AMENDMENTS
157 - 765

Draft report
Billy Kelleher
(PE689.801v01-00)


Proposal for a regulation
Amendment 157
Alfred Sant, Carmen Avram
Proposal for a regulation
Recital 1

Text proposed by the Commission

(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.

Amendment

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are nowadays core features of all activities of Union financial entities, digital resilience has yet to be sufficiently built in their operational frameworks.

Or. en

Amendment 158
Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru
Proposal for a regulation
Recital 2

Text proposed by the Commission

(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

Amendment

(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.

The insurance sector has also been transformed by the use of ICT technology, from the emergence of digital insurance intermediaries operating with InsurTech to digital insurance underwriting and contract distribution. 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.

Amendment 159
 Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 4

Text proposed by the Commission

(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.

Amendment

(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. Consequently, it is necessary to consider cyber risk in the context of a highly interconnected global financial system in which consistency of international regulation and cooperation between competent authorities globally needs to be
Amendment 160
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 8

Text proposed by the Commission

(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.

Amendment

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

Amendment 161
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Recital 9

Text proposed by the Commission

(9) **Legislative disparities and uneven** national regulatory or supervisory approaches on ICT risk trigger obstacles to

Amendment

(9) **Lack of coordination and of interoperability between** national regulatory or supervisory approaches on
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.

ICT risk trigger obstacles to cross-border cyber resilience, impeding 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.

Amendment 162
Mikuláš Peksa on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 10 a (new)

Text proposed by the Commission

(10 a) Establishing and maintaining adequate network and information system infrastructures is also a fundamental precondition for effective risk data aggregation and risk reporting practices, which are in turn an essential requisite for the sound and sustainable risk management and decision-making processes of credit institutions. In 2013, the Basel Committee on Banking Supervision published a set of principles for effective risk data aggregation and risk reporting (‘BCBS 239’) based on two overarching principles of governance and IT infrastructure, to be implemented by the beginning of 2016. According to the Basel Progress Report of April 2020 and the ECB Report on the Thematic Review
of May 2018 on effective risk data aggregation and risk reporting, the implementation progress made by global systemically important banks was unsatisfactory and a source of concern. In order to facilitate compliance and alignment with international standards, the Commission, in close cooperation with the ECB and after consulting EBA and ESRB, should produce a report in order to assess how the BCBS 239 principles interact with the provisions of the DORA Regulation and, if appropriate, how those principles should be incorporated into Union law.

**Amendment 163**
Mikuláš Peksa
on behalf of the Greens/EFA Group

**Proposal for a regulation**
Recital 12 – point 1

*Text proposed by the Commission*

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.

*Amendment*

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. *This initiative also intends to raise awareness of ICT risks and acknowledges that ICT incidents and lack of operational resilience might jeopardise the financial soundness of financial entities.*
Amendment 164
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 13 – introductory part

**Text proposed by the Commission**

(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.

**Amendment**

(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk, *according to their size, nature, complexity and risk profile*. 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.

Or. en

Amendment 165
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 13 – introductory part

**Text proposed by the Commission**

(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.

**Amendment**

(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 high reliance on ICT systems, platforms and infrastructures, which entails increased digital risk.

Or. en

Amendment 166
Gunnar Beck, Maximilian Krah, Jörg Meuthen
Proposal for a regulation
Recital 14

Text proposed by the Commission

(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.

Amendment 167
Alfred Sant, Carmen Avram

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission

(14 a) However, that approach should in no way be taken to mean that, in its implementation, this Regulation should serve to hamper innovation and flexibility with regard to how financial entities deal with resilience issues while complying with its provisions. Through dialogue with supervisory authorities, which should acknowledge the virtues of flexibility, there will be full scope for adaptation and innovation while fully maintaining a high level of resilience.
Amendment 168
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 16 – introductory part

Text proposed by the Commission

(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 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.

Amendment

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

Or. en

Amendment 169
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 16 – introductory part

Text proposed by the Commission

(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 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.

Amendment

(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 financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, for financial entities, this Regulation constitutes lex specialis to Directive (EU) 2016/1148.
Proposal for a regulation
Recital 17 – point 1

**Text proposed by the Commission**

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.

**Amendment**

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, in particular when finalising the Oversight plan for, or recommendations addressed to, critical ICT third-party service providers, in order to ensure that there are no inconsistencies or duplications with critical ICT third-party service providers' obligations under Directive (EU) 2016/1148.

---

**Amendment 171**

Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 18

**Text proposed by the Commission**

(18) It is also important to ensure consistency with the European Critical Infrastructure (ECI) Directive, which is

**Amendment**

(18) It is also important to ensure consistency with both 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, and the Directive on Resilience of Critical Entities, with possible implications for the financial sector.\textsuperscript{31}


Amendment 172
Alfred Sant

Proposal for a regulation
Recital 19

\textit{Text proposed by the Commission}

(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.

\textit{Amendment}

(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 \textit{and both substantive and procedural requirements applicable to critical ICT third-party service providers under this Regulation should be coherent and seamless with those applicable under that}
Directive. 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.

Or. en

Amendment 173
Markus Ferber

Proposal for a regulation
Recital 20

Text proposed by the Commission

(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.

Amendment

(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;

_________________


Or. en

Justification

The provisions should be applied in a proportionate matter to all entities in the scope.

Amendment 174
Alfred Sant

Proposal for a regulation
Recital 20

*Text proposed by the Commission*

(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\(^{32}\).


*Amendment*

(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 *and small* enterprises as defined in Commission recommendation 2003/361/EC\(^{32}\) also taking into account their nature, scale, complexity and overall risk profile.


Or. en

Amendment 175
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Recital 20 a (new)

*Text proposed by the Commission*

(20 a) Where financial entities are required to report ICT-related incidents under this Regulation or under other Union or national law, the competent authorities should ensure that the reporting process is streamlined and done in a manner which utilises the model of a
‘one-stop shop’ authority in order to facilitate efficient reporting. Furthermore, given the regulatory framework under the Single Rulebook and cybersecurity legislation, national legislators and competent authorities at both Union and national level should ensure that the principle of proportionality is strictly followed in order to prevent an excessive burden on market participants.

