative input from identified stakeholders across the global financial sector.

- Impact assessment

This proposal is accompanied by an impact assessment, which was submitted to the Regulatory Scrutiny Board (RSB) on 29 April 2020 and approved on 29 May 2020. The RSB

10 [*Add reference*] IA

11 [*Add reference*] Minute published on the webpage

recommended improvements in some areas with a view to: (i) provide more information on how proportionality would be ensured; (ii) better highlight the extent to which the preferred option differs from the ESAs joint technical advice, and why that option is the optimal one; and (iii) further highlight how the proposal interacts with existing EU legislation, including with rules currently being reviewed. The impact assessment was adjusted to address these points, also addressing the RSB's more detailed comments.

The Commission considered a number of policy options for developing a digital operational resilience framework:

- "Do nothing": rules on operational resilience would continue to be set by the current, diverging set of EU financial services provisions, partly by the NIS Directive, and by existing or future national regimes;
- Option 1 - strengthening capital buffers: an additional capital buffer would be introduced to increase financial entities' ability to absorb losses that could arise due to a lack of digital operational resilience;
- Option 2 - introducing a financial services digital operational resilience act: enabling a comprehensive framework at EU level with consistent rules addressing the digital operational resilience needs of all regulated financial entities;
- Option 3 - a financial services digital operational resilience act combined with centralised supervision of CTPPs: in addition to a digital operational resilience act (option 2), a new authority would be established to supervise the provision of services by ICT third party service providers.

The second option was retained, as it achieves most of the intended objectives in a manner that is effective, efficient and coherent with other Union policies. Most stakeholders also prefer this option.

The retained option would give rise to costs of both one-off and recurring nature (see impact assessment). The former costs are mainly due to investments in IT systems and as such are difficult to quantify given the different state of firms' complex IT landscapes and in particular of their legacy IT systems. Even so, these costs are likely to be limited for large firms, given the significant ICT investments they have already made. Costs are also expected to be limited for smaller firms, as proportionate measures would apply given their lower risk.

The retained option would have positive effects on SMEs operating in the financial services industry in terms of economic, social and environmental impacts. The proposal will bring clarity to SMEs on what rules apply, which will reduce compliance costs.

The main social impacts of the retained policy option would be on consumers and investors. Higher levels of digital operational resilience of the EU financial system would decrease the number and average costs of incidents. Society as a whole would benefit from the increased trust in the financial services industry.

Finally, in terms of environmental impacts, the policy option chosen would encourage an enhanced use of the latest generation of ICT infrastructures and services, which are expected to become environmentally more sustainable.

- Regulatory fitness and simplification

The removal of overlapping ICT-related incident reporting requirements would reduce administrative burdens and decrease associated costs. In addition, harmonised digital operational resilience testing with mutual recognition across the Single Market would decrease costs, especially for cross-border firms that could otherwise face multiple tests across Member States (see impact assessment).

- Fundamental rights

The EU is committed to ensuring high standards of protection of fundamental rights. In this context, the proposal is not likely to have a direct impact on those rights, as listed in the Charter of Fundamental Rights of the European Union.

4. BUDGETARY IMPLICATIONS

In terms of budgetary implications, as the current Regulation foresees an enhanced role for the ESAs by means of powers granted upon them to adequately oversee critical ICT third-party providers, the proposal would entail the deployment of increased resources, in particular to fulfil the oversight missions (such as onsite and online inspections and audits exercises) and the use of staff possessing specific ICT security expertise.

The scale and distribution of these costs will depend on the extent of the new oversight powers and the (precise) tasks to be performed by the ESAs. In terms of providing new staff resources, EBA, ESMA and EIOPA will require in total 15 full-time employees (FTE) - 5 FTEs for each authority - when the different provisions of the proposal will enter into application (estimated at EUR 13,1 million for the period 2022 - 2027). The ESAS will also incur additional IT costs, mission expenses for the onsite inspections and translation costs (estimated at EUR 12 million for the period 2022 - 2027), as well as other administrative expenditure (estimated at EUR 2,06 million for the period 2022 - 2027). Therefore, the estimated total cost impact is approximately EUR 27, 16 million for the period 2022 - 2027.

It should also be noted that, while the headcount (e.g. new staff members and other expenditure related to the new tasks) necessary for direct oversight will depend over time on the development of the number and size of the critical ICT third-party service providers to be overseen, the respective expenditure will be fully funded by fees raised from those market participants. Therefore, no impact on EU budget appropriations is foreseen (except for the additional staff), as these costs will be fully funded by fees.

The financial and budgetary impacts of this proposal are explained in detail in the legislative financial statement annexed to this proposal.

5. OTHER ELEMENTS

- Implementation plans and monitoring, evaluation and reporting arrangements

The proposal includes a general plan for monitoring and evaluating the impact on the specific objectives, requiring the Commission to carry out a review at least three years after the entry into force, and to report to the European Parliament and the Council on its main findings.

The review is to be conducted in line with the Commission's Better Regulation Guidelines.

- Detailed explanation of the specific provisions of the proposal

The proposal is structured around several main policy areas which are key inter-related pillars consensually included in European and international guidance and best practices aimed at enhancing the cyber and operational resilience of the financial sector.

Scope of the Regulation and proportionality application of required measures (Article 2)

To ensure consistency around the ICT risk management requirements applicable to the financial sector, the Regulation covers a broad range of financial entities, namely credit institutions, payment institutions, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds and management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement pensions, credit rating agencies, statutory auditors and audit firms, administrators of critical benchmarks and crowdfunding service providers.

Such a broad coverage facilitates a homogenous and coherent application of all components of the risk management on ICT-related areas, while safeguards the level playing field among financial entities in respect of their regulatory obligations on ICT risk. At the same time, the Regulation acknowledges that significant differences exist between financial entities in terms of size, business profiles or in relation to their exposure to digital risk. Since larger financial entities enjoy more resources, only financial entities not qualifying as microenterprises shall be required, for instance, to establish complex governance arrangements, dedicated management functions, perform in-depth assessments after major changes in the network and information system infrastructures, regularly conduct risk analyses on legacy ICT systems, expand the testing of business continuity and response and recovery plans to capture switchovers scenarios between primary ICT infrastructure and redundant facilities. Moreover, only financial entities identified as significant for the purposes of the advanced digital resilience testing will be required to conduct threat led penetration tests.

Governance related requirements (Article 4)

This Regulation aims at better aligning financial entities' business strategies and the conduct of the ICT risk management. To that effect, the management body will be required to maintain a crucial, active role in steering the ICT risk management framework and shall pursue the respect of a string cyber hygiene. The full responsibility of the management body in managing financial entity's ICT risk will be an overarching principle to be further translated into a set of specific requirements, such as the assignment of clear roles and responsibilities for all ICT-related functions, a continuous engagement in the control of the monitoring of the ICT risk management, as well in the full range of approval and control processes and an appropriate allocating of ICT investments and trainings.

ICT risk management requirements (Articles 5 to 14)

Digital operational resilience is rooted in a set of key principles and requirements on ICT risk management framework, in line with the joint ESAs technical advice. These requirements, inspired from relevant international, national and industry-set standards, guidelines and recommendations, revolve around specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication). To keep pace with a quickly evolving cyber threat landscape, financial entities are required to set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk, to identify on a continuous basis all sources of ICT risk, to set-up protection and prevention measures, promptly detect anomalous activities, put in place dedicated and comprehensive business continuity policies and disaster and recovery plans as an integral part of the operational business continuity policy. The latter components are required for a prompt recovery after ICT-related incidents, in particular cyber-attacks, by

limiting damage and prioritising safe resumption of activities. The Regulation does not itself impose specific standardization, but rather builds on European and internationally recognized technical standards or industry best practices, insofar they are fully compliant with supervisory instructions on the use and incorporation of such international standards.

ICT-related incident reporting (Articles 15 to 20)

Harmonising and streamlining the reporting of ICT-related incidents is achieved via, first, a general requirement for financial entities to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them based on criteria developed by the ESAs through a common ICT-related incident taxonomy that should specify materiality thresholds. Second, only ICT-related incidents that are deemed major must be reported to the competent authorities. The reporting should be processed using a common template and following a harmonised procedure as developed by the ESAs. Financial entities should submit initial, intermediate and final reports and inform their users and clients where the incident has or may have an impact on their financial interests. Competent authorities should provide pertinent details of the incidents to other institutions or authorities: to the ESAs, to the ECB and to the single points of contact designated under Directive (EU) 2016/1148.

To set off a dialogue between financial entities and competent authorities that would help minimising the impact and identifying appropriate remedies, the reporting of major ICT-related incidents should be complemented by supervisory feedback and guidance.

Lastly, the possibility of centralisation at Union level of ICT-related incident reporting should be further explored in a joint report by the ESAs, ECB and ENISA assessing the feasibility of establishing a single EU Hub for major ICT-related incident reporting by financial entities.

Digital operational resilience testing (Articles 21 to 25)

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. This Regulation allows for a proportionate application of digital operational resilience testing requirements depending on the size, business and risk profiles of financial entities: while all entities should perform a testing of ICT tools and systems, only those identified by competent authorities (based on criteria developed by the ESAs) as significant and cyber mature should be required to conduct advanced testing based on TLPTs. This Regulation also sets out requirements for testers and the recognition of TLPT results across the Union for financial entities operating in several Member States.

ICT third party risk (Articles 26 to 35)

The Regulation aims at ensuring a sound monitoring of ICT third-party risk. This objective will be achieved first through the respect of principle-based rules applying to financial entities' monitoring of risk arising through ICT third-party dependencies. Second, this Regulation harmonises key contractual elements throughout the performance of contracts with ICT third-party providers. These elements cover minimum contractual aspects deemed crucial to enable a complete monitoring by the financial entity of ICT third-party risk throughout the conclusion, performance, termination and post-contractual stages. Most notably, such contracts will be required to contain specifications of complete descriptions of services, indication of locations where data is to be processed, full service level descriptions accompanied by quantitative and qualitative performance targets, relevant provisions on

accessibility, availability, integrity, security and protection of personal data, and guarantees for access, recover and return in the case of failures of the ICT third-party service providers, notice periods and reporting obligations of the ICT third-party service providers, rights of access, inspection and audit by the financial entity or an appointed third-party, clear termination rights and dedicated exit strategies. Moreover, as some of these contractual elements can be standardized, the Regulation promotes a voluntary use of standard contractual clauses which are to be developed for the use of cloud computing service by the Commission.

Finally, the Regulation seeks to promote convergence on supervisory approaches to the ICT-third-party risk in the financial sector by subjecting CTPPs to a Union Oversight Framework. Through a new harmonised legislative framework, the ESAs designated as Lead Overseers for each such CTPP receive powers to ensure that technology services providers fulfilling a critical role to the functioning of the financial sector are adequately monitored on a Pan-European scale. The Oversight Framework envisaged by this Regulation builds on the existing institutional architecture in the financial services area, whereby the Joint Committee of the ESAs ensures cross-sectoral coordination in relation to all maters on ICT risk, in accordance with its tasks on cybersecurity, supported by the relevant Subcommittee (Oversight Forum) carrying out preparatory work for individual decisions and collective recommendations to CTPPs.

Information sharing (Article 36)

To raise awareness on ICT risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques, the Regulation allows financial entities to set-up arrangements to exchange amongst themselves cyber threat information and intelligence.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on digital operational resilience for the Union financial sector and amending Regulation EU/909/2014, Regulation EU/648/2012 and Regulation EC/1060/2009

(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,[12]

Having regard to the opinion of the European Economic and Social Committee,[13]

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In the digital age, information and communications 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, the digital resilience is not yet 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. Digitalization 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, insurance underwriting, claim management and back-office operations. 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[14] how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and

---

12 [*add reference*] OJ C , , p. .

13 [*add reference*] OJ C , , p. .

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

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[15] towards 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 (BCBS), the Committee on Payments and Markets Infrastructures (CPMI), the Financial Stability Board (FSB), the Financial Stability Institute (FSI), as well as G7 and G20 aim to provide competent authorities and market operators across different jurisdictions with tools to bolster the resilience of their financial systems.

Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and the stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the EU financial sector and aimed at safeguarding the EU 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 EU financial services policy and regulatory landscape, or only in a few Member States.

(5) The Commission's 2018 Fintech action plan[16] highlighted the paramount importance of making the EU 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 EU, including under situations of stress, while also preserving consumer and market trust and confidence. In April 2019, the European Supervisory Authorities (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 an EU sector-specific initiative.

(6) 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

---

15 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.

16 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.

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 and enlarging the mandates of financial supervisors tasked to monitor and protect financial stability and market integrity.

(7) The ICT risk requirements for the financial sector are unevenly and incompletely spread over the Union's financial services legislation. In some cases ICT risk is only implicitly addressed. For instance, in the banking services area, Directive 2013/36/EU on access to the activity of credit institutions and the prudential regulation of credit institutions and investment firms (the Capital Requirements Directive, CRD)[17] only sets out general internal governance rules and operational risk provisions which implicitly serve as a basis for addressing ICT risk management, while more detailed yet non-binding expectations have been developed through different sets of EBA Guidelines in relation to the way in which credit institutions, investment firms and payment service providers should manage internal and external ICT risk.

The payment services component, in its dedicated framework (Directive (EU) 2015/2366 on payment services in the internal market, PSD2), went beyond Directive 2013/36/EU through, inter alia, bespoke and explicit rules at the authorisation stage[18] (ICT security controls and mitigation elements), ICT-related provisions in the management of operational and security risk, which have been developed further by EBA guidelines[19] to encompass more specific provisions on ICT incident reporting and separate rules on strong customer authentication.[20]

(8) Elements of ICT risk have also been covered by the Union securities markets legislation, albeit equally unevenly across the relevant subsectors. At the high end, explicit and specific rules on ICT risk apply to central securities depositories and central counterparts through few provisions of Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories (EMIR)[21] and Regulation (EU) No 909/2014 on improving securities settlement in the European Union and on central securities depositories (CSDR)[22] that have been further specified in their respective delegated regulations, while investment firms and trading venues are subject to more stringent rules when performing algorithmic trading according to

---

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

18 This is not however a unique feature to PSD 2. Several other financial services pieces of legislation contain requirements for information pertaining to the IT systems to be reported to supervisors at the stage of authorisation.

19 EBA Guidelines on security measures for operational and security risks of payments services under the revised Payment Services Directive. https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2.

20 Articles 97-98 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (OJ L 337 23.12.2015, p. 35) and related Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJ L 69, 13.3.2018, p. 23).

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

22 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (OJ L 257 28.8.2014, p. 1).

