EUROPEAN
COMMISSION

Brussels, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

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 arising from it. 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[1]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 consumers and businesses. In addition to this proposal, the package also includes a proposal for a regulation on markets in crypto assets[2], a proposal for a regulation on a pilot regime on distributed ledger technology (DLT) market infrastructure[3], and a proposal for a directive to clarify or amend certain related EU financial services rules[4].Digitalisation and operational resilience in the financial sector are two sides of the same coin. Digital, or Information and 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 as well as 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[5] of the EU financial sector, only addressing ICT risks indirectly in some areas, as part of the 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 financial risks associated with financial services, they did not fully address digital operational resilience. The measures taken in relation to the latter were characterised by a number of features that limited their effectiveness. For example, they were often devised as minimum harmonisation directives or principled-based regulations, leaving substantial room for diverging approaches across the Single Market. In addition, there has been only some limited or incomplete focus on ICT risks in the context of the operational

1 Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, 23 September 2020, COM(2020)591.

2 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, COM(2020) 593.

3 Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM(2020) 594.

4 Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, COM(2020) 596.

5 The different measures adopted fundamentally aimed at increasing the capital resources and liquidity of financial entities, as well as to reduce market and credit risks.

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 for managing operational risks in a way that 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 prevent financial instability stemming from the materialization of those ICT risks.

The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies). Action at Member State level, however, only has a limited effect given cross-border nature of ICT risks. Moreover, the uncoordinated national initiatives have resulted in overlaps, inconsistencies, duplicative requirements, high administrative and compliance costs - especially for cross-border financial entities - or in ICT risks remaining undetected and hence unaddressed. This situation fragments the single market, undermines the stability and integrity of the EU financial sector, and jeopardises the protection of consumers and investors.

It is therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities. This framework will deepen the digital risk management dimension of the Single Rulebook. In particular, it will enhance and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce 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.[6]

It also responds to the 2019 Joint technical advice[7] 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.[8]

- Consistency with other Union policies

As stated by President von der Leyen in her Political Guidelines,[9] and set-out in the Communication 'Shaping Europe's digital future',[10] it is crucial for Europe to reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe

---

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

7 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).

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

9 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.

10 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.

and ethical boundaries. The European strategy for data[11] sets out four pillars - data protection, fundamental rights, safety and cybersecurity - as essential pre-requisites for a society empowered by the use of data. More recently, the European Parliament is working on a report on digital finance, which inter alia calls for a common approach on cyber resilience of the financial sector[12].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 Directive) by keeping the financial sector within its scope. The financial sector would remain closely 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. Finally, this proposal is fully in line with the Security Union Strategy[13] that called for an initiative on the digital operational resilience for financial sector given its high dependence on ICT services and its high vulnerability to cyber-attacks.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- Legal basis

The proposal for regulation is based on Article 114 TFEU.

It removes obstacles to, and improves the establishment and functioning of the internal market for financial services by harmonising the rules applicable in the area of ICT risk management, reporting, testing and ICT third-party risk. Current disparities in this area, both at legislative and supervisory levels, as well as national and EU levels, act as obstacles to the single market in financial services because financial entities that engage in cross-border activities face different, where not overlapping, regulatory requirements or supervisory expectations with the potential to impede the exercise of their freedoms of establishment and of 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, the development of divergent national rules or approaches, either already in force or in the process of adoption and implementation at national level, can act as a deterrent to the single market freedoms for financial services. This is particularly the case as regards to digital operational testing frameworks and the oversight of critical ICT third-party service providers.

---

[11] 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.

[12] 'Report with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

[13] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM(2020) 605 final.

As the proposal has an impact on 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 also adopted at the same time to reflect the necessary amends to those Directives.

- 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 or multiple requirements applying to the same financial entities operating cross-border or holding several authorisations[14] across the Single Market can only be tackled efficiently at Union level.

This proposal harmonises 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 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 in the absence of Union rules are or may be subject to different frameworks in different Member States. Only action at Union level can address the differences in testing approaches that Member States have introduced. EU-wide action is also needed to address the lack of 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 do not go beyond what is necessary in order to achieve the objectives of the proposal. They 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 their specific characteristics in terms of their size and business profiles. Proportionality is also embedded in the rules on ICT risk management, digital resilience testing, reporting of major ICT-related incidents and oversight of critical ICT third-party service providers.

- Choice of the instrument

The measures needed to govern ICT risk management, ICT-related incident reporting, testing and oversight of critical ICT third-party service providers must be contained in a Regulation in order to ensure that the detailed requirements be effectively and directly applicable in a uniform manner, 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 its stability. Since the use of a regulation

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

helps reducing regulatory complexity, fosters supervisory convergence and increases legal certainty, this Regulation also contributes to limit financial entities' compliance costs, especially for those operating on a cross-border basis, which in turn would help remove competitive distortions.

This Regulation also does away with legislative disparities and uneven national regulatory or supervisory approaches on ICT risk and thus removes obstacles to the single market in financial services, in particular to the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence.

Lastly, the Single Rulebook has mostly been developed via regulations, and its update with the digital operational resilience component should follow the same choice of legal instrument.

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

- Ex-post evaluations/fitness checks of existing legislation

No Union financial services legislation has until now focussed on operational resilience and none has comprehensively tackled risks emerging from digitalisation, not even those whose rules address more generally the operational risk dimension with ICT risk as a sub-component. Union intervention so far have helped to address needs and problems that were present in the aftermath of the 2008 financial crisis: credit institutions were not sufficiently capitalised, financial markets were not sufficiently integrated, and harmonisation up until that point had been kept minimal. ICT risk was not considered a priority then, and, as a result, the legal frameworks for the different financial subsectors has evolved in an uncoordinated manner. Still, Union action has achieved its objectives of ensuring financial stability and to establish a single set of harmonised prudential and market conduct rules applicable to financial entities throughout the EU. Since factors driving Union legislative intervention in the past did not enable specific or comprehensive rules to address the widespread use of digital technologies and consequent risks in finance, carrying out an explicit evaluation appears challenging. An implicit evaluation exercise and consequent legislative amendments are reflected in each pillar of this Regulation..

- 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);[15]

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

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

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);[17]

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 (within 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 call for preserving proportionality and following a principle and risk-based approach in the design of rules. On the institutional side, the 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[18], which was submitted to the Regulatory Scrutiny Board (RSB) on 29 April 2020 and approved on 29 May 2020. The RSB

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

[18] Commission Staff Working Document - Impact Assessment Report Accompanying the document Regulation of the European Parliament and of the Council on digital operational resilience for the

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: additional capital buffers 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 and establishing an Oversight framework for critical ICT third-party providers;
- Option 3: a financial services digital operational resilience act combined with centralised supervision of critical ICT third-party service providers: 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[19]. The one-off 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.

---

financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, SWD(2020)198 of 24.09.2020.

19 *Ibid, p 89-94.*

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 will decrease costs, especially for cross-border firms that could otherwise face multiple tests across Member States[20].