Amendment 176
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Recital 21

Text proposed by the Commission

(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) 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.

Amendment

(21) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. The European Union Agency for Cybersecurity (ENISA) and the NIS Cooperation Group for the financial entities under Directive (EU) 2016/1148, provide the necessary coordination between national practices. ENISA and the NIS Cooperation group should improve cross-border 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.
Amendment 177
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission

(21 a) In order to reduce the administrative burden and avoid complexity and duplicative reporting requirements for payment service providers that fall within the scope of this Regulation, the incident reporting requirements under Directive (EU) 2015/2366 should cease to apply. As such, credit institutions, e-money institutions and payment institutions should report, under this Regulation, all operational or security payment-related and non-payment related incidents that were previously reported under Directive (EU) 2015/2366, irrespective of whether the incidents are ICT-related or not.

Amendment

Amendment 178
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 22

Text proposed by the Commission

(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.

Amendment 179
Gunnar Beck, Maximilian Krah, Jörg Meuthen, Francesca Donato, France Jamet

Proposal for a regulation
Recital 22

Text proposed by the Commission
(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

Amendment
(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 streamline 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, after consultation of the national supervisory authorities.

Amendment 180
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Recital 23

Text proposed by the Commission

(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.

Amendment

(23) Digital operational resilience testing requirements have developed in some financial subsectors within several and sometimes under-coordinated, national frameworks addressing the same issues in a different way. This leads to duplication of costs for cross-border financial entities and could hamper the mutual recognition of results. Uncoordinated testing can therefore segment the single market.

Amendment 181
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Recital 24

Text proposed by the Commission

(24) In addition, where no testing is required, vulnerabilities remain undetected putting the financial entity and ultimately the financial sector’s stability and integrity

Amendment

(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 *could be useful* 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.

Or. en

---

**Amendment 182**

Markus Ferber

**Proposal for a regulation**

**Recital 28**

*Text proposed by the Commission*

(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, 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

*Amendment*

(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, 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.

Existing guidelines and guidelines currently under preparation by the ESAs should be reviewed, revised and harmonised to reflect the provisions of this Regulation.

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

Amendment 183
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 29

Text proposed by the Commission

(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.

Amendment

(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 frequent monitoring of the activities of ICT third-party service providers that provide critical services to financial entities.

Amendment 184
Markus Ferber

Proposal for a regulation
Recital 29
(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.

Amendment 185
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Recital 30

(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 inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules. Data protection does not constitute an obstacle to intelligence sharing in the financial sector because data protection requirements should be perceived as a basic requirement, which should be complied with to ensure that the rights of individuals within the data operational resilience framework of financial entities are safeguarded. In that regard, the national data protection authorities (DPAs) have an important role to play in promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to data processing, as well as the awareness of controllers and processors in relation to their obligations under the General Data Protection Regulation. Moreover, the European Data Protection Board’s guidance set out in its guidelines, recommendations and best practices encourages consistent application of the General Data Protection Regulation.

Amendment 186
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 30

Text proposed by the Commission

(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 inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules. It is therefore important to strengthen cooperation arrangements and reporting amongst financial entities and the competent authorities as well as information-sharing with the public, with a view to developing an open intelligence sharing framework and a 'security by design' approach, which are essential in order to increase the operational resilience and preparedness of the financial sector with regard to cyber threats.

Amendment 187
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 33

Text proposed by the Commission

(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.

Amendment

(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, *nature, complexity and risk profile*. As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size, *nature, complexity and risk profile*, while competent authorities should continue to assess and review the approach of such distribution. *Accordingly, the risk management framework should be applied to financial entities according to a risk-based approach which takes due*
account of their size, nature, complexity and risk profile.

Amendment 188
Markus Ferber

Proposal for a regulation
Recital 33

Text proposed by the Commission

(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.

Amendment

(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, complexity, business model and risk profile, while competent authorities should continue to assess and review the approach of such distribution with a view to ensure a proportionate application;

Amendment 189
José Gusmão

Proposal for a regulation
Recital 34

(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate structures and set up various corporate structures, the approach to their ICT risk management framework should take into account their size, business profile and complexity.

Text proposed by the Commission

(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate structures, the approach to their ICT risk management framework should take into account their size, business profile and complexity.

Amendment

(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate structures, the approach to their ICT risk management framework should take into account their size, business profile and complexity.
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 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.

Amendment 190
Markus Ferber

Proposal for a regulation
Recital 34 – introductory part

Text proposed by the Commission

(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

Amendment

(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 small and medium 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
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.

Amendment 191
José Gusmão

Proposal for a regulation
Recital 35

Text proposed by the Commission
Amendment

(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.

Amendment 192
Markus Ferber

Proposal for a regulation
Recital 35

Text proposed by the Commission
Amendment

PE693.603v01-00 26/294 AM\1232471EN.docx
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 ICT disruptions.

Proposal for a regulation
Recital 35

Text proposed by the Commission

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.

Amendment

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 significant ICT disruptions and the results of post-incident reviews after significant ICT disruptions.

Or. en
Amendment 194
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 35

Text proposed by the Commission

(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.

Amendment

(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 estimated costs and losses caused by ICT disruptions and the results of post-incident reviews after significant ICT disruptions.

Or. en

Amendment 195
José Gusmão

Proposal for a regulation
Recital 39 a (new)

Text proposed by the Commission

(39 a) Sharing of threat intelligence should be compulsory; financial institutions should be legally obliged to file reports of known threats to their NCAs and relevant ESA. The information could then be shared if requested (confidentially and anonymously), through a central clearing house, such as an EU Hub for Incident Reporting.