Directive 2014/65/EU on markets in financial instruments (MIFID2).[23] Less granular requirements apply to data reporting services, trade repositories and even much less specific rules apply to managers of alternative investment funds and management companies subject to Directives 2011/61/EU on Alternative Investment Fund Managers (AIFMD)[24] and Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).[25]

For the insurance and re-insurance undertakings, Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)[26] partially captures ICT risk by means of general provisions on governance and risk management addressing ICT risk management capabilities, while certain requirements have been specified through delegated regulations[27] with or without specific references to the ICT risk. Regulation (EC) No 1060/2009 on credit rating agencies[28] covers ICT risk for credit rating agencies through general organisational requirements supplemented by few requirements of a delegated regulation.

Even less specific provisions apply to statutory auditors and audit firms. Directive 2014/56/EU amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts[29] only contains some general provisions on internal organisation with limited references to measures on control and safeguard arrangements for the information processing systems, as well as on the use of appropriate systems, resources and procedures to ensure continuity and regularity.

(9) This Regulation consequently aims first at consolidating and upgrading the ICT risk requirements addressed so far separately in the abovementioned Regulations and Directives. These 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) but could not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk requirements, when further developed in the above mentioned Union legal acts, often favoured a traditional quantitative approach to addressing risk (i.e. setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through

---

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

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

25 Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (OJ L 302, 17.11.2009, p. 32–96).

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

27 Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 12, 17,1 2015, p.1).

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

29 Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (OJ L 158, 27.5.2014, p. 196–226).

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 consolidating exercise, all provisions addressing ICT risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This should fill in the gaps or inconsistencies in some of these legal acts, including in relation to the terminology used therein, and should make explicit references to ICT risk via several targeted rules on ICT risk management capabilities, reporting and testing.

(10) Besides the financial services legislation, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive)[30] is the current general cybersecurity framework at Union level. That Directive also covers three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 sets out a mechanism of identification at national level of operators of essential services, only a limited number of credit institutions, trading venues and central counterparties are in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements thereof.

(11) Moreover, by means of a *lex specialis* clause, EU sector-specific rules take precedence when at least equivalent in objective, nature and effect to the corresponding provisions of Directive (EU) 2016/1148. One year after the entry into force of that Directive, the Commission adopted an interpretative communication[31], which clarified which EU sector-specific acts are *lex specialis*. For the financial sector, Directive (EU) 2015/2366 (PSD2) is *lex specialis* for both the ICT security requirements and incident notification, while Directive 2014/65/EU (MiFID) and Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories (EMIR) are *lex specialis* for the ICT security requirements, thus taking take precedence over the requirements of Directive (EU) 2016/1148.

(12) As this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on the ICT risk management and ICT-related incident reporting that are heightened in respect to those foreseen by the current EU financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, this Regulation would constitute *lex specialis* to Directive (EU) 2016/1148.

(13) There is merit in maintaining a strong relation between the three types of financial entities mentioned above and the Union horizontal cybersecurity framework to ensure full consistency with the cyber security strategies already adopted by Member States, and to allow financial sectors' competent authorities to be made aware of cyber incidents affecting other sectors covered by the Directive (EU) 2016/1148.

(14) To enable a cross-learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (EU) 2016/1148 should remain covered by the 'ecosystem provisions' of that Directive (e.g.

---

30 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. 1–30).

31 Communication from the Commission to the European Parliament and the Council, *Making the most of NIS - towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, COM/2017/0476 final.

NIS Cooperation Group, network of Computer Security Incident Response Teams, CSIRTs). This should take place mainly through the participation of the ESAs referred to under this Regulation to the workings of the NIS Cooperation Group, as well as via exchanges of information and further cooperation between the competent authorities under this Regulation and the single points of contact designated under Directive (EU) 2016/1148. The competent authorities under this Regulation should also consult and cooperate with the national CSIRTs designated in accordance with Article 9 of Directive 2016/1148.

(15) Cloud computing service providers are one category of digital service providers covered by Directive (EU) 2016/1148. As such they are subject to an ex-post supervision carried out by the national authorities designated according to that Directive which is limited to requirements on ICT security and incident notification foreseen by that act. Since the Oversight framework established by this Regulation applies to all critical ICT third-party service providers - cloud computing service providers included - when they provide ICT services to financial entities it should be considered complementary to the supervision that is taking place under Directive (EU) 2016/1148. Moreover, the Oversight Framework set up by this Regulation should cover the cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority entrusted with duties and powers least equivalent to those provided for in this Regulation.

(16) To remain in full control of ICT risks, financial entities need to have in place comprehensive capabilities enabling a strong and effective ICT risk management, alongside specific mechanisms and policies for ICT-related incident reporting, testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. As financial entities are likely to impose heavy costs on the economy in case they suffer ICT disruptions, the Union legislation should require them to respect an essential cyber hygiene. This would raise the digital operational resilience bar for the financial system as a whole, while allowing for a proportionate application of requirements for financial entities qualifying as micro enterprises as defined in Commission Recommendation 2003/361/EC.

(17) 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 like finance 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.[32]

[32] It is estimated that, on average, the costs for a big European bank for developing an internal template for incident reporting would amount to approx. €9.000. The total additional one-off costs for financial institutions is estimated in the range of €9 and €18 million. According to industry data and to the Commission's calculations, the recurring costs associated to managing and reporting incidents are around €18.000/year for a big European banks. Taking as reference this figure, and using the same methodology and assumptions as for the one-off costs, we could estimate the recurring costs to be in the range of €18 to €36 million.

(18) In the absence of Union harmonisation, ICT-related incident reporting thresholds and taxonomies vary significantly at national level. Only the recently adopted guidelines under PSD 2 have set in more detail the criteria, thresholds and methodology for identifying and reporting major ICT-related incidents to the competent authority of the home Member States of the payment service providers. Directive (EU) 2016/1148 (applying to credit institutions, trading venues and central counterparties designated as operators of essential services) sets out criteria to determine the significance of the impact of ICT-related incidents. While common ground may be achieved through relevant work undertaken by the European Union Agency for Cybersecurity (ENISA)[33] and the NIS Cooperation Group for the financial entities under Directive (EU) 2016/1148, divergent approaches on thresholds and taxonomies still exist or can emerge for the remainder of financial entities. This entails multiple requirements that financial entities must abide to, especially when operating across several Union jurisdictions and when part of a financial group. Moreover, these divergences may hinder the creation of further EU 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.

(19) To enable competent authorities to obtain for their supervisory roles 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 complete the ICT-related incident reporting regime with the requirements that are currently missing in financial subsector legislation and remove overlaps and duplications where they exist today to alleviate costs. This Regulation should therefore harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities only, and should also empower the ESAs to further specify ICT-related incident reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds.

(20) In the absence of Union harmonisation, digital operational resilience testing requirements have developed in some financial subsectors (banking and financial market infrastructures) with several and possibly uncoordinated, national frameworks addressing the same issues in a different way. This leads to duplication of costs for cross-border financial entities and makes difficult the mutual recognition of results. In an attempt to avoid fragmentation, the ECB published in 2018 a voluntary sector-agnostic framework for threat lead penetration testing, namely TIBER-EU (intelligence-based ethical red teaming framework), which constitutes a common framework that delivers a controlled, bespoke, intelligence-led red team test of financial entities' critical live production systems.

Several Member States implemented TIBER-EU. However, the same financial entity group can still be tested in 2 to 5 Member States on the same ICT infrastructure. Uncoordinated testing can potentially segment the single market. In addition, where no testing is required, vulnerabilities remain undetected putting the financial entity and ultimately the financial sector's stability and integrity at higher risk. Without Union intervention, digital operational resilience testing would continue to be patchy and

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

there would be no mutual recognition of testing results across different jurisdictions. Also, as it is unlikely that other financial subsectors would adopt such schemes on a meaningful scale, they would miss out on the potential benefits, such as revealing vulnerabilities and risks, test defence capabilities and business continuity, increased trust of customers, suppliers and business partners. To remedy such overlaps, divergences and gaps, this Regulation should introduce provisions aiming at coordinated testing by financial entities and competent authorities, thus easing the mutual recognition of advanced testing for significant financial entities.

(21) 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 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.

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 standardized services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors.

(22) Despite some general rules on outsourcing in some of the Union's financial services pieces of legislation, the monitoring of the contractual dimension is not fully anchored into the Union legislation. Not only there are different implementation practices within the Union, but there is also a clear asymmetry in the negotiating positions of small financial entities and hyper-scale technology providers. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with the ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. This Regulation consequently sets out certain key principles to guide financial entities' management of ICT third-party risk, 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 an ICT third party level.

(23) In the absence of more specific Union legislative rules on the monitoring of ICT third-party risk, the ESAs have tried to remedy the lack of homogeneity and convergence on ICT third-party dependencies, by tackling the specific area of outsourcing. Most notably, the 2017 recommendations on outsourcing to cloud service providers[34] represented a first step to overcome a high level of uncertainty regarding supervisory expectations on the use of certain ICT services (cloud computing services) and to remove associated barriers. These recommendations have been superseded by recently

[34] Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), now repealed by the EBA Guidelines on outsourcing (EBA/GL/2019/02).

adopted guidelines on outsourcing,[35] and other guidelines in the process of adoption.[36] However, guidelines are subject to the 'comply or explain' approach, cover solely outsourcing (not all relevant contractual relationships) and do not apply to all financial entities.

(24) The Final Report of the High Level Forum on the Capital Markets Union also called for rebalancing the relationship between the providers of cloud computing services and their financial services clients in order to make the use of cloud computing services more secure and preserve the financial system's resilience.[37]

(25) Moreover, the issue of systemic risk which may be triggered by the financial sectors' exposure to a limited number of critical ICT third-party service providers is barely addressed in the Union legislation. This lack at Union level is compounded by the absence of specific mandates and tools allowing national supervisors to acquire a good understanding of ICT third-party dependencies and adequately monitor risks arising from concentration of such ICT third-party dependencies.

(26) Concerns about cyber vulnerabilities that may emerge at the level of third parties have also been voiced at international level in particular by the G7 Cyber Expert Group. In the context of the 2018 'Fundamental Elements for Third Party cybersecurity risk management in the financial sector', the group recommended considering more rigorous and frequent monitoring as well as an appropriate oversight of third-party service providers delivering critical functions or posing a higher material level of risk to financial entities. In its 2019 report on third-party dependencies,[38] the Financial Stability Board highlighted that operational risk failures may, in the context of concentrated markets (such as for cloud computing services), be further amplified and potentially lead to system-wide disruptions or stability risks if financial entities increased their reliance on cloud computing technology for core operations.

(27) Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, and mindful of how insufficient are the national mechanisms enabling financial superiors to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, the ESAs have in their 2019 Joint Advice recommended the establishment of 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.

---

35 EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) specify the risk management provisions which credit institutions, payment institutions and electronic money institutions need to implement when outsourcing functions, in particular with regard to the outsourcing of critical or important functions, as well as how these arrangements are to be reviewed and monitored by competent authorities, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.
EIOPA has also recently adopted guidelines on outsourcing. These provide clarification and transparency to market participants to avoid potential regulatory arbitrages and to foster supervisory convergence regarding the expectations and processes that are applicable in relation to cloud outsourcing, https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

36 ESMA public consultation on guidelines on outsourcing to cloud service providers, https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines.

37 *A New Vision for Europe's Capital Markets, Final Report of the High Level Forum on the Capital Markets Union*, June 2020, https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf.

38 *Third-party dependencies in cloud services, Considerations on financial stability implications*, https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

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

(29) Hesitations about the type of information which 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, fragmented, with relevant exchanges being done mostly local (via national initiatives) and with no consistent EU-wide information sharing arrangements tailored for the needs of an integrated financial sector.

Several platforms - such as the Financial Services Information Sharing and Analysis Center (FS-ISAC EU), the World Federation of Exchanges (WFE GLEX) and the Financial Sector Cyber Collaboration Centre - are based outside the Union, and only two such initiatives have developed within the Union: the TCO Advisory Group Cyber in the Netherlands and the recently pan-European Cyber Information and Intelligence Sharing Initiative (CIISI-EU),[39] strongly supported by the ECB.

(30) This Regulation should therefore encourage financial entities to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels ultimately to enhance financial entities' capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. This Regulation should therefore 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.

(31) The mechanisms allowing for a voluntary sharing of information should be conducted in full compliance with the applicable EU competition law rules[40] as well as in a way that guarantees the full respect of Union data protection rules, mainly Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), in particular 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.

(32) According to a well-established case law of the Court of Justice of the European Union,[41] the Union legislature may have recourse to the use of Article 114 TFEU in particular where differences between national rules are such as to obstruct the

---

39 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en html.

40 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.

41 Judgment of 8 June 2010, Vodafone, C-58/08, ECLI:EU:C:2010:321, paragraphs 32 and 33.

fundamental freedoms, and have thus a direct effect on the functioning of the internal market, or to cause significant distortions of competition. Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk triggering 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 in different Member States may equally be distorted.

The use of Article 114 TFEU is also possible if the aim is to prevent the emergence of obstacles to trade resulting from the divergent development of national laws, when the emergence of such obstacles is likely to occur, and the measure in question are be designed to prevent them. Therefore, for specific areas where the EU harmonisation is limited - such as digital operational resilience testing - or is absent - such as a comprehensive oversight of ICT third-party risk - disparities derived from envisaged developments at national level could generate further obstacles to the functioning of the single market to the detriment of market participants and the financial stability.

(33) As the Single Rulebook currently lacks a comprehensive and modern digital operational framework applying to all financial entities, this Regulation should set out the key digital operational resilience requirements for financial entities. It should consequently establish the digital operational component of the functioning of financial services markets. By building up capabilities which allow all financial sectors to withstand digital operational outages, these rules are meant to preserve the financial stability of all entities operating on the Union's financial markets and to ensure a high level of protection of investors and consumers. 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.

(34) Shaping digital operational resilience requirements by means of a regulation would ensure that such requirements are directly applicable and that all financial entities follow the same rules across the Union, without prejudice to proportionality and specific rules foreseen by this Regulation. Consistency in addressing digital operational risks contributes to enhancing confidence in the financial system and preserves the stability of the latter especially in times of overuse of ICT systems, platforms and infrastructures which entail increased digital risk. Since the use of a regulation helps reducing regulatory complexity, fosters supervisory convergence and increases legal certainty, this proposal would also contribute to limit financial entities' compliance costs, especially for those operating on a cross-border basis, which in turn would help removing competitive distortions.

(35) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of their 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 (TEU).

(36) The provisions of this Regulation respect the principle of proportionality, having regard in particular to the diversity in size and scale of operations and to the range of activities of financial entities or third-party providers. Member States should ensure that the requirements laid down in this Regulation apply in a manner proportionate to the nature, scale and complexity of the risks associated with financial entities' reliance on ICT infrastructures.