- Fundamental rights

The EU is committed to ensuring high standards of protection of fundamental rights. All voluntary information sharing arrangements between financial entities that this Regulation promotes would be conducted in trusted environments in full respect of Union data protection rules, notably Regulation (EU) 2016/679 of the European Parliament and of the Council[21] in particular when processing personal is necessary for the purposes of a legitimate interest pursued by the controller.

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 18 full-time employees (FTE) - 6 FTEs for each authority - when the different provisions of the proposal will enter into application (estimated at EUR 15,71 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 2,48 million for the period 2022 - 2027). Therefore, the estimated total cost impact is approximately EUR 30,19 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.

---

20 *Ibid*.

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

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 range of financial entities regulated at Union level, 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 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 have more resources, only financial entities not qualifying as microenterprises are 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 switchover scenarios between their 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.

Notwithstanding this broad coverage, it is not exhaustive. Notably, this regulation does not capture system operators as defined in point (p) of Article 2 of Directive 98/26/EC[22] on settlement finality in payment and securities settlement systems (SFD), nor any system participant unless such participant is itself a financial entity regulated at Union level and as such it would be covered by this regulation in its own right (i.e. credit institution, investment firm, CCP). In addition, the Union registry for emission allowances which is operated, in

[22] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.6.1998, p. 45).

accordance with Directive 2003/87/EC,[23] under the aegis of the European Commission is also outside the scope.

Such exclusions from the SFD take into account the need for a further review of legal and policy matters touching the SFD system operators and participants while duly considering the impact of frameworks currently applying to payment systems[24] operated by central banks. As these matters may entail aspects, which remain distinct from issues covered by this regulation, the Commission will continue assessing the necessity and impact of a further extension of this regulation's scope to entities and ICT infrastructures currently outside of its remit.

Governance related requirements (Article 4)

This regulation is designed to 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. This regulation also covers the integrity, safety and resilience of physical infrastructures and facilities that support the use of technology and the relevant ICT-related processes and people, as part of the digital footprint of a financial entity's operations.

ICT-related incident reporting (Articles 15 to 20)

[23] Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC (OJ L 275, 25.10.2003, p. 32).

[24] In particular Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems.

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 detailed in the regulation and further developed by the ESAs through to 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 24)

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 in this regulation and further 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 25 to 39)

The regulation is designed to ensure 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 providers. Second, this regulation harmonises key elements of the service and relationship with ICT third-party providers. These elements cover minimum 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 of their relationship.

Most notably, the contracts that govern that relationship will be required to contain a complete description 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 critical ICT third-party service providers to a Union oversight framework. Through a new harmonised legislative framework, the ESA designated as lead overseer for each such critical ICT third-party service provider receives 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 40)

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.

2020/0266 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(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,[25]

Having regard to the opinion of the European Economic and Social Committee,[26]

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are nowadays core features of all activities of Union financial entities, digital resilience 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. Digitalisation covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, 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[27] how the existing high level of interconnectedness

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

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

across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities[28] to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches occurring in finance do not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union's financial system, generating liquidity runs and an overall loss of confidence and trust in financial markets.

(4) In recent years, ICT risks have attracted the attention of national, European and international policy makers, regulators and standard-setting bodies in an attempt to enhance resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Markets Infrastructures, the Financial Stability Board, the Financial Stability Institute, as well as the G7 and G20 groups of countries aim to provide competent authorities and market operators across different jurisdictions with tools to bolster the resilience of their financial systems.

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

(6) The Commission's 2018 Fintech action plan[29] highlighted the paramount importance of making the Union financial sector more resilient also from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling financial services to be effectively and smoothly delivered across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence.

(7) In April 2019, the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) (jointly called "European Supervisory Authorities" or "ESAs")

---

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

28 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.

29 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.

jointly issued two pieces of technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a Union sector-specific initiative.

(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than for example common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this component, by enlarging the mandates of financial supervisors tasked to monitor and protect financial stability and market integrity.

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

(10) The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user 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.

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

(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements addressed so far separately in the different Regulations and Directives. While those

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

Through this exercise, which consolidates and updates rules on ICT risk, all provisions addressing digital risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This initiative should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via targeted rules on ICT risk management capabilities, reporting and testing and third party risk monitoring.

(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of overuse of ICT systems, platforms and infrastructures, which entails increased digital risk.

The respect of a basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.

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

(15) Besides the financial services legislation, Directive (EU) 2016/1148 of the European Parliament and of the Council[30] is the current general cybersecurity framework at Union level. Among the seven critical sectors, that Directive also applies to 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 certain credit institutions, trading venues and central counterparties identified by the Member States are in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements laid down in it.

(16) As this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in respect to those laid down in the current Union

[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).

financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, this Regulation constitutes lex specialis to Directive (EU) 2016/1148.

It is crucial to maintain a strong relation between the financial sector and the Union horizontal cybersecurity framework would ensure consistency with the cyber security strategies already adopted by Member States, and allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by Directive (EU) 2016/1148.

(17) To enable a cross-sector learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (EU) 2016/1148 should remain part of the 'ecosystem' of that Directive (e.g. NIS Cooperation Group and CSIRTs).

ESAs and national competent authorities, respectively should be able to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, exchanges information and further cooperate with 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 (EU) 2016/1148.

(18) It is also important to ensure consistency 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, with possible implications for the financial sector. [31]

(19) Cloud computing service providers are one category of digital service providers covered by Directive (EU) 2016/1148. As such they are subject to 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 laid down in that act. Since the Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities, it should be considered complementary to the supervision that is taking place under Directive (EU) 2016/1148. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority.

(20) To remain in full control of ICT 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. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements for financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC[32].

---

[31] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

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

(21) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. 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 Union uniform or centralised mechanisms speeding up the reporting process and supporting a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risks in case of large scale attacks with potentially systemic consequences.

(22) To enable competent authorities to fulfil their supervisory roles by obtaining 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, it is necessary to lay down rules in order to complete the ICT-related incident reporting regime with the requirements that are currently missing in financial subsector legislation and remove any existing overlaps and duplications to alleviate costs. It is therefore essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities only. In addition, the ESAs should be empowered to further specify ICT-related incident reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds.

(23) Digital operational resilience testing requirements have developed in some financial subsectors within several and 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. Uncoordinated testing can therefore segment the single market.

(24) 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 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, testing defence capabilities and business continuity, and increased trust of customers, suppliers and business partners. To remedy such overlaps, divergences and gaps, it is necessary to lay down rules aiming at coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition of advanced testing for significant financial entities.

(25) Financial entities' reliance on ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in the past years, driving cost reduction in financial intermediation, enabling

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

business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.

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

(27) 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 Union legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level.

(28) There exists a lack of homogeneity and convergence on ICT third party risk and ICT third-party dependencies. Despite some efforts to tackle the specific area of outsourcing such as the 2017 recommendations on outsourcing to cloud service providers,[34] the issue of systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed in 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.

(29) Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms enabling financial superiors to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Union oversight framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities.

(30) 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

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

inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules.

(31) In addition, 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 locally (via national initiatives) and with no consistent Union-wide information sharing arrangements tailored to the needs of an integrated financial sector.