Amendment

(39 a) Sharing of threat intelligence should be compulsory; financial institutions should be legally obliged to file reports of known threats to their NCAs and relevant ESA. The information could then be shared if requested (confidentially and anonymously), through a central clearing house, such as an EU Hub for Incident Reporting.

Or. en
Amendment 196
José Gusmão

Proposal for a regulation
Recital 39 b (new)

Text proposed by the Commission

(39 b) The collective interest in preventing systemic instability and wide-ranging harm to the financial system clearly outweighs any individual institution’s interest in protecting commercial secrets or preventing damage to its reputation. Nevertheless, proper mechanisms for the confidential exchange and handling of incident data should be put in place to mitigate the risk of leaks.

Or. en

Amendment 197
Alfred Sant, Carmen Avram

Proposal for a regulation
Recital 41 a (new)

Text proposed by the Commission

(41 a) The definition of critical or important functions in this Regulation should encompass critical functions as defined in Directive (EU) 2014/59. Thereby, functions that are deemed to be critical functions pursuant to Directive (EU) 2014/59 should be deemed to be critical or important within the meaning of this Regulation.

Or. en

Justification

This reference to the BRRD directive ensures that DORA encompasses critical functions as defined under the BRRD.
Amendment 198
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Recital 43

Text proposed by the Commission

(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.

Amendment

(43) Centralisation of ICT-related incident reports will be achieved with the establishment of a single central EU Hub for major ICT-related incident reporting. The new EU Hub will centralise reports forwarded by the national competent authorities and fulfil a coordination role.

Or. en

Amendment 199
Gunnar Beck, Maximilian Krah, Jörg Meuthen, Francesca Donato, France Jamet

Proposal for a regulation
Recital 43

Text proposed by the Commission

(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.

Amendment

(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, ENISA and national supervisory authorities, by a certain date a joint report exploring the
a central EU Hub.

feasibility of setting up such a central EU Hub.

Amendment 200
Bogdan Rzońca
Proposal for a regulation
Recital 44

Text proposed by the Commission

(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

Amendment

(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.

Furthermore, in order to strengthen cooperation in the field of resilience of financial entities with trusted third countries, the Commission and competent authorities should seek to establish a framework for mutual recognition of TLPTs results.

Amendment 201
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Recital 45

Text proposed by the Commission

(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.

Amendment

(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, particularly regarding the provision of critical or important functions by ICT third-party service providers, and, more generally, in the context of ICT third-party dependencies.
Amendment 202  
Frances Fitzgerald, Isabel Benjumea Benjumea  

Proposal for a regulation  
Recital 47  

**Text proposed by the Commission**  

(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.

**Amendment**  

(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 **frequent** 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.

Or. en

Amendment 203  
Gunnar Beck, Maximilian Krah, Jörg Meuthen  

Proposal for a regulation  
Recital 47  

**Text proposed by the Commission**  

(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.

**Amendment**  

(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.
thereof on an ad-hoc basis. The frequency of such interactions should be proportionate to the risk assessment of the entities, their size, and the reliability and security of the information sharing systems.

Amendment 204
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Recital 48

Text proposed by the Commission

(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.

Amendment

(48) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, while corrective and remedial measures, which may include contract termination, should be taken in the case of at least a set of circumstances that show shortfalls at the ICT third-party service provider.

Amendment 205
Markus Ferber
Proposal for a regulation
Recital 48

Text proposed by the Commission

(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.

Amendment

(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 severe shortfalls at the ICT third-party service provider.
Amendment 206  
Mikuláš Peksa  
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 49

Text proposed by the Commission

(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.\(^\text{38}\)

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

Amendment

(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 Joint Oversight Body overseeing critical ICT third-party provider 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.\(^\text{38}\)

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.

Amendment 207
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet, Francesca Donato

Proposal for a regulation
Recital 49

Text proposed by the Commission

(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 if those third parties have, or are suspected of having, ties to foreign governments or to foreign militaries. 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 if those third parties have, or are suspected of having, ties to foreign governments or to foreign militaries.

Amendment

(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.
providers where that risk is identified.\textsuperscript{38}

\textsuperscript{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.

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.\textsuperscript{38}

\textsuperscript{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.

\textbf{Amendment 208}

Alfred Sant, Carmen Avram

\textbf{Proposal for a regulation}

Recital 52

\texttt{Text proposed by the Commission}

(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.

\texttt{Amendment}

(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 relevant to the services being provided by the ICT third-party service provider to the financial institution at no additional cost or at a cost that is determined ex-ante. \textit{Ancillary ICT services on which the financial entities are not operationally dependent shall not be covered by this Regulation.}

\texttt{Or. en}
Amendment 209
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Recital 53

Text proposed by the Commission

(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.

Amendment

(53) Rights of access, inspection and audit by the financial entity or an appointed third party should 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. They 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.

Amendment 210
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 53

Text proposed by the Commission

(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.

Amendment

(53) Rights of access, inspection and audit by the financial entity or an appointed third party, in relation to the use of ICT services provided by the third-party service provider concerning critical or important functions, 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
confidentiality.

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.

Or. en

**Amendment 211**

Alfred Sant, Carmen Avram

Proposal for a regulation

Recital 53

**Text proposed by the Commission**

(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.

**Amendment**

(53) Rights of access, inspection and audit by the financial entity or an appointed third party **shall cover only critical and important functions and** 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.

Or. en

**Amendment 212**

Markus Ferber

Proposal for a regulation

Recital 54

**Text proposed by the Commission**

(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

**Amendment**

(54) Contractual arrangements should provide for clear termination rights as **a solution of last resort** and related minimum notices as well as dedicated exit strategies enabling, in particular, mandatory transition periods during which the ICT third-party service providers
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-party service providers, or alternatively resort to the use of **on-premises** solutions, consistent with the complexity of the provided service.

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-party service providers, or alternatively resort to the use of **in-house** solutions, consistent with the complexity of the provided service.