(37) With a view to enable a common framework for the digital operational resilience of interlinked financial entities, and thereby ease the homogenous and coherent application of all components of the risk management on ICT-related areas, and in order to guarantee a level playing field among financial entities with regard to their regulatory obligations on ICT-risk related matters, and to promote the necessary digital innovation in the financial sector, a wide range of regulated financial entities in the Union should fall in the scope of this Regulation.

(38) Notwithstanding such broad coverage, the application of the digital operational resilience rules should take into consideration significant differences between financial entities in terms of size, business profiles or exposure to digital risk. As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework, all financial entities should duly balance their ICT-related needs to their size and business profile, while competent authorities should continue to assess and review the approach of such distribution.

(39) 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 not qualifying as micro enterprises 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 overlooking arrangements with ICT third-party service providers or for dealing with crisis management, to organize their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining the access rights policies.

By the same token, only such financial entities should be called to perform in-depth assessments after major changes in the network and information system infrastructures and processes, to regularly conduct risk analyses on legacy ICT systems, or expand the testing of business continuity and response and recovery plans to capture switchovers scenarios between primary ICT infrastructure and redundant facilities.

(40) 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 consequently be devolved to a small percentage of financial entities. Finally, and with a view to ease regulatory burdens, only financial entities other than micro enterprises should be asked to regularly report to the competent authorities all costs and losses caused by ICT disruptions and the results of the post-incident reviews after significant ICT disruptions.

(41) To ensure full alignment and overall consistency between financial entities' business strategies on the one hand, and the conduct of the 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 information and communication technology 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 at all levels a strict cyber hygiene.

(42) The final responsibility of the management body in managing financial entity's ICT risks should be an overarching principle of that comprehensive approach. It should be based upon an assignment of clear roles and responsibilities for all ICT-related functions and should be further reflected through the continuous and active engagement of the management body in the control of the monitoring of the ICT risk management.

The relevant missions of the management body in this context should notably regard the entity's ICT risk tolerance to be set, as well as a full range of approval and control processes, in particular for the ICT risk management framework, the implementation of ICT business continuity and disaster recovery plans, the information security policy and the arrangements with ICT third-party service providers.

Moreover, full accountability of the management body cannot be conceived in the absence of efforts towards a realist estimation of ICT investments and subsequent allocation of appropriate budget ensuring financial entity's digital operational resilience in respect to all needs.

(43) Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk,[42] this Regulation promotes a set of functions facilitating the overall structuring of the ICT risk management. As long as the main capabilities which financial entities put in place answer the needs of the objectives foreseen by the functions (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities remain free to use ICT risk management models that are differently framed or categorised.

(44) 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 performance of their services, but as technologically resilient as they can be to allow financial entities to adequately deal with additional processing needs which stressed market conditions or other adverse situations may generate. While this Regulation does not entail any standardization of specific ICT systems, tools or technologies, it relies on the financial entities' suitable use of European and internationally recognized technical standards (e.g. ISO) or industry best practices, insofar such use is fully compliant with specific supervisory instruction on the use and incorporation of international standards.

(45) 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. However, while backup systems should begin processing without undue delay, such start should in no way jeopardize the integrity and security of the network and information systems or the confidentiality of data.

While this Regulation moves away from a rigid approach in determining strict recovery time objectives (RTOs) and hence allows financial entities to set such objectives by fully taking into account the nature and the criticality of the concerned

---

42 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/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

function and any specific business needs, an assessment on the potential overall impact on market efficiency should also be required when determining such RTOs.

(46) The significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source. To mitigate such risks, avoid ICT systems losing integrity or becoming unavailable and confidential data being breached or physical ICT infrastructure suffering damage, the reporting of major ICT-related incidents by financial entities should be significantly improved.

This Regulation should harmonise the ICT-related incident reporting for all financial entities by requiring them to report to their competent authorities only. It should empower the ESAs to further specify all relevant ICT-related incident reporting elements, such as taxonomy, timeframes, data sets, templates and materiality thresholds. While all financial entities would be subject to this reporting, not all of them should be affected in the same manner, since relevant materiality thresholds and time frames should be calibrated to only capture major ICT-related incidents. Direct reporting would enable financial supervisors' access to information on ICT-related incidents. Nevertheless, financial supervisors should pass on this information to non-financial public authorities (NIS competent authorities, national data protection authorities and law enforcement authorities for incidents of criminal nature). The ICT-related incident information should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity while the ESAs should share anonymized data on threats and vulnerabilities relating to an event to aide wider collective defence.

(47) Further reflection on the possible centralisation of ICT-related incident reports should be envisaged, by means of a single EU central Hub either directly receiving the relevant reports and automatically notifying national competent authorities, or merely centralising reports forwarded by the national competent authorities and fulfilling a coordination role. By xx/20xx [*OJ: insert 3 years after the date of entry into force of this Regulation*], the ESAs, in consultation with the ECB and ENISA, should prepare a joint report exploring the feasibility of setting-up such a central EU Hub.

(48) In order to achieve robust digital operational resilience, and in line with international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing (TLPT), financial entities should regularly test their ICT systems and staff with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities. To respond to differences across and within the financial subsectors regarding the financial entities' cybersecurity preparedness, testing should include a wide variety of tools and actions, ranging from an 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 (e.g. TLPT for those financial entities mature enough from an ICT perspective to be capable of carrying out such tests). Digital operational resilience testing should thus be more demanding for significant financial entities (such as large credit institutions, stock exchanges, CSDs, CCPs, etc.). At the same time, digital operational resilience testing should also be more relevant for some subsectors playing a core systemic role (e.g. payments, banking, clearing and settlement), and less relevant for other subsectors (e.g. asset managers, credit rating

agencies, etc.). Cross-border financial entities exercising their freedom of establishment or provision of services within the Union should comply with a single set of advanced testing requirements (e.g. TLPTs) in their home Member State, and that test should include the ICT infrastructures in all jurisdictions where the cross-border group operates within the Union, thus allowing cross-border groups to incur testing costs in one jurisdiction only.

(49) To ensure a sound monitoring of ICT third-party risk, this Regulation crystalizes a set of principle-based rules to guide financial entities' monitoring of risk arising in the context of outsourced functions to ICT third-party services providers and, more generally, in the context of ICT third-party dependencies.

(50) Irrespective of the type of contractual arrangements and the specific rights and obligations enshrined therein, a financial entity should at all times remain fully responsible for complying with obligations under this Regulation. A proportionate monitoring of risk emerging at the level of the ICT third-party service provider should be organized by duly considering the scale, complexity and importance of ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and ultimately a careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.

(51) 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 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 Oversight Framework foreseen by this Regulation, financial supervisors should regularly receive essential information from the Registers and should be able to request on an ad-hoc basis any extracts thereof.

(52) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, while termination of contracts should be prompted by at least a set of circumstances that show shortfalls at the ICT third-party service provider.

(53) To address systemic impact of ICT third-party concentration risk, this Regulation strives to promote a flexible and gradual approach. Financial entities should thoroughly assess contractual arrangements to identify the likelihood for such risk to emerge, including by means of in-depth analyses of sub-outsourcing arrangements, notably when concluded with ICT third-party service providers established in a third country. Lead Overseers should in the exercise of Oversight tasks pay particular attention to fully grasp the magnitude of interdependences and discover specific instances where a high degree of concentration of critical ICT third-party service providers (CTPPs) in the Union is likely to put a strain on the Union financial system's stability and integrity. 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, this Regulation should not foresee strict caps and limits to ICT third-party exposures. Where such a risk is nonetheless identified by Lead Overseers, a very

rigorous dialogue should be initiated with CTPPs and necessary remedial actions should be sought and mandated.[43]

(54) To be able 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 resilience, this Regulation harmonises key contractual elements throughout the performance of contracts with ICT third-party providers. These elements only cover minimum contractual aspects retained crucial for enabling the full monitoring by the financial entity from the perspective of ensuring its digital resilience reliant on the stability and security of the ICT service.

(55) In the context of approval processes which may be required by specific pieces of the Union financial services legislation, competent authorities shall duly check that financial entities introduce and maintain contractual clauses giving effect to safeguards required by this Regulation for such key contractual elements.

(56) Contractual arrangements should in particular provide for a specification of complete descriptions of functions and services, of locations where such functions are provided and where data are processed, as well as an indication of full service level descriptions accompanied by quantitative and qualitative performance targets within agreed service levels to allow an effective monitoring by the financial entity. In the same vein, provisions on accessibility, availability, integrity, security and protection of personal data, as well as guarantees for access, recover and return in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider should also be considered essential elements for a financial entity's ability to ensure the monitoring of the third party risk.

(57) To ensure that financial entities remain in full control of all developments which may impair their ICT security, notice periods and reporting obligations of the ICT third-party service provider should be foreseen in case of developments with a potential material impact on the ICT third-party service provider's ability to effectively carry out critical or important functions, as well as the assistance of the latter in case of an ICT-related incident at no additional cost or at a cost that is determined ex-ante.

(58) Unrestricted rights of access, inspection and audit by the financial entity or an appointed third-party are crucial instruments in the financial entities' ongoing monitoring of the ICT third-party service provider's performance, coupled with full cooperation of the ICT third-party service provider during inspections. In the same vein, unrestricted rights of the competent authority of the financial entity to inspect and audit the ICT third-party service provider, subject to confidentiality, should be foreseen based on notices.

(59) Contractual arrangements should foresee clear termination rights and related minimum notices compliant with competent authorities' expectations, as well as dedicated exit strategies enabling, in particular, mandatory transition periods during which the ICT third-party service providers should continue providing the relevant functions with a view to reduce the risk of disruptions at the level of the financial entity or, allowing the latter to effectively switch to other ICT third-party service providers, or alternatively resort to the use of on-premises solutions, consistent with the complexity of the provided service.

---

[43] 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 EU Competition Law Authority or with the National Competition Law Authorities.

(60) Moreover, the voluntary use of standard contractual clauses developed by the Commission for cloud computing services may provide further comfort to the financial entities and their 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 foreseen in the 2018 Fintech Action Plan which 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 into the process.

(61) With a view to promote convergence and efficiency in relation to supervisory approaches to ICT-third party risk to the financial sector, this Regulation should subject CTPPs to a Union Oversight Framework. Through a new harmonised legislative framework, the ESAs designated as Lead Overseers for each CTPP would be best placed to ensure that ICT third-party providers fulfilling a critical role to the functioning of the financial sector are commensurately overseen on a Union scale.

(62) A designation mechanism for the purposes of applying the Union Oversight Framework should take into account the dimension and nature of the financial sector's reliance on such ICT third-party providers, translated into a set of quantitative and qualitative criteria that would set the criticality parameters as basis for inclusion into the Oversight. CTPPs which are not automatically designated by virtue of the application of the above-mentioned criteria should have the possibility to voluntary opt-in to the Oversight Framework, while those ICT third-party providers subject to cooperative and cross-border oversight mechanisms conducted by Union institutions should consequently be exempted.

(63) In addition to, and without prejudice to, the Union Oversight Framework which is set up by this Regulation, where ICT third-party service providers not fulfilling the designation criteria set under this Regulation are deemed to be important at national level, Member States may conduct own oversight missions in respect to such ICT third-party providers.

(64) To leverage the current 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 maters on ICT risk, in accordance with its tasks on cybersecurity, supported by a new Subcommittee (the Oversight Forum) carrying out preparatory work for both individual decisions addressed to CTPPs and collective recommendations, notably on benchmarking CTPPs' oversight programs and identifying best practices for addressing concentration risk issues.

(65) To acquire insight into the type, dimension and impact of the ICT third-party risk posed to the Union's financial system, Lead Overseers should enjoy powers and tools which allow them to effectively address the systemic dimension of such risk. While unrestricted rights of access and inspection are prerequisite to pursuing the Oversight missions, additional rights to address mandatory instructions and oppose certain contractual arrangements are needed to remedy identified shortfalls that may ultimately affect the stability of the financial entity or the financial system. In addition, Lead Overseers should be able to compel CTPPs to give access to the representatives of the Lead Overseer in particular in the context of onsite and offsite inspections and to submit complete and updated information as requested and, in case of non-

compliance, to apply penalties. Compliance of the CTPPs with the substantive recommendations laid down by the Lead Overseers should be ensure through enforcement by the national competent authorities.

(66) Where oversight missions might have to be carried out in third countries, EBA, ESMA and EIOPA should be encouraged to conclude cooperation arrangements with the relevant supervisory and regulatory third-country competent authorities to facilitate the conduct of such missions.

(67) To leverage technical expertise of competent authorities' experts on operational and ICT risk management Lead Overseers should draw on national supervisory experience and set-up dedicated examination teams for each individual CTPP, pooling together multidisciplinary teams to supporting both the preparation and the actual execution of the oversight activities, including onsite inspections of CTPPs, as well as needed follow-up thereof.

(68) Competent authorities should possess all necessary 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 sectoral competent authorities, close cooperation between the relevant competent authorities, including the European Central Bank (ECB) with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013, and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities.

(69) In accordance with Declaration No 39 on Article 290 TFEU, the Commission should continue to consult experts appointed by the Member States in the preparation of draft delegated acts in the financial services area, in accordance with established practice.

(70) Since this Regulation, together with Directive xx/20xx (DORAD), entails a consolidation of the ICT risk management provisions spanning across multiple regulations and directives of the Union's financial services acquis, this Regulation should amend such regulations to ensure full consistency with these acts by clarifying that ICT risk-related provisions are dealt within this Regulation.

Regulations (EC) No EU/909/2014, EU/648/2012 and EC/1060/2009 of the European Parliament and of the Council are amended accordingly to ensure consistency of the existing Union legal framework with this Regulation, the main object of which is the establishment and functioning of the single market, in particular by ensuring a level playing field of all financial entities.

(71) Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards, this Regulation should mandate 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. This exercise will entail the subsequent amendment of existing delegated and implementing acts adopted in different areas of the financial services legislation.

The scope of the operational risk articles upon which empowerments in those acts had mandated the adoption of delegated and implementing acts should be modified with a

view to carry over into this Regulation all provisions covering the digital operational resilience which are today part of financial services regulations.

(72) In their quality of bodies with highly specialised expertise, it would be efficient and appropriate for the ESAs, through the Joint Committee, to ensure efficient administrative and reporting processes when drafting technical standards. The reporting formats should be proportionate to the nature, scale and complexity of the activities of the financial entities.

(73) The Commission should adopt draft regulatory technical standards developed by ESAs in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk by means of delegated acts pursuant to Article 290 TFEU and in accordance with Article 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 respectively. It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. The Commission and ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to the nature, scale and complexity of those entities and their activities.

(74) The Commission should also be empowered to adopt implementing technical standards developed by ESAs with regard to templates for the purposes of major ICT incident reporting, registering information in relation to arrangements on the use of ICT services provided by ICT third-party service providers, by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 respectively.