(32) Financial entities should therefore be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements which, when conducted in trusted environments, would help the financial community to prevent and collectively respond to threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels. Those mechanisms should be conducted in full compliance with the applicable competition law rules of the Union[35] as well as in a way that guarantees the full respect of Union data protection rules, mainly Regulation (EU) 2016/679 of the European Parliament and of the Council,[36] 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.

(33) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into consideration significant differences between financial entities in terms of size, 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, 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.

(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities which are not 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 supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining 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

---

35 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.

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

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.

(35) Moreover, as solely those financial entities identified as significant for the purposes of the advanced digital resilience testing should be required to conduct threat led penetration tests, the administrative processes and financial costs entailed by the performance of such tests should be devolved to a small percentage of financial entities. Finally, 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 post-incident reviews after significant ICT disruptions.

(36) To ensure full alignment and overall consistency between financial entities' business strategies, on the one hand, and the conduct of ICT risk management, on the other hand, the management body should be required to maintain a pivotal and active role in steering and adapting the ICT risk management framework and the overall digital resilience strategy. The approach to be taken by the management body should not only focus on the means to ensure the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness over cyber risks and a commitment to respect a strict cyber hygiene at all levels.

The ultimate responsibility of the management body in managing a financial entity's ICT risks should be an overarching principle of that comprehensive approach, further translated into the continuous engagement of the management body in the control of the monitoring of the ICT risk management.

(37) Moreover, the management body's full accountability goes hand in hand with securing a level of ICT investments and overall budget for the financial entity to be able to achieve its digital operational resilience baseline.

(38) Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk,[37] 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.

(39) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and endowed with sufficient capacity not only to guarantee the processing of data as it is necessary for the performance of their services, but also to ensure technological resilience allowing 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

[37] 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.

standardization of specific ICT systems, tools or technologies, it relies on the financial entities' suitable use of European and internationally recognised technical standards (e.g. ISO) or industry best practices, insofar as such use is fully compliant with specific supervisory instructions on the use and incorporation of international standards.

(40) Efficient business continuity and recovery plans are required to allow financial entities to promptly and quickly resolve ICT-related incidents, in particular cyber-attacks, by limiting damage and giving priority to the resumption of activities and recovery actions. However, while backup systems should begin processing without undue delay, such start should in no way jeopardise the integrity and security of the network and information systems or the confidentiality of data.

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

(42) 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 and to prevent 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.

ICT-related incident reporting should be harmonised for all financial entities by requiring them to report to their competent authorities only. 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 anonymised data on threats and vulnerabilities relating to an event to aid wider collective defence.

(43) Further reflection on the possible centralisation of ICT-related incident reports should be envisaged, by means of a single central EU 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. The ESAs should be required to prepare, in consultation with ECB and ENISA, by a certain date a joint report exploring the feasibility of setting up such a central EU Hub.

(44) 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, 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, central securities depositories, central counterparties, 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. TLPT) 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.

(45) To ensure a sound monitoring of ICT third-party risk, it is necessary to lay down 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.

(46) 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 organised 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, on the basis of a careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.

(47) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated 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 established by this Regulation, financial supervisors should regularly receive essential information from the Registers and should be able to request extracts thereof on an ad-hoc basis.

(48) 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.

(49) To address the systemic impact of ICT third-party concentration risk, a balanced solution through a flexible and gradual approach should be promoted since rigid caps or strict limitations may hinder business conduct and contractual freedom. 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. At this stage, and with a view to strike a fair balance between the imperative of preserving contractual freedom and that of guaranteeing

financial stability, it is not considered appropriate to provide for strict caps and limits to ICT third-party exposures. The ESA designated to conduct the oversight for each critical ICT third-party provider ("the Lead Overseer") 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 in the Union is likely to put a strain on the Union financial system's stability and integrity and should provide instead for a dialogue with critical ICT third-party service providers where that risk is identified.[38]

(50) 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, there should be a harmonisation of key contractual elements throughout the performance of contracts with ICT third-party providers. Those elements only cover minimum contractual aspects considered crucial for enabling full monitoring by the financial entity from the perspective of ensuring its digital resilience reliant on the stability and security of the ICT service.

(51) 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 third party risk.

(52) 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 set out 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, including the provision of assistance by the latter in case of an ICT-related incident at no additional cost or at a cost that is determined ex-ante.

(53) 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 the latter's full cooperation during inspections. In the same vein, the competent authority of the financial entity should have those rights, based on notices, to inspect and audit the ICT third-party service provider, subject to confidentiality.

(54) Contractual arrangements should provide for clear termination rights and related minimum notices 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 allow the latter to effectively switch to other ICT third-

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

party service providers, or alternatively resort to the use of on-premises solutions, consistent with the complexity of the provided service.

(55) 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 envisaged 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.

(56) With a view to promote convergence and efficiency in relation to supervisory approaches to ICT third-party risk to the financial sector, strengthen the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the performance of operational functions, and thus to contribute to preserving the Union's financial system stability, the integrity of the single market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework.

(57) Since only critical third-party service providers warrant a special treatment, a designation mechanism for the purposes of applying the Union Oversight Framework should be put in place to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers, which translates into a set of quantitative and qualitative criteria that would set the criticality parameters as a basis for inclusion into the Oversight. Critical ICT third-party service providers which are not automatically designated by virtue of the application of the above-mentioned criteria should have the possibility to voluntary opt-in to the Oversight Framework, while those ICT third-party providers already subject to oversight mechanisms frameworks established at Eurosystem level with the aim to supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union should consequently be exempted.

(58) The requirement of legal incorporation in the Union of ICT third-party service providers which have been designated as critical does not amount to data localisation since this Regulation does not entail any further requirement on data storage or processing to be undertaken in Union.

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

(60) 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 matters pertaining to 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 critical ICT third-party service providers and collective recommendations, notably on benchmarking the oversight programs of critical ICT third-party service providers, and identifying best practices for addressing ICT concentration risk issues.

(61) To ensure that ICT third-party service providers fulfilling a critical role to the functioning of the financial sector are commensurately overseen on a Union scale, one of the ESAs should be designated as Lead Overseer for each critical ICT third-party service provider.

(62) Lead Overseers should enjoy the necessary powers to conduct investigations, onsite and offsite inspections at critical ICT third-party service providers, access all relevant premises and locations and obtain complete and updated information to enable them to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to the financial entities and ultimately to the Union's financial system.

Entrusting the ESAs with the lead oversight is a prerequisite for grasping and addressing the systemic dimension of ICT risk in finance. The Union footprint of critical ICT third-party service providers and the potential issues of ICT concentration risk attached to it call for taking a collective approach exercised at Union level. The exercise of multiple audits and access rights, conducted by numerous competent authorities in separation with little or no coordination would not lead to a complete overview on ICT third-party risk while creating unnecessary redundancy, burden and complexity at the level of critical ICT third-party providers facing such numerous requests.

(63) In addition, Lead Overseers should be able to submit recommendations on ICT risk matters and suitable remedies, including opposing certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system. Compliance with such substantive recommendations laid down by the Lead Overseers should be duly taken into account by national competent authorities as part of their function relating to the prudential supervision of financial entities.