**Amendment 213**

Alfred Sant, Carmen Avram

**Proposal for a regulation**

**Recital 54**

_**Text proposed by the Commission**_

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

_**Amendment**_

(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-party service providers, or alternatively resort to the use of on-premises solutions, consistent with the complexity of the provided service. **Moreover, credit institutions should also ensure that the relevant ICT contracts are robust and fully enforceable in the event of resolution of the credit institution. In line with the resolution authorities’ expectations, credit institutions should ensure that the relevant contracts for ICT services are resolution-resilient. As long as critical and important ICT functions continue to be performed, those financial entities should ensure that the contracts foresee, among other requirements, non-termination, non-suspension and non-modification clauses on the grounds of**
restructuring or resolution.

Amendment 214
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 54

Text proposed by the Commission

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

Amendment

(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-party service providers, or alternatively resort to the use of on-premises solutions, consistent with the complexity of the provided service. In addition, credit institutions should also ensure that the relevant ICT contracts are robust and fully enforceable in the event of resolution of the credit institution. In that regard, credit institutions should include, in the relevant contracts for ICT services, resolution-resilient clauses, which ensure, among other requirements, non-termination, suspension or modification on the grounds of resolution as long as substantive obligations continue to be performed.

Or. en

Justification

In line with resolution authorities expectations for banks to ensure operational continuity in the event of resolution.
Amendment 215
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 57

Text proposed by the Commission

(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.

Amendment

(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.

Similarly, undertakings which are part of a financial group and which provide ICT services exclusively to financial entities within the same financial group should not be subject to the designation mechanism.

Or. en

Amendment 216
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 58
(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.

Amendment 217
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel

Proposal for a regulation
Recital 58

Text proposed by the Commission

(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.

Amendment

(58) The requirement to establish a subsidiary 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. The requirement to have a subsidiary in the Union is intended to provide a contact point between the ICT third-party service provider, on the one hand, and the ESAs and Joint Oversight Executive Body, on the other, and to ensure that the Joint Oversight Executive Body is able to carry out its duties and exercise its powers of oversight and enforcement as foreseen under this Regulation.

Justification

References to the Joint Oversight Executive Body to be aligned throughout the Regulation
Amendment 218  
Frances Fitzgerald, Isabel Benjumea Benjumea  
Proposal for a regulation  
Recital 58 a (new)  

Text proposed by the Commission

(58 a) Due to the significant impact that designation as critical may have on ICT third-party service providers, prior hearing rights should be established as an obligation imposed on the Lead Overseer to duly take into consideration any additional information provided by ICT third-party service providers in the course of the designation process.

Amendment

Or. en

Amendment 219  
Mikuláš Peksa  
on behalf of the Greens/EFA Group  
Proposal for a regulation  
Recital 60

Text proposed by the Commission

(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.

Amendment

(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, through a new Committee (the Joint Oversight Body) adopting 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.

Or. en
Amendment 220  
Mikuláš Peksa  
on behalf of the Greens/EFA Group

Proposal for a regulation  
Recital 61

*Text proposed by the Commission\*  
(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.

*Amendment*  
(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, the Joint Oversight Body should be responsible for the supervision of each critical ICT third-party service provider and rely on joint examination teams.

Or. en

Amendment 221  
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation  
Recital 61

*Text proposed by the Commission\*  
(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.

*Amendment*  
(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, this Regulation foresees that the European Banking Authority (EBA) should act as Lead Overseer for each critical ICT third-party service provider.

Or. en

Amendment 222  
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation  
Recital 62 – introductory part
(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.

(62) **The Lead Oversee**r 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 the **Lead Oversee**r 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.

**Amendment 223**
Mikuláš Peksa
on behalf of the Greens/EFA Group

**Proposal for a regulation**
**Recital 62 – introductory part**

(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.

Or. en

**Amendment 224**
Frances Fitzgerald, Isabel Benjumea Benjumea

**Proposal for a regulation**
**Recital 62 – point 1**

(62) **The Joint Oversight Body** 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.

Or. en
Text proposed by the Commission

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.

Amendment

Entrusting the **EBA** with the lead oversight role, in close cooperation with **EIOPA and ESMA**, 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.

Or. en

**Amendment 225**
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 63

Text proposed by the Commission

(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.

Amendment

(63) In addition, **the Lead Overseer** 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. **Prior to the finalisation of such recommendations, critical ICT third-party service providers should be given the opportunity to provide information which it reasonably believes should be taken into account before the recommendation is finalised and issued.**

Compliance with such substantive recommendations laid down by the Lead
Overseer should be duly taken into account by national competent authorities as part of their function relating to the prudential supervision of financial entities.

Amendment 226
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Recital 63 a (new)

Text proposed by the Commission

(63 a) In order to avoid duplication and contradictions with the technical and organisational measures that may apply to critical ICT third-party service providers, Lead Overseers should take due account of the framework established by Directive (EU) 2016/1148 in the exercise of their powers according to the Oversight Framework in this Regulation. Before exercising such powers, the Lead Overseer should consult the relevant competent authorities that have jurisdiction under Directive (EU) 2016/1148 and the Oversight Forum.

Amendment 227
Mikuláš Peksa on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 66

Text proposed by the Commission

(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

Amendment

(66) To leverage technical expertise of competent authorities’ experts on operational and ICT risk management, the Joint Oversight Body should rely on joint examination teams composed by national
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.

supervisory *experts and dedicated ESAs staff* for each individual critical ICT third-party service provider, pooling together multidisciplinary teams to supporting the actual execution of oversight activities, including onsite inspections of critical ICT third-party service providers, as well as needed follow-up thereof.