(75) In order to ensure a high degree of transparency, ESAs should launch consultations relating to the draft technical standards referred to in this Regulation. ESAs and the Commission should start preparing their reports on [*OJ: insert date 1 year after the date of entry into force of this Regulation*], as provided for in this Regulation, as soon as possible.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

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

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

   – Information Communication Technology (ICT) risk management,

   – reporting of major ICT-related incidents to the competent authorities,

   – digital operational resilience testing,

   – information and intelligence sharing in relation to cyber threats and vulnerabilities,

   – measures for a sound management by financial entities of the ICT third-party risk,

   (b) key requirements for ICT third-party service providers in the context of contractual arrangements concluded with financial entities, with a view and extent necessary to support a secure provision of ICT services to financial entities, and with due consideration for the observance of parameters necessary to achieving regulatory compliance and fulfilling business needs, in particular performance, stability, capacity, data and information integrity and confidentiality;

   (c) the establishment of an Oversight Framework with regard to 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 2016/1148, this Regulation shall be considered as *lex specialis* pursuant to Article 1(7) of that Directive.

Article 2

Scope ratione personae

1. This Regulation applies to the following entities:

   (a) credit institutions,

   (b) payment institutions,

(c) electronic money institutions,

(d) investment firms,

(e) crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant 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 pensions,

(p) credit rating agencies,

(q) statutory auditors and audit firms,

(r) administrators of critical benchmarks,

(s) crowdfunding service providers,

(t) securitisation repositories.

2. For the purposes of this Regulation, entities referred to in paragraph 1 shall collectively be referred to as 'financial entities'.

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 from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party 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;

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

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

(4) 'ICT risk' means any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-

malicious event - which, if materialized, may compromise the security of the network and information systems, of any technology-dependant tool or process, of the operation and process' running, or of the provision of services, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects';

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

(6) 'ICT-related incident' means an unforeseen identified occurrence in the network and information systems, whether resulting from malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity;

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

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

(9) 'cyber-attack' means a malicious ICT-related incident 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 which brings relevant and sufficient understanding for mitigating the impact of an ICT-related incident or 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 entity;

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

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

(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 further sub-contractors of the latter;

(15) 'ICT third-party service provider' means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centers, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication

network and services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 ;

(16) ‘ICT services’ means digital and data services provided through the ICT systems to one or more internal or external users, including provision of data, data entry, data storage, data processing and reporting services, data monitoring as well as data based business and decision support services;

(17) ‘critical or important function’ means a function 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, or its financial performance or the soundness or the continuity of its services and activities;

(18) ‘critical ICT third-party service provider (CTPP)’ means an ICT third-party service provider designated in accordance with Article 29 and subject to the Oversight Framework referred to in Articles 31 to 34;

(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, has not set up business/presence in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services;

(20) ‘ICT sub-contractor established in a third country’ means an ICT sub-contractor that is a legal person established in a third-country, has not set up business/presence in the Union and 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; ‘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, and ultimately of the Union’s financial system as a whole, to deliver critical functions, or to suffer other type of adverse effects, including large losses;

(21) ‘Oversight Framework’ means a set of monitoring activities carried out by the Lead Overseer in accordance with Article 29 with the aim to assess and attest whether a critical ICT third-party service provider acts in accordance and full compliance with a set of principles and rules when providing ICT services to financial entities;

(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, point (u) of Article 3(1) of Regulation (EU) xx/20xx [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation;

(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013;

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

(25) ‘payment institution’ means a payment institution as defined in point (d) of Article 1(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;

(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 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 as defined in point (63) of Article (4)(1) of Directive 2014/65/EU;

(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 of Directive (EU) 2016/97;

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

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

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

(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) ‘statutory auditor’ means statutory auditor as defined in point (2) of Article 2 of 2006/43/EC;

(42) ‘audit firm’ means an audit firm as defined in point (3) of Article 2 of 2006/43/EC;

(43) ‘crypto-asset service provider’ means crypto-asset service provider as defined in point (n) of Article 3 (1) of [*OJ: insert reference to MICA Regulation*];

(44) ‘issuer of crypto-assets’ means issuer of crypto-assets as defined in point (h) of Article 3 (1) of [*OJ: insert reference to MICA Regulation*];

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

(46) ‘issuer of significant asset-referenced tokens’ means issuer of significant asset-referenced payment tokens ad defined in point (j) of Article 3 (1) of [*OJ: insert reference to MICA Regulation*];

(47) ‘administrator of critical benchmarks’ means an administrator of critical benchmarks as defined in point (x) of Article x of Regulation xx/202x [*OJ: insert reference to Benchmark Regulation*];

(48) ‘crowdfunding service provider’ means a crowdfunding service provider as defined in point (x) Article x of Regulation xx/202x [*OJ: insert reference to Crowdfunding Regulation*];

(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 as defined in Article 2(3) of Recommendation 2003/361/EC.

CHAPTER II

ICT RISK MANAGEMENT

SECTION I

Article 4

Governance and organisation

1. Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks.

2. The management body of a financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements implementing the ICT risk management framework referred to in Article 5(1) and for their quality.

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

   (a) hold the final responsibility for managing the financial entity’s ICT risks;

   (b) set clear roles and responsibilities for all ICT-related functions;

   (c) determine the appropriate level of ICT risk tolerance of the financial entity, as referred to in point (b) of Article 5(8);

   (d) approve, oversee and periodically review the implementation of the financial entity's ICT business continuity and disaster recovery plans referred to in paragraphs (1) and (3) of Article 10;

   (e) approve and periodically review the ICT 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 to all types of resources, including training on ICT risks and skills for all relevant 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, in case of 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 ICT-related incidents, their impact and response, recovery and corrective measures.

3. Financial entities which do not qualify as microenterprises shall establish a role to overlook 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 shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.

SECTION II

General Provisions

Article 5

ICT risk management framework

1. Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework, which enables them to address ICT risk quickly, efficiently and as comprehensively as possible, to ensure a high level of digital operational resilience that matches business needs, size and complexity.

2. The ICT risk management framework referred to in paragraph 1 shall also include strategies, policies, procedures, as well as the ICT protocols and tools which are necessary to duly and effectively protect all relevant physical components and infrastructures, including computer hardware, servers, as well as all relevant premises, data centres or sensitive designated area, to ensure that all such physical elements are adequately protected from risks including damage or unauthorized access and usage.

3. Financial entities shall minimize the impact of ICT risk by deploying the full range of appropriate strategies, policies, procedures, protocols and tools. They shall provide complete and updated information on ICT risks as required by the competent authorities.

4. As part of the ICT risk management framework, financial entities other than microenterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance and shall regularly review it.

5. Financial entities other than microenterprises shall ensure appropriate segregation of ICT 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, 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 with lessons derived from implementation and monitoring.

7. The ICT risk management framework shall be subject on a regular basis to audit by ICT auditors possessing sufficient knowledge, skills and expertise in ICT risk. 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 while having due regard to the nature, scale and complexity of the financial entities' services and activities.

9. The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it 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 level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance of ICT disruptions;

   (c) setting out clear information security objectives;

   (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 number of reported major ICT-related incidents and the effectiveness of preventive measures;

   (g) defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of third-party service providers;

   (h) the implementation of the digital operational resilience testing;

   (i) outlining a communication strategy in case of ICT-related incidents.

Article 6

ICT systems and tools

1. Financial entities shall have and maintain updated ICT systems and tools or source from ICT third-party service providers such systems and tools, which:

(a) are appropriate to the nature, variety, complexity and magnitude of operations supporting the conduct of their activities;

(b) are reliable;

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

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

2. The use of internationally recognized technical standards and industry leading practices on information security and ICT internal controls shall be in line with relevant supervisory recommendations on the incorporation of such international standards.

Article 7

Identification

1. As part of the ICT risk management framework referred to in Article 5(1) financial entities shall identify and adequately document all functions, the information assets supporting these functions, the ICT system configurations and interconnections with internal and external systems. Financial entities shall review as needed, but at least yearly, the adequacy of the classification of the information assets 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 business processes, functions and information assets. Financial entities shall regularly review, 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 ICT systems accounts, including those on remote sites, the network resources, hardware equipment and shall map physical equipment considered critical. They shall map the configuration of the ICT assets and the links and interdependencies between the different 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.

6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain and regularly update the relevant inventories.

7. Financial entities other than microenterprises shall on a regular basis, and at least annually, conduct a specific ICT risk assessment on all legacy ICT systems, especially before and after connecting old and new 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 functioning of the ICT systems and tools and shall minimize the impact of such risks through the deployment of appropriate ICT security tools, policies and procedures.
2. Financial entities shall design, procure and implement the ICT security strategies, policies, procedures, protocols and tools that aim at, in particular, ensuring the resilience, continuity and availability of the network and information systems, as well as maintaining high standards of security, confidentiality and integrity of data and systems. Data shall be understood as referring to data at rest, data in use and data in transit.
3. To achieve the objectives referred to in the second paragraph financial entities shall use state-of-the-art ICT technology and processes that guarantee the security of the means of transfer of information, minimise the risk of data corruption, loss and unauthorized access and technical flaws that may hinder business activity, prevent information leakage and ensure data is protected from poor administration or processing - related risks, including inadequate record-keeping.
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 theirs, and their customers' ICT resources, data and information assets;

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

   (c)For the purposes of ensuring the compartmentalisation and segmentation of the network connection infrastructure, and in order to minimize and prevent contagion, especially for interconnected financial processes, the network connection infrastructure shall be designed in a way that allows it to be instantaneously severed;

   (d) implement policies that limit the physical and virtual access to ICT system resources and data 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;

(e) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys.

Data shall be encrypted based on results of approved data classification and risk assessment processes.

(f) implement 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.

This process shall be subject to approval by appropriate lines of management. Specific protocols shall be enabled for emergency changes.

(g) have appropriate and comprehensive policies for patches and updates.

Article 9

Detection

1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify all 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 ICT-related incident detection and ICT-related incident response processes, and shall put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response.

3. Financial entities shall devote sufficient resources and capabilities, with due consideration to their size, business and risk profiles, to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

4. Financial entitles referred to in point (l) of Article 2(1) shall 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 a dedicated and comprehensive ICT Business Continuity Policy (ICT BCP) as an integral part of the operational business continuity policy of the financial entity.

2. Financial entities shall implement the ICT BCP referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:

(a) recording all ICT-related incidents;

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

(c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritizes 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 set-out in accordance with Article 11;

(e) estimating preliminary impacts, damages and losses; and

(f) setting out communication and crisis management actions which 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 an associated ICT Disaster Recovery Plan (ICT DRP) which, in the case of financial entities other than microenterprises, shall be subject to independent audit reviews.

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

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

(a) test the ICT BCP and DRP at least annually and after substantive changes to the ICT systems;

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

For the purposes of point (a) of the first subparagraph, 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.

6. Financial entities shall regularly review their ICT BCP and DRP taking into account the results of tests carried out in accordance with paragraph 5 and recommendations from audit checks or supervisory reviews.

7. Financial entities other than microenterprises shall have a crisis management function, which, in case of activation of ICT BCP and DRP, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13.

8. Financial entities shall keep records of activities before and during disruption events when ICT BCP and DRP are activated. Such records shall be readily available.

9. Financial entities listed 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.

10. Financial entities other than microenterprises shall report to competent authorities all costs and losses caused by ICT disruptions and ICT-related incidents.

Article 11

Backup policies and recovery methods

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

   (a) a backup policy 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 sensitiveness of the data;

   (b) recovery methods.

2. Backup systems shall begin processing without undue delay, unless such start would jeopardize the security of the network and information systems or the integrity or confidentiality of data.

3. When restoring backup data using own systems, financial entities shall use systems that have an operating environment different from the main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption.

   For the financial entitiesreferred to in point (g) of Article 2(1), the recovery plans shall allow 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.

4. Financial entities shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.

5. Financial entitieslisted in point (f) of Article 2(1) shall maintain or ensure that their ICT third party providers 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 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. It shall be capable of ensuring the continuity of critical services 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. It shall be immediately accessible to the financial entity's staff to ensure continuity of critical services 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 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, and in order to provide for the highest level of assurance on data integrity, financial entities shall perform multiple checks, including reconciliations. 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, suited to their size, business and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyze their likely impacts on their digital operational resilience.

2. Financial entities shall put in place post ICT-relatedincident reviews after significant ICT disruptions of their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT BCP referred to in Article 10.

   When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authorities.

   The post-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;

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

   (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 business continuity or recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly and on a continuous basis incorporated into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework set out in Article 5.

4. Financial entities shall monitor the effectiveness of the implementation of their digital resilience strategy set out in Article 5(8). They shall map the evolution of ICT risks over time, analyze 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 and enhance the cyber maturity and preparedness of the financial entity.

5. Senior ICT staff such as the Chief information officer, or senior security staff such as the Chief information security officer, shall report at least annually to the management body on these conclusions and put forward recommendations.

6. Financial entities shall develop ICT security awareness programs and digital operational resilience trainings as compulsory modules in the staff training schemes. These shall be applicable to all employees and to senior management staff.

Financial entities shall monitor on a continuous basis relevant technological developments 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 ICT-related incidents or major 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 for that purpose the role of public and media spokesperson.

Article 14

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

EBA, ESMA and EIOPA shall, in consultation with the European Union Agency on Cybersecurity (ENISA), develop draft regulatory technical standards to:

(a) specify further elements to be included in the ICT security tools, protocols, policies, measures and procedures 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 authenticity and integrity of data, including cryptographic techniques and guarantee an accurate and prompt data transmission without major disruptions;

(b) prescribe how the ICT security tools, policies and procedures referred to in Article 8(2) shall incorporate security controls into systems from inception (security by design), allow for adjustments to the evolving threat landscape, and foresee for the use of defence-in-depth technology;

(c) specify further the appropriate techniques, methods and protocols referred to in point (b) of Article 8(4);

(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 paragraph 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 BCP referred to in Article 10(1);

(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) which 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 DRP referred to in Article 10(3).

EBA, ESMA and EIOPA shall submit those draft regulatory technical standards to the Commission by [*OJ: insert date 1 year after the date of entry into force*].

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (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 establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents and shall put in place early warning indicators as alerts.

2. Financial entities shall establish appropriate processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents.

3. The ICT-related incident management process referred to in paragraph 1 shall:

(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 set out 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 information to financial entities that act as counterparts, as appropriate;

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

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

Article 16

Classification of ICT-related incidents

1. Financial entities shall classify ICT-related incidents and shall determine their impact based on criteria set out in the common ICT-related incident taxonomy for financial services referred to in point (a) of paragraph 2 and in paragraph 3.