(64) The Oversight Framework 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 critical ICT third-party service providers, 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. To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring the critical ICT third-party service provider's risks Any such measures should be previously coordinated and agreed in in the context of the Oversight Framework.

(65) To promote convergence at international level on best practices to be used in the review of ICT third-party service providers' digital risk-management, the ESAs should be encouraged to conclude cooperation arrangements with the relevant supervisory and regulatory third-country competent authorities to facilitate the development of best practices addressing ICT third-party risk.

(66) 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 critical ICT third-party service provider, pooling together multidisciplinary teams to supporting both the preparation and the actual execution of oversight activities, including onsite inspections of critical ICT third-party service providers, as well as needed follow-up thereof.

(67) 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 ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013[39], and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities.

(68) In order to further quantify and qualify the designation criteria for critical ICT third-party service providers and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of: further specifying the systemic impact that a failure of an ICT third-party provider could have on the financial entities it serves, the numbers of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider, the number of ICT third-party service providers active on a specific market, the costs of migrating to another ICT third-party service provider, the number of Member States in which the relevant ICT third-party service provider provides services and in which financial entities using the relevant ICT third-party service provider are operating, as well as the amount of the oversight fees and the way in which they are to be paid.

It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.[40] In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(69) Since this Regulation, together with Directive (EU) 20xx/xx of the European Parliament and of the Council,[41] entails a consolidation of the ICT risk management provisions spanning across multiple regulations and directives of the Union's financial services acquis, including Regulations (EC) No 1060/2009, (EU) No 648/2012 (EU) No 600/2014 and (EU) No 909/2014, in order to ensure full consistency, those Regulations should be amended to clarify that the relevant ICT risk-related provisions are laid down in this Regulation.

Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. As bodies with highly specialised expertise, the ESAs should be mandated to develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk.

---

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

40 OJ L 123, 12.5.2016, p. 1.

41 [*Please insert full reference*]

(70) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to the nature, scale and complexity of those entities and their activities.

(71) To facilitate the comparability of major ICT-related incident reports and to ensure transparency on contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should be mandated to develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident, as well as standardized templates for the register of information. When developing those standards, the ESAs should take into account the size and complexity of financial entities, as well as the nature and level of risk of their activities. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively. Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, respectively, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.

(72) This exercise will entail the subsequent 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 digital operational resilience which are today part of those Regulations.

(73) Since the objectives of this Regulation, namely to achieve a high level of digital operational resilience applicable to all financial entities, cannot be sufficiently achieved by the Member States because they require the harmonisation of a multitude of different rules, currently existing either in some Union acts, either in the legal systems of the various Member States, but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

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

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

   – Information and Communication Technology (ICT) risk management;

   – reporting of major ICT-related incidents 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) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

   (c) the oversight framework for critical ICT third-party service providers when providing services to financial entities;

   (d) rules on cooperation among competent authorities and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

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

Article 2

Personal scope

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,

(u) ICT third-party service providers.

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

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 point (2) of Article 4 of Directive (EU) No 2016/1148;

(4) 'ICT risk' means any reasonably identifiable circumstance in relation to the use of network and information systems, - including a malfunction, capacity overrun, failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialised, 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 of the European Parliament and of the Council[42];

(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’ 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 entity’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 centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication

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

services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council[43];

(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 continuity of its services and activities;

(18) 'critical ICT third-party service provider' means an ICT third-party service provider designated in accordance with Article 29 and subject to the Oversight Framework referred to in Articles 30 to 37;

(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;

(21) 'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of the latter may potentially endanger the ability of a financial entity, 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;

(22) 'management body' means a management body as defined in point (36) of Article 4(1) of Directive 2014/65/EU, point (7) of Article 3(1) of Directive 2013/36/EU, point (s) of Article 2(1) of Directive 2009/65/EC, point (45) of Article 2(1) of Regulation (EU) No 909/2014, point (20) of Article 3(1) of Regulation (EU) 2016/1011 of the European Parliament and of the Council[44], point (u) of Article 3(1) of Regulation (EU) 20xx/xx of the European Parliament and of the Council[45] [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation;

---

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

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

45 [*please insert full title and OJ details*]

(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[46];

(24) ‘investment firm’ means an investment firm as defined in point (1) of 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 of the European Parliament and of the Council[47];

(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;

---

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

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

(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 Directive 2006/43/EC;

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

(43) ‘crypto-asset service provider’ means crypto-asset service provider as defined in point (n) of Article 3(1) of Regulation (EU) 202x/xx [*PO: 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 (EU) 202x/xx [*PO: 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 the Annex to 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 the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework referred to in Article 5(1):

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

(a) bear the 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 risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9);

(d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan referred to in, respectively, 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 of 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, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;

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

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

4. Members of the management body 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

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 comprehensively and to ensure a high level of digital operational resilience that matches their business needs, size and complexity.

2. The ICT risk management framework referred to in paragraph 1 shall include strategies, policies, procedures, 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 and sensitive designated areas, to ensure that all those physical elements are adequately protected from risks including damage and unauthorized access or usage.

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

4. As part of the ICT risk management framework referred to in paragraph 1, 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 on the basis of lessons derived from implementation and monitoring.

7. The ICT risk management framework referred to in paragraph 1 shall be audited on a regular basis 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) implementing digital operational resilience testing;

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

10. Upon approval of competent authorities, financial entities may delegate the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings.

Article 6

ICT systems, protocols and tools

1. Financial entities shall use and maintain updated ICT systems, protocols and tools, which fulfil the following conditions:

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

(b) they are reliable;

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

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

2. Where financial entities use internationally recognized technical standards and industry leading practices on information security and ICT internal controls, they shall use those standards and practices in line with any relevant supervisory recommendation on their incorporation.

Article 7

Identification

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed, and 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 ICT-related business functions and information assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.

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

4. Financial entities shall identify all ICT systems accounts, including those on remote sites, the network resources and 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 relevant inventories.

7. Financial entities other than microenterprises shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems, 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 minimise the impact of such risks through the deployment of appropriate ICT security tools, policies and procedures.

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

3. To achieve the objectives referred to in paragraph 2, financial entities shall use state-of-the-art ICT technology and processes which:

   (a) guarantee the security of the means of transfer of information;

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

   (c) prevent information leakage;

   (d) ensure that 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) 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;

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

(e) 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;

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

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

For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.

Article 9

Detection

1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify 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, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors and request re-transmission of any such erroneous reports.

Article 10

Response and recovery

1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy of the financial entity.

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

   (a) 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 prioritises resumption of activities and recovery actions;

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

   (e) estimating preliminary impacts, damages and losses;

   (f) setting out communication and crisis management actions 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, 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 Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to the ICT systems;

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

   For the purposes of point (a), financial entities other than microenterprises shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 11.

   Financial entities shall regularly review their ICT Business Continuity Policy and ICT Disaster Recovery Plan taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.

6. Financial entities other than microenterprises shall have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13.

7. Financial entities shall keep records of activities before and during disruption events when their ICT Business Continuity Policy or ICT Disaster Recovery Plan is activated. Such records shall be readily available.

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

9. Financial entities other than microenterprises shall report to competent authorities 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 ICT 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 ICT 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 financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.