Or. en

**Amendment 228**

Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation

Recital 66 a (new)

*Text proposed by the Commission*

(66 a) *In order to include the full range of practical experience and operational expertise, the Joint Oversight Executive Body should include independent directors from each ESA, in charge of digital operational resilience for the financial sector.*

*Or. en*

*Justification*

References to the Joint Oversight Executive Body to be aligned throughout the Regulation

**Amendment 229**

Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation

Recital 66 b (new)

*Text proposed by the Commission*

(66 b) *To provide for an appropriate level of expertise and accountability, the independent directors should be appointed by the Board of Supervisors of each ESA*
on the basis of merit, knowledge and relevant experience on digital operational resilience, following an open selection procedure organised and managed by the relevant Board of Supervisors, assisted by the Commission, which should respect the principle of gender balance. Before the appointment of the independent directors, and up to one month after their selection by the relevant Board of Supervisors, the European Parliament should, after having heard the persons selected, approve or reject their designation. Only selected candidates approved by the European Parliament may be appointed by the relevant Board of Supervisors.

Amendment 230
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru
Proposal for a regulation
Recital 66 c (new)

Text proposed by the Commission

(66 c) In order to ensure transparency and democratic control, as well as to safeguard the rights of the Union institutions, the independent directors should be accountable to the European Parliament and to the Council for any decisions taken on the basis of this Regulation.

Amendment 231
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru
Proposal for a regulation
Recital 66 d (new)
(66 d) The independent directors should act independently and objectively in the interests of the Union. They should ensure that appropriate account is taken of the proper functioning of the internal market as well as financial stability in each Member State and in the Union.

Or. en

Amendment 232
Gunnar Beck, Maximilian Krah, Jörg Meuthen, Francesca Donato, France Jamet

Proposal for a regulation
Recital 67

Text proposed by the Commission

(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, and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities.


Amendment

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


Or. en
Amendment 233
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Recital 67

Text proposed by the Commission

(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.

Amendment

(67) Competent authorities, including the Joint Oversight Body, 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. The Single Resolution Board and national resolution authorities should be involved in the mechanisms for the mutual exchange of information for entities referred to in Article 7 of Regulation (EU) No 806/2014. National resolution authorities should provide a summary of the reported incidents for entities under their remit to the Single Resolution Board on a quarterly basis.

---

Amendment 234
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Recital 69 – point 1

Text proposed by the Commission

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.

Amendment

Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation without hindering innovation and equal treatment of different types of technology. 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.

Or. en

Amendment 235
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Engin Eroglu

Proposal for a regulation
Recital 69 – point 1

Text proposed by the Commission

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.

Amendment

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. When developing draft regulatory technical standards, the
ESAs should take due consideration of their mandate in relation to proportionality aspects, and seek advice from their respective Advisory Committees on Proportionality, in particular in relation to the application of the DORA framework to SMEs and mid-caps.

Amendment 236
Alfred Sant

Proposal for a regulation
Recital 69 a (new)

Text proposed by the Commission

(69 a) Guidelines issued by the ESAs on the application of those regulations and directives should be reviewed and revised as part of the consolidation process so that the legal basis for ICT risk requirements in Union law exclusively derive from this Regulation, its implementing acts and/or decisions and recommendations taken in accordance therewith, concerning entities within its scope.

Amendment 237
Markus Ferber

Proposal for a regulation
Recital 71

Text proposed by the Commission

(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.

Amendment 238
José Gusmão

Proposal for a regulation
Recital 73 a (new)

Text proposed by the Commission

(73 a) Although protection against cyberattacks is an important tool against financial instability, it is of note that the most significant systemic risks are not the
result of external threats but instead originate within the financial system itself, due to its internal mechanisms and incentives structure. In that regard, this Regulation should be understood as a necessary, though not sufficient, condition for the promotion of financial stability;

Amendment 239
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 1 – paragraph 1 – point a – indent 2 a (new)

Text proposed by the Commission

Amendment

— reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in points (a) to (c) of Article 2 (1);

Amendment 240
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 1 – paragraph 1 – point a – indent 5

Text proposed by the Commission

Amendment

— measures for a sound management by financial entities of the ICT third-party risk;

— measures for the sound management of ICT third-party risk by financial entities;

Amendment 241
Alfred Sant
Proposal for a regulation
Article 1 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1 a. This Regulation provides for the development of regulatory technical standards by the ESAs in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk. When developing those regulatory technical standards, the ESAs shall fully take into account and incorporate previous guidelines and any other regulatory requirements issued before the entry into force of this Regulation, aiming to provide regulatory continuity and stability, wherever possible, and in accordance with this Regulation.

Or. en

Amendment 242
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 1 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. This Regulation is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.

Or. en

Amendment 243
Markus Ferber
Text proposed by the Commission

2 a. The requirements of this Regulation shall be applied in a way that is proportionate to the size and risk of the entities subject to this Regulation.

Or. en

Justification

Introduces a risk-based and proportionate approach into the regulation.

Amendment 244
Engin Eroglu

Proposal for a regulation
Article 2 – paragraph 1 – point a

Text proposed by the Commission

(a) credit institutions,

Amendment

Or. en

Amendment 245
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 2 – paragraph 1 – point e

Text proposed by the Commission

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

Amendment

Or. en
Amendment 246
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 2 – paragraph 1 – point f

Text proposed by the Commission

(f) central securities depositories,

Amendment

(f) central securities depositories, and operators of securities settlement systems,

Or. en

Amendment 247
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 2 – paragraph 1 – point f

Text proposed by the Commission

(f) central securities depositories,

Amendment

(f) central securities depositories and operators of securities settlement systems,

Or. en

Amendment 248
Alfred Sant

Proposal for a regulation
Article 2 – paragraph 1 – point k

Text proposed by the Commission

(k) management companies,

Amendment

(k) management companies and self-managed UCITS investment companies within the meaning of Directive 2009/65/EC and managers of alternative investment funds as defined in Article 4(1)(b) of Directive 2011/61/EU,

Or. en
Amendment 249
Carmen Avram

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

Amendment

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

Or. en

Justification

This amendment aim is to protect SMEs from additional bureaucracy and extra costs, considering the fact that insurance intermediaries do not stock personal data, but they just facilitate the flux of data between consumers and insurance companies. Moreover, the GDPR Regulation remains applicable to insurance intermediaries.