2. In order to ensure consistent application of this Article, and after consultation with the ECB and ENISA, the ESAs shall, through the Joint Committee, develop common draft regulatory technical standards specifying:

(a) a common taxonomy in support of the classification of ICT-related incidents, to be applied by financial entities;

(b) the criteria to be applied by competent authorities for the purposes of assessing the relevance of major ICT-related incidents to other Member States' jurisdictions and the details of ICT-related incidents reports to be shared with such competent authorities following Article 17(6).

3. The taxonomy referred to in point (a) of paragraph 2 shall set out:

(a) an ICT-related incident impact matrix, based on:

i) The type of impact, in particular integrity loss, confidentiality loss and availability loss;

ii) The criteria to measure the impact, based on the degree of severity and the type of ICT systems and functions that are impacted.

(b) the nature of services affected, including the type of transactions and operations, service users or financial counterparts that are impacted;

(c) the type of ICT-related incidents and their further sub-classification;

(d) a set of uniform criteria and materiality thresholds to be applied by financial entities for categorising an ICT-related incident as a major one for the purpose of the reporting obligation foreseen in Article 17(1).

4. While issuing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account international standards, as well as specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors.

5. The ESAs shall submit those common draft regulatory technical standards to the Commission by [*OJ: insert date 1 year after the date of entry into force*].

6. 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 Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.

Article 17

Reporting of major ICT-related incidents

1. Financial entities shall report major ICT-related incidents to the competent authority within the deadlines foreseen in paragraph 3.

   For the purpose of the first subparagraph, the financial entity shall produce, after collecting and analysing all relevant information, an incident report using the template referred to in Article 18 and submit it to the competent authority.

   The report 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.

2. Where a major ICT-related incident has or may have an impact on the financial interests of service users and clients, financial entities shall, without undue delay, inform their service users and clients about the major ICT-related incident and shall as soon as possible inform them of all measures which have been taken to mitigate the adverse effects of such incident.

3. Without prejudice to ICT-related incident reporting requirements provided in other Union legislative acts, financial entities shall submit to the competent authority:

   (a) an initial notification without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available;

   (b) an intermediate report no later than 1 week 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 the specific request of the competent authority; and

   (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, but not later than one month from the moment of sending the initial report.

4. Where delegations to third-party service providers are permitted under national law by the competent authority, financial entities wishing to delegate reporting obligations under this Chapter to a third-party service provider should inform the competent authority and seek supervisory approval.

5. Upon receipt of the report referred to in paragraph 1, the competent authority shall, without undue delay, provide details of the incident to:

   (a) the EBA, ESMA or EIOPA as relevant;

   (b) the EBA and ECB as applicable in the case of financial entities referred to in points (a) to (c) of Article 2(1); or

   (c) the single point of contact designated under Article 8 of Directive (EU) 2016/1148.

6. EBA, ESMA or EIOPA and the ECB shall assess the relevance of the major ICT-related incident to other relevant public authorities and notify them 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.

Article 18

Harmonisation of reporting content and templates

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

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

      i. establish the content of the reporting for major ICT-related incidents;

      ii. specify further the conditions under which financial entities may delegate to a third-party service provider, upon prior approval by the competent authority, the reporting obligations set out in this Chapter;

   (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.

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 [*OJ: insert date 1 year after 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 conferred on the Commission to adopt the implementing technical standards referred to in the second 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 the paragraph 1 shall comprise at least the following elements:
   (a) prerequisites for the establishment of such an EU Hub;
   (b) benefits, limitations and possible risks;
   (c) elements of operational management;
   (d) conditions of membership;
   (e) modalities for financial entities and national competent authorities to access the EU Hub;
   (f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the EU Hub, including the required expertise.
3. The ESAs shall submit the report to the Commission, the European Parliament and to the Council by xx 202x [*OJ: insert date 3 years after entry into force*].

Article 20

Supervisory feedback

1. Upon receipt of the reports referred to in Article 17(1), the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity, in particular to discuss remedies at the level of the entity or ways to minimise adverse impact across sectors.
2. The ESAs shall, through the Joint Committee, report annually on an anonymised and aggregated basis on the ICT-related incident notifications received from competent authorities, setting out at least the number of ICT-related major incidents, their nature, impact on the operations of financial entities or customers, costs and remedial actions taken.

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

3. Competent authorities and the ESAs, through the Joint Committee, shall duly consider whether supplementary measures to those set out in paragraphs 1 and 2 shall be envisaged to ensure the digital operational resilience of other financial counterparties or the financial system.

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 ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities shall establish, maintain and review, with due consideration to their size, business and risk profiles, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.

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

2. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme, taking into account 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.

3. Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external.

4. Financial entities 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.

5. Financial entities shall test all critical ICT systems and applications at least annually.

Article 22

Testing of ICT tools and systems

1. The digital operational resilience testing programme referred to in Article 21 shall foresee the periodical execution of a full range of appropriate tests, including 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.

In performing these tests, financial entities shall adhere to established European or international norms and standards insofar they are in line with supervisory instructions on the use and incorporation of such norms and standards.

2. Financial entities listed 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.

Article 23

Advanced testing of ICT tools, systems and processes based on TLPTs

1. Financial entities identified in accordance with paragraph 6 shall carry out at least every 3 years advanced testing by means of threat led penetration testing (TLPT).

2. TLPT shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of TLPTs, based on the assessment of critical 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 functions and services, including 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 TLPT, the financial entity shall take the necessary measures to ensure the participation of these providers.

3. Financial entities shall apply effective risk management controls to reduce the risks of any potential impact to data, damage to assets and disruption to critical services or operations at the financial entity itself, its counterparties or to the financial sector.

4. 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 competent authority the documentation confirming that the TLPT has been conducted in accordance with the requirements. Competent authorities shall validate the documentation and issue an attestation.

5. Financial entities shall contract testers for the purposes of undertaking the TLPT in accordance with Article 24.

6. Competent authorities shall identify financial entities to perform TLPTs in a manner that is proportionate to the size, scale, activity and overall risk profile of the financial entity, based on the assessment of:

(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.

7. For the purpose of harmonising the identification of financial entities referred to in paragraph 6 and achieving cross-sectoral convergence that enables the mutual recognition foreseen in Article 25, EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further:

(a) the criteria used for the purpose of the application of paragraph 6 of this Article;

(b) for financial entities when conducting TLPTs, and for competent authorities when validating TLPTs, the requirements in relation to:

i. the scope of TLPTs referred to in paragraph 2;

ii. the testing methodology and approach to be followed for each specific phase of the testing process;

iii. the results, closure and remediation stages.

(c) the type of supervisory cooperation needed for the implementation of TLPTs in the context of financial entities which operate across multiple Union jurisdictions.

The requirements referred to in point (b) of the first subparagraph of this paragraph which are addressed to competent authorities shall guarantee an appropriate level of supervisory involvement, while allowing for a flexible implementation to take into account specificities of financial sub-sectors or local financial markets.

The ESAs shall submit those draft regulatory technical standards to the Commission by [*OJ: insert date 2 months before 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

1. For the purpose of benefitting from the mutual recognition of TLPT results set out in Article 25, financial entities shall contract testers for the deployment of TLPT, which:

(a) are of the highest suitability and reputability;

(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or 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) in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of

TLPTs, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;

(e) in case of external testers, are dully and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

2. Financial entities shall ensure that agreements concluded with external testers require a sound management of the TLPT results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.

3. By [*OJ: insert date 1 year after the date of entry into force*], the ESAs shall, through the Joint Committee, assess the range of practices across financial entities in relation to procurement conditions applying to external testers and shall issue guidelines for the consistent application by financial entities of the requirements provided for in this Article and for achieving convergence in the procurement process.

Those guidelines shall be issued in accordance with Articles 16 and 56(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.

Article 25

Recognition of TLPT results across the Union

1. Results of TLPT tests shall be recognised across the Union when executed and completed in compliance with the provisions of this Regulation and all measures based on its implementation by financial entities exercising the right of establishment and provision of service in accordance with the provisions of Article 33 of Directive 2013/36/EU in the case of financial entities referred to in point (a) of Article 2(1) of this Regulation, Articles 28 and 29 of Directive (EU) 2015/2366 in the case of financial entities referred to points (b) and (c) of Article 2(1) of this Regulation, Article 13 of Directive (EU) 2019/2034 and respectively Articles 34 - 36 of Directive 2014/65/EU in the case of financial entities referred to in point (d) Article 2(1) of this Regulation, Article *xx* of MICA Regulation in the case of financial entities referred to in point (e) of Article 2(1) of this Regulation, Articles 23 and 24 of Regulation (EU) No 909/2014 in the case of financial entities referred to in point (f) of Article 2(1) of this Regulation, Article 14 of Regulation (EU) No 648/2012 in the case of financial entities referred to in point (g) of Article 2(1) of this Regulation, Article 53 of Directive 2014/65/EU in the case of financial entities referred to in point (h) of Article 2(1) of this Regulation, Article 55 of Regulation (EU) No 648/2012 in the case of financial entities referred to in point (i) of Article 2 (1) of this Regulation, Article 60 of Directive 2014/65/EU in the case of financial entities referred to in point (l) of Article 2(1) of this Regulation, Articles 32 and 33 of Directive 2011/61/EU in the case of financial entities referred to in point (j) of Article 2(1), Articles 16–21 of Directive 2009/65/EC in the case of financial entities referred to in point (k) of Article 2(1) of this Regulation, Chapter VIII of Directive 2009/138/EC in the case of financial entities referred to in point (m) of Article 2(1) of this Regulation, Articles 11 and 12 of Directive 2016/2341 in the case of financial entities referred to in point (o) of Article 2(1) of this Regulation, Article 3a of Directive 2006/43/EC in the case of financial entities referred to in point (q) of

Article 2(1) this Regulation, Articles 4 to 9 of Directive (EU) 2016/97 in the case of financial entities referred to in point (n) of Article 2(1) of this Regulation, Article 14 of Regulation (EC) No 1060/2009 in the case of financial entities referred to in point (p) of Article 2(1) this Regulation, Article 29 of Regulation 2016/1011 of in the case of financial entities referred to in point (r) of Article 2(1) of this Regulation and Article xx of in the case of financial entities referred to in point (s) of Article 2(1) of this Regulation xx/202x [*OJ: insert reference to Crowdfunding Regulation*].

2. The attestation referred to Article 23(4) shall serve as declaration for the purposes of the mutual recognition foreseen in the paragraph 1 by other relevant competent authorities.

CHAPTER V

MANAGING OF ICT THIRD-PARTY RISK

SECTION I

KEY PRINCIPLES FOR A SOUND MANAGEMENT OF ICT THIRD PARTY RISK

Article 26

General principles

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

1. Responsibility of the financial entity

   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. Proportionality

   Financial entities' management of ICT third party risk and the supervision by competent authorities of financial entities' of such management shall be implemented in light of the principle of proportionality, taking into account:

   (a) the 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, for which financial entities shall have due regard to the criticality or importance of the respective service, process or function, as applicable, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level, where applicable.

3. Strategy on ICT third party risk

   As part of their ICT risk management framework, financial entities shall adopt and regularly review a Strategy on ICT third-party risk, building on the multi-vendor

strategy as defined in Article 5(8). This shall include a policy on the contractual arrangements on the use of ICT services 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 shall regularly review the risks identified in respect of contracting of critical or important functions.

4. Documentation and evidence

As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, where applicable, 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.

Without prejudice to requirements laid down in other Union financial services acts to provide more detailed information, financial entities shall report at least annually to the competent authorities and on ad hoc basis as required by 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 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 planned contracting of critical or important functions and when a function has become critical or important.

5. Pre-contracting analysis

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

(a) assess whether the contractual arrangement covers a critical or important function;

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

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

(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.

Where a prospective ICT third-party service provider is established in a third country, the financial entity shall take all measures to ensure that it is satisfied of the ethical responsibility of such prospective ICT third-party service provider and of the latter's full observance of international standards on human rights, environmental protection and sustainability goals, as well as on appropriate working conditions, including the prohibition of child labour.

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

6. Information security

Financial entities shall enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the latest information security standards.

7. Audits

In exercising access, inspection and audit rights, 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 national audit standards and to international audit standards insofar they are in line with supervisory instructions on the use and incorporation of such international audit standards.

For contractual arrangements that entail a high level of technological complexity, the financial entity shall verify that auditors, whether internal, pools of auditors or external auditors acting on their behalf, possess appropriate skills and knowledge to effectively perform relevant audits and assessments.

8. Termination rights

Financial entities shall, by means of appropriate contractual clauses, ensure they terminate contractual arrangements on the use of ICT services and take appropriate contingency measures to maintain business continuity after consideration of at least the following circumstances:

(a) 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 which 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 in its 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) upon relevant supervisory instructions, in particular for circumstances where the competent authority is no longer in a position to effectively supervise the financial entity as a result of the respective contractual arrangement.

9. Exit strategies

Financial entities shall put in place exit strategies in order to take into account risks that may emerge at the level of ICT third-party service provider, 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.

Financial entities shall ensure 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 its provision of services to clients.

Exit plans shall be comprehensive, documented and, where appropriate, sufficiently tested.

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 in-house.

10. The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the Register referred to in paragraph 4.

The ESAs shall submit those draft implementing technical standards to the Commission by [*OJ: insert date 1 year 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 standards:

(a) 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 provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services;

(b) the types of information to be included in the Register of Information referred to in paragraph 4.

The ESAs shall submit those draft regulatory technical standards to the Commission by [*OJ: insert date 1 year 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 27

Preliminary assessment of concentration risk and further sub-outsourcing arrangements

1. When performing the identification and assessment of concentration risk referred to in point (c) of Article 26(5), financial entities shall take into account whether the conclusion of a contractual arrangement in relation to the ICT services would lead to:

   (a) contracting with a dominant ICT third-party service provider which is not easily substitutable;

   (b) having in place multiple contractual arrangements in relation to the ICT services 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 provider(s), 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 includes the possibility that an ICT third-party service provider further sub-contracts 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 sub-contracting, in particular in the case of an ICT sub-contractor established in a third-country.

   Where contractual arrangements on the use of ICT services are concluded with an ICT third-party service provider established in a third-country, financial entities shall consider relevant contextual factors, such as in particular the respect of data protection, the law enforcement and insolvency law provisions that would apply in the event of the ICT-third party service provider's failure, as well as any constraints that may arise in respect to the urgent recovery of the financial entity's data.

   Financial entities shall assess whether and how potentially long or complex chains of sub-contracting 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 28

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 a written agreement. The full contractual set, which includes the services level agreements, shall be documented in one main written document available to the parties on paper or in a downloadable and accessible format.