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 entities referred to 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:

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

(b) capable of ensuring the continuity of critical 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;

(c) 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, financial entities shall perform multiple checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

Article 12

Learning and evolving

1. Financial entities shall have in place capabilities and staff, suited to their size, business and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.

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

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

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

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

(b) the quality and speed in performing forensic analysis;

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

(d) the effectiveness of internal and external communication.

3. Lessons derived from the digital operation resilience testing carried out in accordance with Articles 23 and 24 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of business continuity or recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework referred to in Article 5(1).

4. Financial entities shall monitor the effectiveness of the implementation of their digital resilience strategy set out in Article 5(9). They shall map the evolution of ICT risks over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understand the level of ICT risk exposure and enhance the cyber maturity and preparedness of the financial entity.

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

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

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

Article 13

Communication

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of 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 the role of public and media spokesperson for that purpose.

Article 14

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

The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) shall, in consultation with the European Union Agency on Cybersecurity (ENISA), develop draft regulatory technical standards for the following purposes:

(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the 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 policies, procedures and tools 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 provide 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 Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;

(f) specify further the components of the ICT Business Continuity Policy referred to in Article 10(1);

(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to ensure that it duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency or other failures of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;

(h) specify further the components of the ICT Disaster Recovery Plan 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 Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.

CHAPTER III

ICT-RELATED INCIDENTS

MANAGEMENT, CLASSIFICATION and REPORTING

Article 15

ICT-related incident management process

1. Financial entities shall 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 referred to in Article 16(1);

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

(c) set out plans for communication to staff, external stakeholders and media in accordance with Article 13, and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;

(d) ensure that 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 established 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 the following criteria:

(a) the number of users or financial counterparts affected by the disruption caused by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;

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

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

(d) the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss;

(e) the severity of the impact of the ICT-related incident on the financial entity's ICT systems;

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

(g) the economic impact of the ICT-related incident in both absolute and relative terms.

2. The ESAs shall, through the Joint Committee of the ESAs (the 'Joint Committee') and after consultation with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards further specifying the following:

(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents which are subject to the reporting obligation laid down in Article 17(1);

(b) the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents to other Member States' jurisdictions, and the details of ICT-related incidents reports to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.

3. When developing 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.

The ESAs shall submit those common draft regulatory technical standards to the Commission by [*PO: 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 paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.

Article 17

Reporting of major ICT-related incidents

1. Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 41, within the time-limits laid down in paragraph 3.

For the purpose of the first subparagraph, financial entities 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. Financial entities shall submit to the competent authority as referred to in Article 41:

(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 a specific request of the competent authority;

(c) a final report, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates, but not later than one month from the moment of sending the initial report

4. Financial entities may only delegate the reporting obligations under this Article to a third-party service provider upon approval of the delegation by the relevant competent authority referred to in Article 41.

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) EBA, ESMA or EIOPA, as appropriate;

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

   (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

1. 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:

      (1) establish the content of the reporting for major ICT-related incidents;

      (2) 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 paragraph 1 and the common draft implementing technical standards referred to in point (b) of the paragraph 1 to the Commission by xx 202x [*PO: insert date 1 year after the date of entry into force*].

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

   Power is conferred on the Commission to adopt the common implementing technical standards referred to in point (b) of paragraph 1 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 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 referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [*OJ: insert date 3 years after the date of entry into force*].

Article 20

Supervisory feedback

1. Upon receipt of a report as 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 yearly 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.

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.

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

3. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme referred to in paragraph 1, 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.

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

5. 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.

6. Financial entities shall test all critical ICT systems and applications at least yearly.

Article 22

Testing of ICT tools and systems

1. The digital operational resilience testing programme referred to in Article 21 shall provide for the 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.

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

Article 23

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

1. Financial entities identified in accordance with paragraph 4 shall carry out at least every 3 years advanced testing by means of threat led penetration testing.

2. Threat led penetration testing 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 threat led penetration testing, 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 threat led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers.

   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.

   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 threat led penetration testing has been conducted in accordance with the requirements. Competent authorities shall validate the documentation and issue an attestation.

3. Financial entities shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.

   Competent authorities shall identify financial entities to perform threat led penetration testing in a manner that is proportionate to the size, scale, activity and overall risk profile of the financial entity, based on the assessment of the following:

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

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

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

4. 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) the requirements in relation to:

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

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

(iii) the results, closure and remediation stages of the testing;

(c) the type of supervisory cooperation needed for the implementation of threat led penetration testing in the context of financial entities which operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets..

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

(a) are of the highest suitability and reputability;

(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing 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 threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;

(e) 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 threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.

CHAPTER V

MANAGING OF ICT THIRD-PARTY RISK

SECTION I

KEY PRINCIPLES FOR A SOUND MANAGEMENT OF ICT THIRD PARTY RISK

Article 25

General principles

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

1. Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.

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

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

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

3. As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in point (g) of Article 5(9). That strategy shall include a policy 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 outsourcing of critical or important functions.

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

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

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

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

Financial entities shall inform the competent authority in a timely manner about planned contracting of critical or important functions and when a function has become critical or important.

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

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

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

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

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

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

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

   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 possess appropriate skills and knowledge to effectively perform relevant audits and assessments.

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under 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) circumstances where the competent authority can no longer effectively supervise the financial entity as a result of the respective contractual arrangement.

9. 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 that they are able to exit contractual arrangements without:

(a) disruption to their business activities,

(b) limiting compliance with regulatory requirements,

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

Exit plans shall be comprehensive, documented and, 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 them in-house.

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

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

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 [*PO: 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 26

Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements

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

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

   (b) having in place multiple contractual arrangements in relation to the provision of 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 providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.

2. Where the contractual arrangement on the use of ICT services 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, at least the following factors:

   (a) the respect of data protection;

   (b) the effective enforcement of the law;

   (c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy;

   (d) 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 27

Key contractual provisions

1. The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in a writing. The full contract, which includes the services level agreements, shall be documented in one 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 the following:

(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 to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity if it envisages changing such locations;

(c) provisions on accessibility, availability, integrity, security and protection of personal data and on 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 to 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) rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

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

  iii) the commitment to fully cooperate 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, including 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 shall consider the use of 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 sub-contracting 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, respectively.

SECTION II

OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS

Article 28

Designation of critical ICT third-party service providers

1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall:

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

(b) appoint either EBA, ESMA or EIOPA as Lead Overseer for each critical ICT third-party service provider, depending on whether the total value of assets of financial entities making use of the services of that critical ICT third-party service provider and which are covered by one of the Regulations (EU) No 1093/2010 (EU), No 1094/2010 or (EU) No 1095/2010 respectively, represents more than a half of the value of the total assets of all financial entities making use of the services of the critical ICT third-party service provider, as evidenced by the consolidated balance sheets, or the individual balance sheets where balance sheets are not consolidated, of those financial entities.

2. The designation referred to in point (a) of paragraph 1 shall be based on all of the following criteria:

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

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

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

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

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

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

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

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

(e) the number of Member States in which the relevant ICT third-party service provider provides services;

(f) the number of Member States in which financial entities using the relevant ICT third-party service provider are operating.