Amendment 250
Bogdan Rzońca

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

Amendment

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

Or. en

Amendment 251
Costas Mavrides

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

Amendment

(n) insurance intermediaries, deleted
reinsurance intermediaries and ancillary insurance intermediaries,
The risk to the financial stability arising out of the activities of intermediaries is very low. The vast majority of intermediaries do not develop/use their own ICT system. Intermediaries use, for their clients and their policies, either the insurers’ system or a market interface. In the cases where, in addition to a “general software” for databases, a more insurance-specific software is used, they are brought by specialised “insurance” software houses (increasingly cloud-based), which guarantee insurance market conformity and allow for safe interaction with insurers or other parties within the insurance value chain. Consequently, the communication and ICT transactions between an intermediary and an insurer are always carried out via a system in which the level of protection is guaranteed by either the insurer or the interface. By including intermediaries in the scope of DORA, compliance with the ICT-risk management requirements will be unnecessarily duplicated or triplicated. The consequences of an intermediary not being operational for a day or a week are of extremely low risk for the insurance contract and service continuity and furthermore for the financial stability. Macro-economically, the shutdown of an intermediary ICT system has no consequence on the provider’s capability of rendering services or on the integrity of the “main-ICT system” of the insurer. Micro-economically, consumers’ personal data are safeguarded as the insurance contract information is stored by the insurer and the integrity of the contract is not affected. Other consequences are covered under GDPR, which is applicable to insurance intermediaries. Moreover, insurance intermediaries are regulated by the Insurance Distribution Directive Article 10.6 of the IDD which includes measures that protect clients’ money.

Amendment 252
Olivier Chastel

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

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

Amendment

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, **unless they are micro, small or medium-sized enterprises and do not rely exclusively on organised automated sales systems,**

Amendment 253
José Manuel García-Margallo y Marfil
Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

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

Amendment

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, unless they are micro, small or medium-sized enterprises and do not rely exclusively on organised automated sales systems,

Amendment 254
Jessica Polfjärd

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

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

Amendment

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, unless they are micro, small or medium-sized enterprises,

Amendment 255
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

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

Amendment

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, unless they are micro, small or medium-sized enterprises,
Amendment 256
Siegfried Mureșan

Proposal for a regulation
Article 2 – paragraph 1 – point n

Text proposed by the Commission

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

Amendment

(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, with the exception of microenterprises,

Or. en

Amendment 257
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 2 – paragraph 1 – point o

Text proposed by the Commission

(o) institutions for occupational retirement pensions,

Amendment

(o) institutions for occupational retirement provisions (IORPs), unless they operate pension schemes which together do not have more than a total of 15 members,

Or. en

Amendment 258
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 2 – paragraph 1 – point o

Text proposed by the Commission

(o) institutions for occupational retirement pensions,

Amendment

(o) institutions for occupational retirement pensions, unless they are micro, small or medium-sized enterprises,

Or. en
Amendment 259
Markus Ferber

Proposal for a regulation
Article 2 – paragraph 1 – point q

Text proposed by the Commission Amendment
(q) statutory auditors and audit firms, deleted

Or. en

Amendment 260
Engin Eroglu

Proposal for a regulation
Article 2 – paragraph 1 – point q

Text proposed by the Commission Amendment
(q) statutory auditors and audit firms, deleted

Or. en

Justification
They are not part of the financial system and not technically connected to it.

Amendment 261
Bogdan Rzońca

Proposal for a regulation
Article 2 – paragraph 1 – point q

Text proposed by the Commission Amendment
(q) statutory auditors and audit firms, deleted

Or. en

Amendment 262
Bogdan Rzońca

Proposal for a regulation
Article 2 – paragraph 1 – point u a (new)
Text proposed by the Commission

Amendment

(u a) ICT intra-group service providers, when providing ICT services related to critical or important functions, with the exception of Section II of Chapter V of this Regulation that is not applicable to such providers,

Or. en

Amendment 263
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Engin Eroğlu

Proposal for a regulation
Article 2 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(b a) payment systems

Or. en

Amendment 264
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 2 – paragraph 1 – point u a (new)

Text proposed by the Commission

Amendment

(u a) operators of payment schemes and payment systems.

Or. en

Amendment 265
Alfred Sant, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 2 – paragraph 1 – point u a (new)
Text proposed by the Commission

Amendment

(u a) payment cards’ networks,

Or. en

Justification

Payment cards’ continuity, efficiency and safety entirely contribute to financial stability, also given their very wide use among consumers.

Amendment 266
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Article 2 – paragraph 1 – point u a (new)

Text proposed by the Commission

Amendment

(u a) central banks, including the ECB.

Or. en

Amendment 267
Alfred Sant

Proposal for a regulation
Article 2 – paragraph 1 – point u b (new)

Text proposed by the Commission

Amendment

(u b) mutatis mutandis, the ESAs, the competent authorities, the Commission’s directorate general responsible for financial policies;

Or. en

Amendment 268
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 2 – paragraph 1 a (new)
Text proposed by the Commission

Amendment

1 a. Chapter III of this Regulation applies to all payment service providers as defined in Directive (EU) 2015/2366.

Or. en

Justification

In line with proposal to establish a single channel of reporting under PSD2 (as amended in Omnibus Directive)

Amendment 269
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Article 2 – paragraph 2

Text proposed by the Commission

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

Amendment

2. For the purposes of this Regulation, entities referred to in paragraph (a) to (t) and central banks, including the ECB, shall collectively be referred to as ‘financial entities’.