2. The contractual arrangements on the use of ICT services shall include at least:

   (a) a clear and complete description of all functions and services to be provided by the ICT third-party service provider, indicating whether sub-contracting of a

critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting;

(b) the locations where the contracted or sub-contracted functions and services are provided and where data is processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity if it envisages changing such locations;

(c) provisions on accessibility, availability, integrity, security and personal data protection and ensuring access, recover 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;

(d) full service level descriptions, including updates and revisions thereof, and 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 when agreed service levels are not met;

(e) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development which may 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;

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

(g) requirements for the ICT third-party service provider to implement and test business contingency plans and have in place ICT security measures, tools and policies which adequately guarantee a secure provision of services by the financial entity in line with its regulatory framework;

(h) 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 by an appointed third-party, and rights to take copies of relevant documentation, the effective exercise of which shall be unimpeded or limited by other contractual arrangements or implementation policies;

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

iii. unrestricted rights of inspection and audit by the competent authority, subject to confidentiality, provided that a notice of audit or access is given to the ICT third-party service provider in a reasonable time period to be defined in the main contract;

iv. full cooperation of the ICT third-party service provider during the onsite inspections performed by the financial

entity and details on the scope, modalities and frequency of remote audits;

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

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

(k) 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 services with a view to reduce the risk of disruptions at the financial entity;

ii. which allows the financial entity to switch to another ICT third-party service provider or change to on-premises solutions consistent with the complexity of the provided service.

3. When negotiating contractual arrangements, financial entities and ICT third-party service providers may use standard contractual clauses developed 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 the sub-contracting of critical or important functions to properly give effect to the provisions of point (a) of paragraph 2.

The ESAs shall submit those draft regulatory technical standards to the Commission by [*OJ: insert date 1 year 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.

SECTION II

OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS (CTPPS)

Article 29

Designation of critical ICT third-party service providers (CTPPs)

1. For the purposes of applying the Oversight Framework foreseen in Article 30(1), and with a view to achieve consistency across the Union, the ESAs shall, through the

Joint Committee of the European Supervisory Authorities ('Joint Committee') and upon recommendation from the Oversight Forum referred to in Article 30(3), designate the ICT third-party service providers which are critical (CTPPs) for financial entities and the financial system, taking into account the criteria specified in paragraph 2 and further developed in accordance with paragraph 3, and shall appoint either EBA, ESMA or EIOPA as Lead Overseer for each CTPP based on the relative importance of the CTPP for financial entities in the area of responsibility of each ESA.

2. The methodology of designation referred to in paragraph 1 shall be based on the following quantitative and qualitative criteria:

(a) the large number of financial entities which use the respective ICT third-party service provider;

(b) the systemic character or importance of the financial entities relying on the respective ICT third-party provider for the delivery of a critical or important function, taking into consideration the following:

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; and

ii. the interdependence between G-SIIs or O-SIIs and other financial entities, such as when the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities.

(c) the interconnectedness of the contractual arrangements on the use of ICT services, evidenced by :

i. the complexity caused by a combination of contractual arrangements directly or indirectly involving (including through sub-contracting) the same ICT third-party service provider in relation to the provision of critical or important functions or services to the financial entity, or

ii. the multi-jurisdictional presence of the respective ICT third-party service provider across the Union.

(d) the substitutability of the ICT third-party service provider, evidenced by:

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 dominant market shares of a specific ICT third-party service provider or the complexity, sophistication or other features linked to the technology involved; or

ii. difficulties to partially or fully migrate the relevant data and workloads from the respective ICT third-party service provider to another one, due to the 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 and which would endanger the digital operational resilience of the financial entity; or

iii. the intrinsic features of the ICT third-party service provider's organisation or activity, including any complexity associated to the latter's organisational structure, or technological characteristics such as proprietary technology.

(e) number of Member States whose financial entities make use of the respective ICT third-party service provider;

(f) the effect that the failure of, or a disruption to, the ICT third-party service provider would have on financial entities and the broader financial system in more than one Member State.

3. The Commission may adopt a delegated act to specify further the criteria referred to in paragraph 2.

4. The designation procedure referred to in paragraph 1 shall not apply to ICT third-party service providers that are subject to cooperative and cross-border oversight conducted by a Union institution with the same objective and intensity as required under this Regulation.

5. The ESAs, through Joint Committee, shall establish, publish and yearly update the list of CTTPs at EU level.

6. With a view to facilitate the process of designation of CTPPs referred to in paragraph 1, competent authorities shall on a regular basis review the information received from financial entities' reporting on arrangements on the use of ICT services provided by ICT third-party service providers, as foreseen in the third subparagraph of Article 26(4), and shall transmit information on aggregated basis to EBA, ESMA and EIOPA yearly.

EBA, ESMA and EIOPA shall assess in their respective areas of competence the ICT third-party dependencies of financial entities based on the information received from the competent authorities.

7. Without prejudice to the designation foreseen in paragraph 1, ICT third-party service providers that have not been designated as CTPPs may on a voluntary basis request to be subjected to the framework.

For the purpose of the first subparagraph, a CTPP shall submit a reasoned application to the Oversight Forum referred to in Article 30(3). The latter shall prepare a recommendation on designation for consideration by the Joint Committee. The ESAs shall, through the Joint Committee, decide within 6 months of receipt of the application. The decision shall be notified to CTPPs accordingly.

8. A CTPP that is not established in the Union shall designate a representative in one of the Member States where it provides services.

Article 30

Establishment of an Oversight Framework for CTPPs

1. With due regard to the requirements on operational risk, operational requirements or risk management, as well as requirements on outsourcing referred to in points (b) and (e) to (g) of Article 4(1) of Regulation (EU) No 1024/2013, in Article 85 of Directive 2013/36/EU, in Articles 30, 42 and 45 of Regulation (EU) No 909/2014, in Articles 26, 35, 78 and 79 of Regulation (EU) No 648/2012, in Articles 16, 47 and 64 of Directive 2014/65/EU, in Articles 19 and 95 of Directive EU/2015/2366, in Article 44 and 49 of Directive 2009/138/EC, in Article 25 and 31 of Directive EU/ 2016/2341, in Article 6(2) and 9 of Regulation (EC) No 1060/2009, in Articles 12, 14 and 51 of Directive 2009/65/EC, in Article 15, 18 and 20 of Directive 2011/61/EU, in Article 24a of Directive 2006/43/EC and in Articles 10 of Directive (EU) 2016/97, in articles 6 and 10 of Regulation (EU) 2016/1011, in Article *xx* of [*Crowdfunding Regulation once reference available*] and competent authorities' powers to ensure compliance with these requirements, an Oversight Framework of CTPPs shall be established with a view to:

   (a) strengthen the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the performance of operational functions and

   (b) contribute to preserving the Union's financial system stability, with full regard to ensuring the integrity of the single market for financial services, and based on the monitoring of operational risks which may arise as a result of the financial system's reliance on critical ICT third-party service providers.

2. An Oversight Forum shall be established as a Subcommittee of the Joint Committee, with a view to prepare and support the work of the latter in the area of ICT third-party risk across financial sectors as follows:

   (a) The Oversight Forum shall regularly discuss relevant developments on ICT risks and vulnerabilities and promote a consistent approach in the monitoring of ICT risk at Union scale. In particular, it shall suggest coordination measures to increase the digital operational resilience of financial entities, foster best practices on addressing concentration risk and explore mitigants for cross-sector risk transfers.

   (b) The Oversight Forum shall be chaired by the Joint Committee's representative(s) and shall comprise representatives of the ECB, the ESRB, EBA, ESMA and EIOPA. Two representatives per Member States' competent authorities, designated on a rotating basis among competent authorities, as well as from the European Commission, ENISA and of each of the EEA EFTA countries shall participate as observers.

3. To facilitate convergence at Union level of recommendations issued in the conduct of Oversight exercises across different CTPPs, and leveraging on the conclusions of the Lead Overseers referred to in Article 29(1), the Oversight Forum shall agree upon recommendations to be submitted to the Joint Committee to comprehensively benchmark different CTPPs' oversight programs against requirements and expectations. Based on these recommendations, the Joint Committee shall prepare draft joint positions for adoption by the ESAs in accordance with Article 56(1) of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

4. EBA, ESMA and EIOPA, when appointed as Lead Overseer in accordance with Article 29(1), and assisted by the examination team referred to in Article 33(5), shall have the task of executing the Oversight over its assigned CTPP.

5. The Lead Overseer shall adopt a clear, detailed and reasoned individual plan for the conduct of the Oversight, based on a recommendation of the Oversight Forum, which shall be communicated each year to the CTPP.

6. The Oversight Framework referred to in paragraph 1 shall not replace, or in any way nor for any part substitute the management by financial entities of the risk entailed by the use of ICT third-party service providers, including the obligation of ongoing monitoring of their contractual arrangements concluded with CTPPs, and shall not affect the full responsibility of the financial entities in complying with, and discharging of, all requirements under this Regulation and relevant financial services legislation, in accordance with the provisions of Article 26(1).

7. Once the annual plans referred to in paragraph 5 have been agreed and notified to the CTPPs, competent authorities shall refrain from individually undertaking any measure aimed at monitoring CTPP risks, in duplication, or in addition to measures conducted in the context of the Oversight Framework.

8. The Oversight Framework referred to in paragraph 1 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.

9. The ESAs, through the Joint Committee, shall present annually to the European Parliament, the Council and the Commission a report on application of the Oversight Framework. The Joint Committee shall conduct the preparatory work.

Article 31

Scope of the Oversight Framework

1. Lead Overseers shall assess that CTPPs have in place, and shall ascertain that they respect sound, comprehensive and effective rules, procedures, mechanisms and arrangements which are appropriate to manage all risks which CTPPs may pose to financial entities and to the overall financial stability.

2. Based on the instruments and tools provided for in Article 32, the Oversight Framework shall cover the monitoring by the Lead Overseers of the continuous respect by CTPPs, throughout different stages in the provision of their ICT services to financial entities, of rules, certification and self-regulation on:

   (a) ICT requirements which ensure, in particular, the security, availability, continuity, scalability and quality of services which CTPPs provide to the financial entities, as well as the ability to maintain at all times high standards of security, confidentiality and integrity of data;

   (b) physical security requirements, including in relation to the security of premises, facilities, datacentres, which successfully contribute to ensuring the ICT security;

   (c) appropriate risk management processes, including ICT risk management policies, ICT business continuity and ICT disaster recovery plans;

   (d) comprehensive governance arrangements, including an organisational structure with well-defined, transparent and consistent lines of responsibility and with accountability rules that enable an effective ICT risk management;

(e) appropriate policies on the identification, monitoring and prompt reporting of ICT-related incidents to the financial entities to whom CTPPs provide service, as well as in relation to the management and resolution of ICT-related incidents, in particular cyber-attacks;

(f) mechanisms on data portability, application portability and interoperability in particular to allow an effective exercise of termination rights;

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

(h) appropriate ICT audits;

(i) compliance with relevant international standards as needed to ensure a safe provision of services to the financial entities.

Article 32

Oversight powers

1. With a view to conduct the Oversight, the Lead Overseer shall have:

(a) the unrestricted right to access and process all information deemed relevant for the purposes of conducting the Oversight, including access to all relevant business or operational documents, contracts, policies documentation, security audit reports, incident reports, as well as to premises (such as head offices, operation centres, secondary premises, etc.) comprising the full range of relevant devices, systems, networks, information and data either used for, or contributing to, the provision of services to the financial entity, as well as any related financial information, personnel and CTPP's external auditors;

(b) the unrestricted right to conduct at regular intervals and as foreseen in Article 33(4) all inspections and auditing at CTPPs deemed necessary by the Lead Overseer for the purposes of conducting the Oversight;

(c) the right to require CTPPs to remedy any shortcoming identified by the Lead Overseer which adversely impact the provision of services to the financial entity and to submit reports on the remedies taken in that regard;

(d) the right to give instructions to CTPPs prescribing the use of specific ICT security and quality requirements or processes - in particular in relation to the roll out of patches and updates, which are deemed by the Lead Overseer crucial for ensuring the ICT security of services;

(e) the right to examine all subcontracting arrangements, including sub-outsourcing planned to be undertaken by the CTPPs with other ICT third-party service providers, and to address to the CTPPs any recommendation on such planned subcontracting or sub-outsourcing, where the Lead Overseer deems that such further subcontracting or sub-outsourcing may trigger risks for the provision of services by the financial entity and risks to the financial stability;

(f) the right to scrutinize and oppose a further subcontracting arrangement including a sub-outsourcing which the CTPP envisages to conclude with another ICT provider, where the following cumulative conditions are met:

- the envisaged sub-contractor is an ICT sub-contractor established in a third country;
- the subcontracting or sub-outsourcing concerns critical or important functions of the financial entity,
- the Lead Overseer considers that the use of such subcontracting or sub-outsourcing may pose a clear and serious risks for the financial entity, including for its ability to comply with the supervisory requirements.

(g) the right to address mandatory instructions to the CTPPs to guarantee that all conditions, including any technical subsequent implementation thereof, under which CTPPs provide services to the financial entities fully and adequately address any risk created by the interdependency of financial entities' services or of the ICT processes supporting the underlying operations, in particular in the case of a high degree of concentration of CTPP services, with a view to prevent the creation of single points of failure and the generation of systemic impact across the Union's financial system.

2. CTPPs shall fully and in good faith cooperate with the Lead Overseers in the fulfilment of the Oversight missions, including providing assistance to the Lead Overseers with a view to swiftly identifying internal documents or data considered relevant for addressing specific questions.

For the purposes of ensuring the confidential treatment of the data accessed by the Lead Overseers, specific provisions shall be included to that effect in a protocol concluded between the CTPPs and the Lead Overseers.

3. CTPPs shall:

(a) comply by immediately granting the accesses foreseen in points (a) and (b) of paragraph 1;

(b) strive to immediately adhere to, and implement the recommendations referred to in points (c) - (e) of paragraph 1;

(c) comply with the instructions referred to in points (f) and (g) of paragraph 1.

Where CTPPs disagree with the assessment of the Lead Overseer referred to in points (c) to (e) of paragraph 1 and, notwithstanding the latter's recommendations, undertake the envisaged subcontracting, the Lead Overseer, assisted by the examination team referred to in Article 33(5), shall require the financial entity to tighten the financial entity' control of the CTPPs by subjecting the CTPP to an enhanced monitoring programme.

Specific clauses to that effect shall be inserted in advance in the contractual arrangements between the CTPP and the financial entity allowing the latter to terminate the contract with the CTPP without any penalty should the abovementioned enhanced monitoring programme confirm the assessment or the risks foreseen by the Lead Overseers.