3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement the criteria referred to in paragraph 2.

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

5. The designation mechanism referred to in point (a) of paragraph 1 shall not apply in relation to ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union.

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

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

8. ICT third-party service providers that are not included in the list referred to in paragraph 6 may request to be included in that list.

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

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

9. Financial entities shall not make use of an ICT third-party service provider established in a third country that would be designated as critical pursuant to point (a) of paragraph 1 if it were established in the Union.

Article 29

Structure of the Oversight Framework

1. The Joint Committee, in accordance with Article 57 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and the Lead Overseer referred to in point (b) of Article 28(1) in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and common acts of the Joint Committee in that area.

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

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

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

3. The Oversight Forum shall be composed of the Chairpersons of the ESAs, and one high-level representative from the current staff of the relevant competent authority from each Member State. The Executive Directors of each ESA and one representative from the European Commission, from the ESRB, from ECB and from ENISA shall participate in the Oversight Forum as observers.

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

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

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

Article 30

Tasks of the Lead Overseer

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

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

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

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

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

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

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

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

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

   (h) the ICT audits;

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

3. Based on the assessment referred to in paragraph 1, the Lead Overseer shall adopt a clear, detailed and reasoned individual Oversight plan for each critical ICT third-

party service provider. That plan shall be communicated each year to the critical ICT third-party service provider.

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

Article 31

Powers of the Lead Overseer

1. For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers:

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

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

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

   (d) to address recommendations on the areas referred to in Article 30(2), in particular concerning the following:

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

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

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

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

         – the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country;

         – the subcontracting concerns a critical or important function of the financial entity.

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

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

4. The Lead Overseer may impose a periodic penalty payment to compel the critical ICT third-party service provider to comply with points (a), (b) and (c) of paragraph 1.

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

6. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be 1% of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year.

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

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

9. Before imposing a periodic penalty payment under paragraph 4, the Lead Overseer shall give the representatives of the critical ICT third-party provider subject to the proceedings the opportunity to be heard on the findings and shall base its decisions only on findings on which the critical ICT third-party provider subject to the proceedings has had an opportunity to comment. The rights of the defence of the persons subject to the proceedings shall be fully respected in the proceedings. They shall be entitled to have access to file, subject to the legitimate interest of other persons in the protection of their business secrets. The right of access to the file shall not extend to confidential information or Lead Overseer's internal preparatory documents.

Article 32

Request for information

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

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

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

(b) state the purpose of the request;

(c) specify what information is required;

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

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

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

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

(b) state the purpose of the request;

(c) specify what information is required;

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

(e) indicate the periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete;

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

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

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

Article 33

General investigations

1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the examination team referred to in Article 34(1), may conduct the necessary investigations of ICT third-party service providers:

2. The Lead Overseer shall be empowered to:

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

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

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

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

(e) request records of telephone and data traffic.

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

That authorisation shall also indicate the periodic penalty payments provided for in Article 31(4) where the production of the required records, data, procedures or any other material, or the answers to questions asked to representatives of the ICT third - party service provider are not provided or are incomplete.

4. The representatives of the ICT third-party service providers are required to submit to the investigations on the basis of a decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the investigation, the periodic penalty payments provided for in Article 31(4), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 and the right to have the decision reviewed by the Court of Justice.

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

Article 34
On-site inspections

1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the examination teams referred to in Article 35(1), may enter and conduct all necessary on-site inspections on any business premises, land or property of the ICT third-party providers, such as head offices, operation centres, secondary premises, as well as to conduct off-line inspections.

2. The officials and other persons authorised by the Lead Overseer to conduct an on-site inspection, may enter any such business premises, land or property and shall have all the powers to seal any business premises and books or records for the period of, and to the extent necessary for, the inspection.

They shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection and the periodic penalty payments provided for in Article 31(4) where the representatives of the ICT third-party service providers concerned do not submit to the inspection.

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

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

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

6. The critical ICT third-party service provider shall submit to on-site inspections ordered by decision of the Lead Overseer. The decision shall specify the subject

matter and purpose of the inspection, appoint the date on which it is to begin and indicate the periodic penalty payments provided for in Article 31(4), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, as well as the right to have the decision reviewed by the Court of Justice.

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

Article 35
Ongoing Oversight

1. Where conducting general investigations or on-site inspections, the Lead Overseers shall be assisted by an examination team established for each critical ICT third-party service provider.

2. The joint examination team referred to in paragraph 1 shall be composed of staff members from the Lead Overseer and from the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides services, who will join the preparation and execution of the Oversight activities, with a maximum of 10 members. All members of the joint examination shall have expertise in ICT and operational risk. The joint examination team shall work under the coordination of a designated ESA staff member (the 'Lead Overseer coordinator').

3. The ESAs, through the Joint Committee, shall develop common draft regulatory technical standards to specify further the designation of the members of the joint examination team coming from the relevant competent authorities, as well as the tasks and working arrangements of the examination team. 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 adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.

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

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

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

Article 36

Harmonisation of conditions enabling the conduct of the Oversight

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

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

   (b) the content and format of reports which may be requested for the purposes of point (c) of Article 31(1);

   (c) the presentation of the information, including the structure, formats and methods that a critical ICT third-party service provider shall be required to submit, disclose or report pursuant to Article 31(1);

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

2. The ESAs shall submit those draft regulatory technical standards to the Commission by 1 January 20xx [*OJ: insert date 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 37

Follow-up by competent authorities

1. Within 30 calendar days after the receipt of the recommendations issued by Lead Overseers pursuant to point (d) of Article 31(1), critical ICT third-party service providers shall notify the Lead Overseer whether they intend to follow those recommendations. Lead Overseers shall immediately transmit this information to competent authorities.

2. Competent authorities shall monitor whether financial entities take into account the risks identified in the recommendations addressed to critical ICT third-party providers by the Lead Overseer in accordance with points (d) of Article 31(1).

3. Competent authorities may, in accordance with Article 44, require financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party provider until the risks identified in the recommendations addressed to critical ICT third-party providers have been addressed. Where necessary, they may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.

4. When taking the decisions referred to in paragraph 3, competent authorities shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

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

(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;

(c) whether financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;

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

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

Article 38
Oversight fees

1. The ESAs shall charge critical ICT third-party service providers 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 activities in accordance with Article 35.

The amount of a fee charged to a critical ICT third-party service provider shall cover all administrative costs and shall be proportionate to their turnover.

2. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid.

Article 39
International cooperation

1. EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, notably by developing best practices for the review of ICT risk-management practices and controls, mitigation measures and incident responses.

2. The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission summarising the findings of relevant discussions held with the third countries authorities referred to in paragraph 1, focussing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection or the functioning of the single market.

CHAPTER VI

INFORMATION SHARING ARRANGEMENTS

Article 40

Information-sharing arrangements on cyber threat information and intelligence

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

   (a) aims at enhancing the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting 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[48] and guidelines on competition policy.[49]

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

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

CHAPTER VII

COMPETENT AUTHORITIES

Article 41

Competent authorities

Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Section II of Chapter V of this Regulation,

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

[49] 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.

compliance with the obligations set out in this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:

(a) for credit institutions, the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, 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, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens, the competent authority designated in accordance with the first indent of point (ee) of Article 3 (1) of [*Regulation (EU) 20xx MICA Regulation*];

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

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

(h) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU;

(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 42

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

1. To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs and the competent authorities, may request to be invited to the workings of Cooperation Group.