Or. en

Amendment 270
Alfred Sant

Proposal for a regulation
Article 2 – paragraph 2 a (new)

Text proposed by the Commission

2 a. This Regulation shall be considered to be a sector-specific Union legal act in relation to the Directive on measures for a high common level of cybersecurity across the Union [insert the full title and OJ publication reference when known] (NIS 2) with regard to financial entities. The provisions of this Regulation relating to ICT risk management measures, management of
ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third-party risk shall apply instead of those set up under the NIS 2 directive. Member States shall therefore not apply the provisions of NIS 2 on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by this Regulation. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under the NIS 2 Directive. To that end, this Regulation allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under this Regulation to participate in strategic policy discussions and the technical workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under the NIS 2 Directive and with the national CSIRTs. The competent authorities under this Regulation shall also transmit details of major ICT-related incidents to the single points of contact designated under the NIS 2 Directive. Moreover, Member States shall continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

Or. en

Justification

Given that the DORA’s requirements will fully replace all NIS requirements on financial entities that currently fall within its scope, recital 13 of the proposed NIS2 Directive is copied into Article 2 DORA in order to clarify the interaction between the two texts. This provides legal certainty that the NIS Directive (and any future revisions) will not apply to entities regulated under the DORA.

Amendment 271
Othmar Karas

Proposal for a regulation
Article 2 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. This Regulation shall not apply to:
(a) statutory auditors and audit firms, which are micro, small and medium-sized enterprises as defined in Article 2 of the Annex to Recommendation 2003/361;
(b) insurance and reinsurance undertakings excluded from the scope due to size in accordance with Article 4 of Directive 2009/138/EC;
(c) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, which are microenterprises in accordance with Article 3 point (50).

Justification

In line with the principle of proportionality and a risk-based approach, this regulation should focus on relevant entities exposed to ICT risks. The scope should therefore be revised to exempt: statutory auditors and audit firms, which are micro, small and medium enterprises, as well as insurance and reinsurance undertakings, which do not fall under the scope of Directive 2009/138/EC (Solvency II), and insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, which are microenterprises in accordance with Article 3 point (50).

Amendment 272
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 1

Text proposed by the Commission

Amendment

(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,

(1) ‘digital operational resilience’ means the ability of a financial entity to build, assure and review its technological operational integrity by ensuring the continued provision of services and their
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;

quality in the face of operational disruptions impacting its ICT capabilities;

Amendment 273
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 3 – paragraph 1 – point 1

Text proposed by the Commission

(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;

Amendment

(1) ‘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;

Amendment 274
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission

(4) ‘ICT risk’ means any reasonably identifiable circumstance in relation to the

Amendment

(4) ‘ICT risk’ means any reasonably identifiable circumstance derived from 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;

Or. en

Amendment 275
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission

(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;

Amendment

(4) ‘ICT risk’ means any reasonably identifiable circumstance in relation to the use of network and information systems, which, if materialised, may compromise the security or adversely affect the network and information systems, of any technology-dependant tool or process, of the operation and process’ running, or of the provision of services;

Or. en
Amendment 276
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission

(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;

Amendment

(4) ‘operational 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;

Or. en

Justification

There is not a clear delineation between ICT risk and non-ICT risk which may affect the use of network and information systems. The definition of risk is therefore revised to ensure it covers all risks having an impact on network and information systems. This amendment is intended to apply horizontally throughout the text.

Amendment 277
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 3 – paragraph 1 – point 4

Text proposed by the Commission

(4) ‘ICT risk’ means any reasonably

Amendment

(4) ‘ICT risk’ means any reasonably

PE693.603v01-00  72/294  AM\1232471EN.docx
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;

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 ICT-dependent 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;

Or. en

Amendment 278
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 5

Text proposed by the Commission

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

Amendment

(5) ‘information asset’ means a collection of information, either tangible or intangible, that has value for an entity and requires protection;

Or. en

Amendment 279
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 3 – paragraph 1 – point 5 a (new)

Text proposed by the Commission

(5 a) ‘incident’ means any event having the potential to disrupt, or that in fact disrupts, the operations of a financial
(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;

(6) ‘ICT-related incident’ means an event or a series of linked events, unplanned by the financial entity, which has or will have an adverse impact on the integrity, availability, confidentiality, continuity and/or authenticity of financial services provided by the financial entity;
Amendment 282
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 3 – paragraph 1 – point 6

Text proposed by the Commission

(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;

Amendment

(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;

Justification

There is not a clear delineation between ICT-related and other kind of non-ICT incidents affecting network and information systems. The definition of incidents is therefore revised in line with definition used in the NIS Directive and in the financial sector. This amendment is intended to apply horizontally throughout the text.

Amendment 283
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 6

Text proposed by the Commission

(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,

Amendment

(6) ‘ICT-related incident’ means an unforeseen identified occurrence or a series of linked occurrences in the network and information systems which compromises the security of network and information systems which has adverse effects on the availability, confidentiality,
Amendment 284
Alfred Sant

Proposal for a regulation
Article 3 – paragraph 1 – point 6

Text proposed by the Commission

(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;

Amendment

(6) ‘ICT-related incident’ means an unforeseen identified incident 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;

Or. en

Amendment 285
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoş Pîslaru

Proposal for a regulation
Article 3 – paragraph 1 – point 6

Text proposed by the Commission

(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

Amendment

(6) ‘ICT-related incident’ means any event having an actual adverse effect on the security of 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
the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity;

adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity;

Or. en

Amendment 286
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 3 – paragraph 1 – point 6 a (new)

Text proposed by the Commission  Amendment

(6 a) ‘operational or security payment-related incident’, means an event or a series of linked occurrences unforeseen by financial entities referred to in points (a) to (c) of Article 2(1) which has or is likely to have an adverse impact on the integrity, availability, confidentiality, authenticity or continuity of payment-related services;

Or. en

Amendment 287
Bogdan Rzońca

Proposal for a regulation
Article 3 – paragraph 1 – point 7

Text proposed by the Commission  Amendment

(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;

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

Or. en

Amendment 288

AM\1232471EN.docx  77/294  PE693.603v01-00  EN
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 7

Text proposed by the Commission

(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;*

Amendment

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

Or. en

Amendment 289
Alfred Sant

Proposal for a regulation
Article 3 – paragraph 1 – point 7

Text proposed by the Commission

(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;*

Amendment

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

Or. en

Amendment 290
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 3 – paragraph 1 – point 7