4. The ESAs may by decision impose a periodic penalty payment in order to compel an ICT third-party service provider designated as CTPP to:

provide access to the representatives of the Lead Overseer, for the purposes of fulfilling Oversight missions, in particular in the context of onsite and offsite inspections, in accordance with points (a) and (b) of paragraph 1 and

submit complete information as required by the Lead Overseer, in accordance with points (a) – (c) of paragraph 1, in particular to produce complete records, data or any relevant material and to complete, update or correct such information as appropriate.

A periodic penalty payment shall be effective and proportionate. The periodic penalty payment may be imposed on a daily basis until compliance is achieved.

The amount of the periodic penalty payment shall be 1% of the average daily worldwide turnover in the preceding business year and shall be calculated from the date stipulated in the decision imposing the periodic penalty payment. A periodic penalty payment may be imposed for a period of no more than six months following the notification of ESA's decision.

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 in the territory of which inspections and access shall be carried out. Enforcement may be suspended by a decision of the Court of Justice of the European Union. 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.

ESAs shall disclose to the public every periodic penalty payment that has been imposed pursuant to the first subparagraph unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

5. Competent authorities shall assist Lead Overseers by enforcing the Lead Overseer's rights referred to in paragraph 1.

6. For the purposes of fulfilling the Oversight missions, Lead Overseers may take into consideration, to the extent appropriate and at their full discretion, any relevant third-party certifications and ICT third-party internal or external audit reports that are made available by the CTPPs.

Article 33

Conduct of Oversight

1. The ESAs, upon recommendation of the Oversight Forum, shall lay down rules of procedure for the practical and operational arrangements in the conduct of the Oversight Framework.

2. The Lead Overseer shall exercise the powers under Article 32 by addressing a decision to the CTPP recommending or as applicable requiring the latter to take the necessary measures and actions foreseen in Article 32(1). The decision shall be based on a recommendation of the Oversight Forum, taking into account the findings and

conclusions of the Lead Overseers' mission reports in the execution of tasks entrusted under the Oversight Framework.

3. The decisions referred to in paragraph 2 shall, after adoption by the ESAs through the Joint Committee, be immediately communicated to the CTPPs. The exercise of the right of appeal by CTPPs shall be done in accordance with the provisions of Article 60 of the Regulation (EU) No 1093/2010, Regulation (EU) No 1095/2010 and Regulation (EU) No 1094/2010 respectively.

4. Before any planned on-site visit, Lead Overseers shall give a reasonable notice to the CTPPs, 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.

5. Lead Overseers shall compose an examination team for each CTPP, consisting of experts in ICT and operational risk from competent authorities to join the preparation and execution of the oversight activities, including onsite inspections of CTPPs and their follow-up. The details of participation shall be based on cooperation arrangements.

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

   (a) the information to be provided by a CTPPs in the application for a voluntary opt-in set out in Article 29(7);

   (b) the presentation of the information, including the structure, formats, methods that CTPPs shall be required to submit, disclose or report;

   (c) the assessment of compliance by CTPPs with the requirements set by Lead Overseers;

   (d) the content and format of reports which may be requested for the purpose of point (c) of Article 32(1).

   The ESAs shall submit those draft regulatory technical standards to the Commission by 01 January 20xx [*OJ: insert date 1 year 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 34

Oversight fees

The ESAs shall charge CTPPs fees that fully cover ESAs' 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 competent authorities joining the Oversight missions in accordance with Article 33(5).

The amount of a fee charged to a CTPP shall cover all administrative costs and shall be proportionate to the turnover of the CTPP.

The Commission shall adopt a delegated regulation that shall determine the type of fees and the matters for which fees are due, the amount of the fees, and the way in which they are to be paid.

The Commission shall adopt that delegated regulation in accordance with Article 45 and subject to the conditions of Articles 46 and 47.

Article 35

International cooperation

1. EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulation (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 assist in or facilitate the conduct of Oversight missions, foster international cooperation and develop best practices to address third-party risk across financial sectors.
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 the first paragraph focussing on the evolution of ICT third-party risk and implications for financial stability, market integrity, investor protection or the functioning of the single market.

CHAPTER VI

INFORMATION SHARING ARRANGEMENTS

Article 36

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 financial entities' range of 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[44] and competition policy;[45]

For the purpose of point (c), the information sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, as well as operational elements, including the use of dedicated IT platforms.

2. 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.

44 In accordance with Regulation (EU) 2016/679 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. 1–88.

45 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.

CHAPTER VII
COMPETENT AUTHORITIES

Article 37

Competent authorities

Compliance with the obligations set out in this Regulation shall be supervised by the following competent authorities in accordance with the powers granted by the relevant legal acts:

(a) for credit institutions, the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, without prejudice to the specific tasks conferred on the ECB by Regulation (EU) No 1024/2013,

(b) for payment service providers, the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366,

(c) for electronic payment institutions, the competent authority designated in accordance with Article 37 of Directive 2009/110/EC,

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

(e) for crypto-asset service providers, the competent authority designated in accordance with Article xx of *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,

(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 pensions, 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) for statutory auditors and audit firms, the competent authority designated in accordance Articles 3(2) and 32 of Directive 2006/43/EC,

(q) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of Regulation xx/202x,

(r) for crowdfunding service providers, the competent authority designated in accordance with Article x of Regulation xx/202x,

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

Article 38

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

1. To foster cooperation and enable supervisory exchanges between competent authorities and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs may participate through the Joint Committee to the workings of the latter.

2. Whenever appropriate, competent authorities shall consult with the single point of contact and the national CSIRTs designated in accordance with Articles 8 and 9 respectively of Directive (EU) 2016/1148.

Article 39

Financial cross-sector exercises, communication and cooperation

1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB and the ESRB, may organize ad-hoc 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. For the purposes of paragraph 1, competent authorities may designate the financial entities participating in the cross-sectoral crisis management and contingency exercises. They may define together with the involved financial entities the practical modalities of such participation.

3. 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 Article

38 to 44. 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 40

Administrative penalties and remedial measures

1. Competent authorities shall have all supervisory, investigatory and sanctioning powers which are necessary to fulfil their duties under this Regulation.

2. The powers referred to in paragraph 1 shall include at least the following powers to:

   (a) have access to any document or data held in any form which 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;

   (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 42, 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 in the event of the 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 41

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 40 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 40, 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 42

Criminal penalties

1. Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches which are subject to criminal penalties under their national law.

2. Where Member States have chosen, in accordance with paragraph 1, 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 43

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 1 year after entry into force*]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.

Article 44

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, 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 as foreseen in 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 for at least five years after its publication. Personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules.

CHAPTER VIII

DELEGATED ACTS

Article 45

Delegated Acts

7. The power to adopt delegated acts referred to in Articles 29(3) and 34 shall be conferred on the Commission for a period of five years from [*OJ: insert date 5 years after the date of entry into force of this Regulation*].

8. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

9. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in Articles 46 and 47.

Article 46

Revocation of Delegation

The delegation of power referred to in Articles 29(3) and 34 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.

Article 47

Objections to delegated acts

A delegated act adopted pursuant to Articles 29(3) or 34 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

CHAPTER IX

TRANSITIONAL AND FINAL PROVISIONS

SECTION I

Article 48

Review clause

1. By [*OJ: insert date 5 years after the date of entry into force of this Regulation*], the Commission shall, after consulting with 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, regarding the criteria for the identification of CTPPs in Article 29(2).

Article 49

Transitional measures

1. 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 [OJ-insert data - 6 months after the date of entry into force].
2. Notwithstanding paragraph 1, the provisions of Articles 23 to 25 shall apply from the [*OJ-insert data - 36 months after the date of entry into force of this Regulation*].

SECTION II

AMENDMENTS

Article 50

Amendment to Regulation EU/909/2014

Article 45 of Regulation EU/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 the provisions laid down in Regulation (EU) 2021/xx [*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.’;

(2) Paragraph 2 is deleted;

(3) Paragraph 3 is 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 and disaster recovery plans established in accordance with the provisions laid down in 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.’;

Paragraph 4 is replaced by the following:

‘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 foreseen in Article 11(7) of Regulation (EU) 2021/xx [DORA].’;

(4) Paragraph 6 is amended as follows:

‘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) The first subparagraph of paragraph 7 is amended as follows:

‘7. ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT 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 51

Amendment to Regulation EU/648/2012

Regulation EU/648/2012 is amended as follows:

(1) Article 26 is amended as follows:

(a) Paragraph 3 is amended as follows:

‘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 the provisions laid down in Regulation (EU) 2021/xx [DORA].’;

(b) Paragraph 6 is deleted;

(2) Article 34 is amended as follows:

(a) Paragraph 1 is amended as follows:

‘1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set-up in accordance with the provisions laid down in 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) The first subparagraph of paragraph 3 is amended as follows:

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

(3) Paragraph 3 of Article 56 is amended as follows:

‘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 shall be amended as follows:

‘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 the provisions laid down in 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 and disaster recovery plans

established in accordance with the provisions laid down in 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.

Article 52

Amendments to Regulation EC/1060/2009

The first subparagraph of Point 4 of Section A of Annex I of Regulation EC/1060/2009 is amended as follows:

'4. 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 the provisions laid down in Regulation (EU) 2021/xx [DORA].'.

Article 53

Entry into force and application

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

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

Done at Brussels,

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

LEGISLATIVE FINANCIAL STATEMENT

LEGISLATIVE FINANCIAL STATEMENT 'AGENCIES'

3. FRAMEWORK OF THE PROPOSAL/INITIATIVE

3.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council for Digital Operational Resilience for Financial Services.

3.2. Policy area(s) concerned

Policy area: Financial stability, financial services and capital markets union Activity: Digital Operational Resilience

3.3. The proposal relates to

☑ **a new action**

☐ **a new action following a pilot project/preparatory action**[46]

☐ **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

3.4. Objective(s)

3.4.1. General objective(s)

The general objective of the initiative is to strengthen the digital operational resilience of the EU financial sector entities by streamlining and upgrading existing rules and bringing in new requirements where there are gaps. This would also enhance the Single Rulebook on its digital dimension. The overall objective can be structured in three general objectives: (1) reduce the risk of financial disruption and instability, (2) reduce the administrative burden and increase supervisory effectiveness, and (3) increase consumer and investor protection.

3.4.2. Specific objective(s)

The proposal has the following specific objectives: Address ICT risks more comprehensively and strengthen the overall level of digital resilience of the financial sector; Enable financial supervisors' access to information on ICT-related incidents; Ensure that financial entities covered by the proposals assess the effectiveness of their preventive and resilience measures and identify ICT vulnerabilities; Strengthen the contractual safeguards for financial entities when using ICT services, including for outsourcing rules (governing the indirect oversight of ICT TPPs); Enable a direct oversight of the activities of critical ICT TPPs; Incentivise the exchange of threat intelligence in the financial sector. Streamline ICT-related incident reporting and address overlapping requirements; Reduce single market fragmentation and enable cross-border acceptance of testing results.

[46] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

3.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

A digital operational resilience act for the financial sector would ensure a comprehensive framework on digital operational resilience that would be very effective in improving the digital operational resilience of the financial sector. It would safeguard the clarity and coherence within the Single Rulebook.

It would also make the interaction with the NIS Directive and its review clearer and more coherent. It would also bring clarity to financial entities on the different rules on digital operational resilience they need to comply with, in particular for those holding several authorisations and operate in different markets within the EU.

3.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Possible indicators:

Number of ICT-related incidents in the EU financial sector and their impact

Number of major ICT security incidents reported to prudential supervisors

Number of financial entities that would be required to perform TLPT tests

Number of financial entities using Standard Contractual Clauses

Number of critical ICT TPPs overseen by prudential supervisors

Number of financial entities participating in TI solutions

Number of authorities to report the same ICT-related incident

Number of cross-border TLPTs

3.5. Grounds for the proposal/initiative

3.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The financial sector extensively relies on information and communication technologies (ICT). Despite the significant progress made through national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and the stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the EU financial sector and aimed at safeguarding EU competitiveness and stability from economic, prudential and market conduct perspectives. ICT security and overall digital operational resilience are part of operational risk, but have been less in the focus of the post-crisis regulatory agenda, and have developed only in some areas of EU financial markets policy and regulation, or only in a few Member States. This translates into the following challenges, which the proposal should address:

The EU legal framework covering ICT risk and operational resilience across the financial sector is fragmented and not fully consistent.

The lack of consistent reporting of ICT-related incidents leads to supervisors having an incomplete overview of the nature, frequency, significance and impact of incidents.

Some financial entities face complex, overlapping and potentially inconsistent reporting requirements for the same ICT-related incident.

Insufficient information sharing and cooperation on cyber threat intelligence at strategical, tactical and operational level prevent individual financial entities from adequately assessing, monitoring, defending against and responding to cyber threats.

In some financial subsectors, there may be multiple and uncoordinated penetration and resilience testing frameworks, coupled with no cross-border recognition of results, while other subsectors lack such testing frameworks.

The lack of supervisory insights into the activities of financial entities that are provided by ICT TTPs expose financial entities individually, and the financial system as a whole, to operational risks.

Financial supervisors are not equipped with a sufficient mandate, nor the tools to monitor and manage concentration and systemic risks stemming from financial entities' reliance on ICT third -party dependencies.

3.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level (ex-ante):

Digital operational resilience is an issue of common interest to the EU's financial markets. Action at EU level would bring more advantages and greater value than action taken separately at national level. Without completing the European Single Rulebook with operational provisions and tools to address ICT risks and incidents that it currently lacks, all other types of risks would be tackled at European level, but digital operational resilience would remain either left out or subjected to fragmented and uncoordinated national-level initiatives. The proposal would provide legal clarity on whether and how digital operational provisions apply, especially to cross-border financial entities , and it would eliminate the need for Member States to individually improve rules, standards and expectations regarding operational resilience and cybersecurity as a response to the limited coverage of EU financial rules and the general nature of the NIS Directive.

Expected generated Union added value (ex-post):

The proposal would significantly increase the effectiveness of the policy while also reducing complexity, and easing the financial and administrative burden on all operators. It would harmonise an area of the economy that is so deeply connected, integrated, interdependent and that already benefits from a single set of rules and supervision. In terms of incident reporting, the proposal would reduce the reporting burden - and the implicit costs - of the same ICT-related incident being reported to different EU and/or national authorities. It will also facilitate the mutual recognition/acceptance of the testing results of entities operating cross-border that are subject to different testing frameworks in different Member States.