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

Article 43

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 establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors.

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

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

2. Competent authorities, EBA, ESMA or EIOPA and the ECB shall cooperate closely with each other and exchange information to carry out their duties pursuant to Articles 42 to 48. They shall closely coordinate their supervision in order to identify and remedy breaches of this Regulation, develop and promote best practices, facilitate collaboration, foster consistency of interpretation and provide cross-jurisdictional assessments in the event of any disagreements.

Article 44

Administrative penalties and remedial measures

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

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

   (a) have access to any document or data held in any form 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 46, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.

Those penalties and measures shall be effective, proportionate and dissuasive.

4. Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation:

(a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;

(b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;

(c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;

(d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and

(e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.

5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.

6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.

Article 45

Exercise of the power to impose administrative penalties and remedial measures

1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 44 in accordance with their national legal frameworks, as appropriate:

(a) directly;

(b) in collaboration with other authorities;

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

(d) by application to the competent judicial authorities.

2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate:

(a) the materiality, gravity and the duration of the breach;

(b) the degree of responsibility of the natural or legal person responsible for the breach;

(c) the financial strength of the responsible natural or legal person;

(d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;

(e) the losses for third parties caused by the breach, insofar as they can be determined;

(f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses avoided by that person;

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

Article 46

Criminal penalties

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

2. Where Member States have chosen to lay down criminal penalties for breaches of this Regulation they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other competent authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.

Article 47

Notification duties

Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by [*OJ: insert date 1 year after the date of entry into force*]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.

Article 48

Publication of administrative penalties

1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the addressee of the sanction has been notified of that decision.

2. The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the identity of the persons responsible and the penalties imposed.

3. Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt either of the following solutions in respect to the decision imposing an administrative sanction:

   (a) defer its publication until the moment where all reasons for non-publication cease to exist;

   (b) publish it on an anonymous basis, in accordance with national law; or

   (c) refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportional with the leniency of the imposed sanction.

4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with point (b) of paragraph 3, the publication of the relevant data may be postponed.

5. Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and at later stages any subsequent related information on the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.

6. Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website 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.

Article 49

Professional secrecy

1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.

2. The obligation of professional secrecy applies to all persons who work or who have worked for the competent authorities under this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.

3. Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law.

4. All information exchanged between the competent authorities under this Regulation that concerns business or operational conditions and other economic or personal

affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states at the time of communication that such information may be disclosed or where such disclosure is necessary for legal proceedings.

CHAPTER VIII

DELEGATED ACTS

Article 50

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 28(3) and 38(2) shall be conferred on the Commission for a period of five years from [PO: insert date 5 years after the date of entry into force of this Regulation].

3. The delegation of power referred to in Articles 28(3) and 38(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

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

6. A delegated act adopted pursuant to Articles 28(3) and 38(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of 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 51

Review clause

By [*PO: insert date 5 years after the date of entry into force of this Regulation*], the Commission shall, after consulting EBA, ESMA, EIOPA, and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council, accompanied, if appropriate, by a legislative proposal, regarding the criteria for the designation of critical ICT third-party service providers in Article 28(2).

SECTION II

AMENDMENTS

Article 52

Amendments to Regulation (EC) No 1060/2009

In Annex I to Regulation (EC) No 1060/2009, the first subparagraph of point 4 of Section A is replaced by the following:

> ‘A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].
>
> * Regulation (EU) 2021/xx of the European Parliament and of the Council […] (OJ L XX, DD.MM.YYYY, p. X).’.

Article 53

Amendments to Regulation (EU) No 648/2012

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

(1) Article 26 is amended as follows:

(a) paragraph 3 is replaced by the following:

> ‘3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].

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

(b) paragraph 6 is deleted;

(2) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.';

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

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

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

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

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

'1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx *[DORA*].

2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity and disaster recovery plans established in accordance with Regulation (EU) 2021/xx*[DORA],* aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations.';

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

Article 54

Amendments to Regulation (EU) No 909/2014

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

(1) paragraph 1 is replaced by the following:

'1. A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the

Council*[*DORA*], as well as through any other relevant appropriate tools, controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.

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

(2) paragraph 2 is deleted;

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

'3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity and disaster recovery plan, including ICT business continuity and disaster recovery plans established in accordance with Regulation (EU) 2021/xx [DORA], to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations.

4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in paragraphs (5) and (7) of Article 11 of Regulation (EU) 2021/xx [DORA].';

(4) in paragraph 6, the first subparagraph is replaced by the following*:*

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

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

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

Article 55

Amendments to Regulation (EU) No 600/2014

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

(1) Article 27g is amended as follows:

(a) paragraph 4 is deleted;

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

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

(2) Article 27h is amended as follows:

(a) paragraph 5 is deleted;

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

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

(3) Article 27i is amended as follows:

(a) paragraph 3 is deleted;

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

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

Article 56

Entry into force and application

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

It shall apply from [*PO: insert date - 12 months after the date of entry into force*].

However, Articles 23 and 24 shall apply from [*PO: insert date - 36 months after the date of entry into force of this Regulation*].

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

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system(s)

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on appropriations

3.2.3. Estimated impact on human resources

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

Annex

General Assumptions

Oversight powers

LEGISLATIVE FINANCIAL STATEMENT 'AGENCIES'

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council on the Digital Operational Resilience of the financial sector.

1.2. Policy area(s) concerned

Policy area: Financial stability, financial services and capital markets union

Activity: Digital Operational Resilience

1.3. The proposal relates to

☑ **a new action**

☐ **a new action following a pilot project/preparatory action**[50]

☐ **the extension of an existing action**

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

1.4. Objective(s)

1.4.1. 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.

1.4.2. Specific objective(s)

The proposal has the following specific objectives:

Address information and communication technologies ("ICT") risks more comprehensively and strengthen the overall level of digital resilience of the financial sector;

Streamline ICT-related incident reporting and address overlapping reporting requirements;

Enable financial supervisors' access to information on ICT-related incidents;

Ensure that financial entities covered by this proposal assess the effectiveness of their preventive and resilience measures and identify ICT related vulnerabilities;

Reduce single market fragmentation and enable cross-border acceptance of testing results.

Strengthen the contractual safeguards for financial entities when using ICT services, including for outsourcing rules (governing the monitoring of ICT third-party providers ("TPPs"));

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

Enable an oversight of the activities of critical ICT TPPs; Incentivise the exchange of threat intelligence in the financial sector.

1.4.3. 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 covering all digital operational resilience aspects and would be effective in improving the overall 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 bring clarity to financial entities on the different rules on digital operational resilience they need to comply with, in particular for those financial entities holding several authorisations and operating in different markets within the EU.