3.5.3. Lessons learned from similar experiences in the past

New initiative

3.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The objective of this proposal is consistent with a number of other EU policies and ongoing initiatives, notably the Network and Information Security (NIS) Directive and the European Critical Infrastructure (ECI) Directive. The proposal would maintain the benefits associated with the horizontal framework on cybersecurity by keeping the financial sector within its scope. The financial sector would remain associated to the NIS cooperation body and financial supervisors would be able to exchange relevant information within the existing NIS ecosystem. The proposal would not impact the NIS Directive, as it would build on it and address any possible overlaps via a lex specialis exemption. The interaction between financial services regulation and the NIS Directive would continue to be governed by a lex specialis clause, which would continue to exempt financial entities from the substantive NIS requirements and avoid overlaps between the digital operational resilience act and the NIS Directive. In addition, the proposal would be consistent with the European Critical Infrastructure (ECI) Directive, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructure against non-cyber threats.

3.5.5. Assessment of the different available financing options, including scope for redeployment

Several financing options were considered:

First, the additional costs could be funded through ESAs' usual financing mechanism. This would however entail a substantial increase in the EU's contribution to ESAs' financial resources.

This option is being chosen for the costs relating to the regulatory tasks linked to this proposal. Indeed, the ESAs will be asked to redeploy existing staff in order to develop a number of technical standards. However, the additional costs related to the oversight of third party providers could not be met through redeployment of resources within the ESAs as the ESAs have other tasks in addition to those envisaged under this proposal, as well as under other legislation. Moreover, supervisory tasks related to digital operational resilience requires specific technical knowledge and expertise. The current level of such resources at the ESAs is insufficient, and this calls additional resources.

Finally, according to the proposal, fees will be levied from the critical ICT third party providers that will be subject to direct oversight. These fees are intended to cover all aditional resources needed by the ESAs to perform their new tasks and powers.

3.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY

☑ **unlimited duration**

Implementation with a start-up period from 2021

followed by full-scale operation.

3.7. Management mode(s) planned[47]

47 Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Direct management by the Commission through

☐ executive agencies

☐ **Shared management** with the Member States

☑ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐ the EIB and the European Investment Fund;

☑ bodies referred to in Articles 70 and 71;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

Comments

N/A

4. MANAGEMENT MEASURES

4.1. Monitoring and reporting rules

Specify frequency and conditions.

In line with already existing arrangements, the ESAs prepare regular reports on their activity (including internal reporting to Senior Management, reporting to Boards and the production of the annual report), and are subject to audits by the Court of Auditors and the Commission's Internal Audit Service on their use of resources and performance. Monitoring and reporting of the actions included in the proposal will comply with the already existing requirements as well as with any new requirements resulting from this proposal.

4.2. Management and control system(s)

4.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Management will be indirect through the ESAs. The funding mechanism would be implemented through fees levied from the critical ICT third party providers concerned.

4.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

In relation to the legal, economic, efficient and effective use of appropriations resulting from the proposal, it is expected that the proposal would not bring new significant risks that would not be covered by an existing internal control framework. However, a new challenge might be related to ensuring timely collection of fees from the critical ICT third party providers concerned.

4.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

Management and control systems as provided for in the ESAs Regulations are already implemented. ESAs work closely together with the Internal Audit Service of the Commission to ensure that the appropriate standards are met in all areas of internal control framework. These arrangements will apply also with regard to the role of ESA according to the present proposal. In addition, every financial year, the European Parliament, following a recommendation from the Council, grants discharge to each ESA for the implementation of their budget.

4.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

For the purpose of combating fraud, corruption and any other illegal activity, the provisions of Regulation (EU, Euratom) N°883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) apply to the ESAs and the EEA without any restriction.

The ESAs have a dedicated anti-fraud strategy and resulting action plan. The ESAs' strengthened actions in the area of anti-fraud will be compliant with the rules and guidance provided by the Financial Regulation (anti-fraud measures as part of sound financial management), OLAF's fraud prevention policies, the provisions provided by the Commission Anti-Fraud Strategy (COM(2011)376) as well as set out by the Common Approach on EU decentralised agencies (July 2012) and the related roadmap.

In addition, the Regulations establishing the ESAs and the EEA, as well as the ESAs' Financial Regulations set out the provisions on implementation and control of the ESAs' and EEA's budgets and applicable financial rules, including those aimed at preventing fraud and irregularities.

5. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

5.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation

New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation

5.2. Estimated impact on expenditure

5.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	Heading

DG : <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAL**
	Commitments	(1)									
	Payments	(2)									
TOTAL appropriations for DG <>	Commitments										
	Payments										

Heading of multiannual financial framework	**7**	‘European Public administration’

EUR million (to three decimal places)

		2022	2023	2024	2025	2026	2027	**TOTAL**
DGs:								
• Human Resources								
• Other administrative expenditure <>								
TOTAL DGs	Appropriations							

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)							

EUR million (to three decimal places) in constant prices

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments							
	Payments							

5.2.2. Estimated impact on appropriations

☑ The proposal/initiative does not require the use of operational appropriations

☐ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places) in constant prices

Indicate objectives and outputs ⇩			2022		2023		2024		2025		2026		2027		**TOTAL**	
	OUTPUTS															
	Type	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1…																
- Output																
Subtotal for specific objective No 1																
SPECIFIC OBJECTIVE No 2 ...																
- Output																
Subtotal for specific objective No 2																
TOTAL COST																

5.2.3. Estimated impact on human resources

5.2.3.1. Summary

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places) in constant prices

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**TOTAL**
Temporary agents (AD Grades)	0,953	1,905	1,905	1,905	1,905	1,905	10,477
Temporary agents (AST grades)	0,238	0,476	0,476	0,476	0,476	0,476	2,619
Contract staff							
Seconded National Experts							
TOTAL	1,191	2,381	2,381	2,381	2,381	2,381	13,096

Staff requirements (FTE):

EBA, EIOPA, ESMA & EEA	2022	2023	2024	2025	2026	2027	**TOTAL**
Temporary agents (AD Grades) EBA=4, EIOPA=4, ESMA = 4	6	12	12	12	12	12	12
Temporary agents (AST grades) EBA=1, EIOPA=1, EEA=1	1,5	3	3	3	3	3	3
Contract staff							
Seconded National Experts							
TOTAL	**7,5**	**15**	**15**	**15**	**15**	**15**	**15**

5.2.3.2. Estimated requirements of human resources for the (parent) DGs

☑ The proposal/initiative does not require the use of human resources.

☐ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

		2022	2023	2024	2025	2026	2027
• **Establishment plan posts (officials and temporary staff)**							
• **External staff (in Full Time Equivalent unit: FTE)**							
XX 01 02 01 (AC, END, INT from the 'global envelope')							
XX 01 02 02 (AC, AL, END, INT and JPD in the Delegations)							
XX 01 04 ***yy***	- at Headquarters						
	- in Delegations						
XX 01 05 02 (AC, END, INT – Indirect research)							
10 01 05 02 (AC, END, INT – Direct research)							
Other budget lines (specify)							
TOTAL							

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	
External staff	

Description of the calculation of cost for FTE units should be included in the Annex V, section 3.

5.2.4. Compatibility with the current multiannual financial framework

☑ The proposal/initiative is compatible the current multiannual financial framework.

☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[48].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts. […]

5.2.5. Third-party contributions

☐ The proposal/initiative does not provide for co-financing by third parties.

☑ The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

EBA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the supervised entities	1,279	1,757	1,557	1,557	1,557	1,557	9,264
TOTAL appropriations co-financed	1,279	1,757	1,557	1,557	1,557	1,557	9,264

EIOPA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the supervised entities	1,222	1,642	1,442	1,442	1,442	1,442	8,632
TOTAL appropriations co-financed	1,222	1,642	1,442	1,442	1,442	1,442	8,632

ESMA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the supervised entities	1,279	1,757	1,557	1,557	1,557	1,557	9,264

6. Estimated impact on revenue

48 See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

☑ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

[…]

Specify the method for calculating the impact on revenue.

[…]

ANNEX

General Assumptions

Title I – Staff Expenditure

The following specific assumptions have been applied in the calculation of the staff expenditure based upon the identified staffing needs explained below:

- Full staffing will be achieved in 2023 and approximatively 50% of the required staff will be recruited in 2022;
- Additional staff hired in 2022 are costed for 6 months given the assumed time needed to recruit the additional staff;
- The average annual cost of a Temporary Agent is EUR 150 000, of a Contract Agent is EUR 85 000 and for a seconded national expert is EUR 80 000, all of which including EUR 25 000 of 'habillage' costs (Buildings, IT, etc.);
- The correction coefficients applicable to staff salaries in Paris (EBA and ESMA) and Frankfurt (EIOPA) are 117.7 and 99.4 respectively;
- Employer's pension contributions for Temporary Agents have been based upon the standard basic salaries included in the standard average annual costs, i.e. EUR 95 660;
- All additional Temporary Agents are AD5s.

Title II – Infrastructure and operating expenditure

Costs are based upon multiplying the number of staff by the proportion of the year employed by the standard cost for 'habillage', i.e. EUR 25 000.

Title III – Operational expenditure

Costs are estimated subject to the following assumptions:

- Translation cost are set at EUR 350 000 per year for each of the ESAs.
- The one-off IT costs of EUR 500 000 per ESA are assumed to be implemented over the two years 2022 and 2023 on the basis of a 50% - 50% split. Yearly maintenance costs are estimate at EUR 50 000 per ESA.
- On-site yearly supervision costs are estimated at EUR 200 000 per ESA.

The estimations presented here above result in the following costs per year:

Heading of multiannual financial framework	Number	Heading 1: Single Market, Innovation & Digital

Constant Prices

EBA: <03.10.02>			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,416	0,832	0,832	0,832	0,832	0,832	4,576
	Payments	(2)	0,416	0,832	0,832	0,832	0,832	0,832	4,576
Title 2:	Commitments	(1a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688
	Payments	(2a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688
Title 3:	Commitments	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Payments	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL appropriations for EBA <03.10.02>	Commitments	=1+1a +3a	1,279	1,757	1,557	1,557	1,557	1,557	9,264
	Payments	=2+2a +3b	1,279	1,757	1,557	1,557	1,557	1,557	9,264

EIOPA: <03.10.03>			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,359	0,717	0,717	0,717	0,717	0,717	3,944
	Payments	(2)	0,359	0,717	0,717	0,717	0,717	0,717	3,944
Title 2:	Commitments	(1a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688
	Payments	(2a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688
Title 3:	Commitments	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Payments	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL appropriations for EIOPA <03.10.03>	Commitments	=1+1a +3a	1,222	1,642	1,442	1,442	1,442	1,442	8,632
	Payments	=2+2a +3b	1,222	1,642	1,442	1,442	1,442	1,442	8,632

ESMA: <03.10.04>			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,416	0,832	0,832	0,832	0,832	0,832	4,576
	Payments	(2)	0,416	0,832	0,832	0,832	0,832	0,832	4,576
Title 2:	Commitments	(1a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688
	Payments	(2a)	0,063	0,125	0,125	0,125	0,125	0,125	0,688

Title 3:	Commitments	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Payments	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL appropriations for ESMA <03.10.04>	Commitments	=1+1a +3a	1,279	1,757	1,557	1,557	1,557	1,557	9,264
	Payments	=2+2a +3b	1,279	1,757	1,557	1,557	1,557	1,557	9,264

The proposal requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places) in constant prices

EBA

Indicate objectives and outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Type	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 Direct oversight of critical ICT TPPs																
- Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specific objective No 1																
SPECIFIC OBJECTIVE No 2 ...																
- Output																
Subtotal for specific objective No 2																
TOTAL COST				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Indicate objectives and outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Type	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 Direct oversight of critical ICT TPPs																
- Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specific objective No 1																
SPECIFIC OBJECTIVE No 2 ...																
- Output																
Subtotal for specific objective No 2																

TOTAL COST		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Indicate objectives and outputs ⇩			2022		2023		2024		2025		2026		2027			
	OUTPUTS															
	Type	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 Direct oversight of critical ICT TPPs																
- Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specific objective No 1																
SPECIFIC OBJECTIVE No 2 ...																
- Output																
Subtotal for specific objective No 2																
TOTAL COST				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

The direct oversight activities shall be fully funded by fees levied from the overseen entities as follows:

EBA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the overseen entities	1,279	1,757	1,557	1,557	1,557	1,557	9,264
TOTAL appropriations co-financed	1,279	1,757	1,557	1,557	1,557	1,557	9,264

EIOPA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the overseen entities	1,222	1,642	1,442	1,442	1,442	1,442	8,632

TOTAL appropriations co-financed	1,222	1,642	1,442	1,442	1,442	1,442	8,632

ESMA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the overseen entities	1,279	1,757	1,557	1,557	1,557	1,557	9,264
TOTAL appropriations co-financed	1,279	1,757	1,557	1,557	1,557	1,557	9,264

SPECIFIC INFORMATION

Direct Oversight powers

As a way of introduction, it should be recalled that entities subject to direct supervision by ESMA should pay fees to ESMA (one-off costs for registration and recurrent costs for ongoing supervision). This is the case for credit rating agencies (see COM delegated regulation 272/2012) and trade repositories (COM delegated regulation 1003/2013).

Under this legislative proposal, the ESAs will be charged with new tasks aimed at promoting convergence on supervisory approaches to the ICT third party risk in the financial sector by subjecting critical ICT third party service providers (CTPPs) to a Union Oversight Framework.

The Oversight Framework envisaged by this proposal builds on the existing institutional architecture in the financial services area, whereby the Joint Committee of the ESAs ensure cross-sectoral coordination in relation to all maters on ICT risk, in accordance with its tasks on cybersecurity, supported by the relevant Subcommittee (Oversight Forum) carrying out preparatory work for individual decisions and collective recommendations to CTPPs.

Through this framework, the ESAs designated as Lead Overseers for each such CTPP receive powers to ensure that technology services providers fulfilling a critical role to the functioning of the financial sector are adequately monitored on a Pan-European scale. The oversight duties are set out in the proposal and further spelled out in the explanatory memorandum. They include, but are not limited to the right to request information and give instructions to CTPPs, unrestricted rights to access and process all information deemed relevant for conducting the oversight, right to conduct audits and inspections, address mandatory instructions, oppose certain arrangements and require CTPPs to remedy any identified shortcomings, right to examine all subcontracting arrangements, as well as day-to-day oversight.

In order to perform the new tasks envisaged in this proposal, additional staff specialised in ICT third party risk shall therefore be hired by the ESAs. Those needs in term of human resources can be estimated at 5 FTEs for each authority (4 ADs and 1 AST to support the ADs). The ESAs will also incur additional IT costs, estimated at EUR 500 000 (one-off costs) as well as EUR 50 000 per year for maintenance for each of the three ESAs. One important element for fulfilling the new tasks are missions to perform onsite inspections and audits, which can be estimated at EUR 200 000 per year for each ESA. Translation costs for the different documents that the ESAs would receive from the CTPPs are also included within the row on operational costs and consist of EUR 350,000 yearly.

All the administrative costs mentioned above will be fully funded by the annual fees levies by the ESAs from the overseen CTPPs (no impact on EU Budget).