1.4.4. 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-related incidents reported to prudential supervisors

Number of financial entities that would be required to perform threat-led penetration tests ("TLPT")

Number of financial entities using Standard Contractual Clauses to enter into contractual arrangements with ICT TPPs

Number of critical ICT TPPs overseen by the ESAs/prudential supervisors

Number of financial entities participating in threat intelligence sharing solutions

Number of authorities to receive reports on the same ICT-related incident

Number of cross-border TLPTs

1.5. Grounds for the proposal/initiative

1.5.1. 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 requirements 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 parties.

1.5.2. 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 adding these operational provisions on ICT risk, the Single Rulebook would provide the tools to tackle all other types of risks at European level, but would leave out the digital operational resilience aspects or would subject them 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 current limited coverage of EU rules and the general nature of the NIS Directive.

Expected generated Union added value (ex-post):

The Union intervention would significantly increase the effectiveness of the policy while also reducing complexity and easing the financial and administrative burden on all financial entities. It would harmonise an area of the economy that is so deeply interconnected and integrated and that already benefits from a single set of rules and supervision. In terms of ICT-related incident reporting, the proposal would reduce the reporting burden - and 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 multiple testing frameworks in different Member States.

1.5.3. Lessons learned from similar experiences in the past

New initiative

1.5.4. 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 three financial sub-sectors within the scope of the NIS Directive. By remaining associated to the NIS ecosystem, financial supervisors would be able to exchange relevant information with NIS authorities and participate in the NIS Cooperation Group. The proposal would not impact the NIS Directive but rather build on it and address possible overlaps via a lex specialis exemption. The interaction between the financial services regulation and the NIS Directive would continue to be governed by a lex specialis clause, thus exempting financial entities from substantive requirements in the NIS Directive and avoiding overlaps between the two acts. In addition, the proposal is consistent with the European Critical Infrastructure (ECI) Directive, currently under revision to enhance the protection and resilience of critical infrastructure against non-cyber threats.

This proposal would not have an impact on the Multiannual Financial Framework (MFF). First, the Oversight Framework of critical ICT third-party providers will be fully funded by fees levied from these providers; second, the additional regulatory tasks related to digital operational resilience entrusted to the ESAs will be ensured by internal redeployment of existing staff.

This will translate into a proposal to increase the authorised staff of the agency during the future annual budgetary procedure. The agency will continue to work towards maximising synergies and efficiency gains (inter alia via IT systems), and closely monitor the additional workload associated with this proposal, which would be reflected in the level of authorised staff requested by the agency in the annual budgetary procedure.

1.5.5. 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 critical TPPs could not be met through a redeployment of resources within the ESAs which also have other tasks in addition to those envisaged under this proposal, as well as under other pieces of Union legislation. Moreover, supervisory tasks related to digital operational resilience require specific technical knowledge and expertise. As the current level of such resources at the ESAs is insufficient, additional resources are needed.

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

1.6. 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.

1.7. Management mode(s) planned[51]

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

[51] 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.

2. MANAGEMENT MEASURES

2.1. 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.

2.2. Management and control system(s)

2.2.1. 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 TPPs concerned.

2.2.2. 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 TPPs concerned.

2.2.3. 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 the ESAs 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.

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

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. 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.[52]	from EFTA countries[53]	from candidate countries[54]	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

[52] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[53] EFTA: European Free Trade Association.

[54] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

3.3. 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		

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 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 of the multiannual financial framework	Commitments							
	Payments							

3.3.1. 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[55]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[56] …																
- Output																
Subtotal for specific objective No 1																
SPECIFIC OBJECTIVE No 2 ...																
- Output																
Subtotal for specific objective No 2																
TOTAL COST																

55 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

56 As described in point 1.4.2. 'Specific objective(s)…'

3.3.2. Estimated impact on human resources

3.3.2.1. 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)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Temporary agents (AST grades)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Contract staff							
Seconded National Experts							
TOTAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Staff requirements (FTE):

EBA, EIOPA, ESMA & EEA	2022	2023	2024	2025	2026	2027	**TOTAL**
Temporary agents (AD Grades) EBA=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Temporary agents (AST grades) EBA=1, EIOPA=1, EEA=1	3	3	3	3	3	3	3
Contract staff							
Seconded National Experts							
TOTAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. 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)**[57]							
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***[58]	- at Headquarters[59]						
	- 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.

[57] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

[58] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

[59] Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

3.3.3. 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[60].

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

3.3.4. 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[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL appropriations co-financed	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the supervised entities[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL appropriations co-financed	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Total

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

61 100% of the total estimated cost plus the full employer's pension contributions

62 100% of the total estimated cost plus the full employer's pension contributions

The costs shall be covered 100% by fees levied from the supervised entities[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL appropriations co-financed	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Estimated impact on revenue

☑ 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[64]						
		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.

[…]

63 100% of the total estimated cost plus the full employer's pension contributions

64 As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

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:

- 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, which includes 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
- The additional Temporary Agents are AD5s and ASTs.

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 as of 2024 are estimated 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	

Constant Prices

EBA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Payments	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Title 2:	Commitments	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Payments	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
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	Commitments	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Payments	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Payments	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Title 2:	Commitments	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Payments	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
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	Commitments	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

for EIOPA	Payments	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Title 1:	Commitments	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Payments	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Title 2:	Commitments	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Payments	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
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	Commitments	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Payments	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

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[65]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[66] 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[67]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[68] Direct oversight of critical ICT TPPs																
- Output				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal for specific																

[65] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[66] As described in point 1.4.2. 'Specific objective(s)…'

[67] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[68] As described in point 1.4.2. 'Specific objective(s)…'

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[69]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[70] 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**

[69] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

[70] As described in point 1.4.2. 'Specific objective(s)…'

The 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[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL appropriations co-financed	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the overseen entities[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL appropriations co-financed	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Total
The costs shall be covered 100% by fees levied from the overseen entities[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL appropriations co-financed	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPECIFIC INFORMATION

Direct Oversight powers

By 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 Commission Delegated Regulation (EU) No 272/2012) and trade repositories (Commission Delegated Regulation (EU) No 1003/2013).

[71] 100% of the total estimated cost plus the full employer's pension contributions
[72] 100% of the total estimated cost plus the full employer's pension contributions
[73] 100% of the total estimated cost plus the full employer's pension contributions

Under this legislative proposal, the ESAs will be entrusted with new tasks aimed at promoting convergence on supervisory approaches to ICT third-party risk in the financial sector by subjecting critical ICT third party service providers 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 addressed to critical ICT third party service providers.

Through this framework, the ESAs designated as Lead Overseers for each critical ICT third party service provider 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 clarified in the explanatory memorandum. They include rights to request all relevant information and documentation to conduct general investigations and inspections, to address recommendations and subsequently submit reports on the actions taken or remedies implemented the address those recommendations.

In order to perform the new tasks envisaged by this proposal, additional staff specialised in ICT risk and focussing on assessing third-party dependencies shall therefore be hired by the ESAs.

Human resources needs can be estimated at 6 FTEs for each authority (5 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 each of the three ESAs for maintenance costs. One important element in the fulfilment of the new tasks are the 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 critical ICT third party service providers 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 levied by the ESAs from the overseen critical ICT third party service providers (no impact on EU Budget).