Text proposed by the Commission

(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;

Amendment

(7) ‘major *operational* incident’ means an incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity;
Amendment 291
Alfred Sant, Jonás Fernández, Niels Fuglsang
Proposal for a regulation
Article 3 – paragraph 1 – point 7 a (new)

Text proposed by the Commission
(7 a) ‘major operational or security payment-related incident’ means an operational or security payment-related incident which meets the criteria set out in Article 16(2)(a);

Or. en

Amendment 292
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang
Proposal for a regulation
Article 3 – paragraph 1 – point 8 a (new)

Text proposed by the Commission
(8 a) ‘significant cyber threat’ means a cyber threat whose characteristics clearly indicate that it is likely to result in a major ICT-related incident or a major operational or security payment-related incident;

Or. en

Amendment 293
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 3 – paragraph 1 – point 12

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

Or. en

Amendment 294  
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation  
Article 3 – paragraph 1 – point 15

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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 services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council.</td>
<td></td>
</tr>
<tr>
<td>(15) ‘ICT third-party service provider’ means an undertaking providing ICT services;</td>
<td></td>
</tr>
</tbody>
</table>


Or. en

Amendment 295  
Engin Eroglu

Proposal for a regulation  
Article 3 – paragraph 1 – point 15

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(15) ‘ICT third-party service provider’</td>
<td></td>
</tr>
<tr>
<td>(15) ‘ICT third-party service provider’</td>
<td></td>
</tr>
</tbody>
</table>
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 services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council\(^\text{43}\);


Justification

Aligning to EBA definition

Amendment 296
Bogdan Rzońca

Proposal for a regulation
Article 3 – paragraph 1 – point 15

Text proposed by the Commission

(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 services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council\(^\text{43}\);

Amendment

(15) ‘ICT third-party service provider’ means an undertaking providing ICT services, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council\(^\text{43}\);
Proposal for a regulation
Article 3 – paragraph 1 – point 15

Text proposed by the Commission

(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 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

Amendment

(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, including an economic unit providing ICT services that forms part of an undertaking which provides a wider range of products or services, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication 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

Amendment 297
Alfred Sant

Amendment 298
Engin Eroglu
Proposal for a regulation
Article 3 – paragraph 1 – point 15 a (new)

Text proposed by the Commission

(15 a) ‘Intra-group ICT service provider’ means an ICT service provider that is part of a group of institutions permanently affiliated to a central body as referred to in Article 10 or 113(6) of Regulation (EU) No 575/2013 or within the same institutional protection scheme as referred to in Article 113(7) of Regulation (EU) No 575/2013 or where credit institutions are associated in a network in accordance with legal or statutory provisions as referred to in Article 400(2)(d) of that Regulation;

Or. en

Justification

a definition “Intra-group ICT service provider” is needed in the context. This suggestion is based on prudential requirements (references to the CRR and aims to cover the various decentralized banking models across Europe.

Amendment 299
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 15 a (new)

Text proposed by the Commission

(15 a) 'ICT intra-group third-party service provider' means an undertaking that is part of a financial group and provides ICT services exclusively to financial entities within the same group, including to their parent undertakings, subsidiaries and branches or other entities that are under common ownership or control;

Or. en
Amendment 300
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 3 – paragraph 1 – point 15 a (new)

Text proposed by the Commission

(15 a) 'intra-group ICT third-party service provider' means an ICT third-party service provider that is in a consolidated situation with a financial entity, or that is within the same group as a financial entity, as defined in Regulation (EU) No 575/2013.

Amendment

Or. en

Amendment 301
Bogdan Rzońca

Proposal for a regulation
Article 3 – paragraph 1 – point 15 a (new)

Text proposed by the Commission

(15 a) ‘ICT intra-group service provider’ means an undertaking that provides ICT services exclusively to financial entities within the same group;

Amendment

Or. en

Amendment 302
Bogdan Rzońca

Proposal for a regulation
Article 3 – paragraph 1 – point 16

Text proposed by the Commission

(16) ‘ICT services’ means digital and data services provided through the ICT systems to one or more internal or external

Amendment

(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;
services; services excluding maintenance contracts for licensed software and telecom contracts;

Amendment 305
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 3 – paragraph 1 – point 17

Text proposed by the Commission

(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;

Amendment

(17) ‘critical or important function’ means a function that is essential to the operation of a financial entity as it would be unable to deliver its services without the function, or whose 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 continuity of its services and activities;

Amendment 306
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 17

Text proposed by the Commission

(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

Amendment

(17) ‘critical or important function’ means an ICT 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;

Amendment 307
Markus Ferber

Proposal for a regulation
Article 3 – paragraph 1 – point 18

Text proposed by the Commission

(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;

Or. en

Amendment

(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,
unless the ICT third-party service
provider is part of the same group or same
institutional protection scheme;

Or. en

Justification

Intragroup services should not be classified as critical third party service providers.

Amendment 308
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 18

Text proposed by the Commission

(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;

Or. en

Amendment

(18) ‘critical ICT third-party service
provider’ means an ICT third-party service
provider designated in accordance with
Article 28 and subject to the Oversight
Framework referred to in Articles 29 to 36;

Or. en
Amendment 309
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 19

Text proposed by the Commission

(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;

Amendment

(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 a legal entity in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services;

Or. en

Amendment 310
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 20

Text proposed by the Commission

(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;

Amendment

(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 a legal entity 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;

Or. en

Amendment 311
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 21
(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;

Amendment

(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 financial stability of the Union as a whole or the ability of a financial entity to deliver critical functions, or to suffer other type of adverse effects, including large losses;

Or. en

Amendment 312
Markus Ferber

Proposal for a regulation
Article 3 – paragraph 1 – point 23

Text proposed by the Commission

(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 Council46;

Amendment

(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 Council46, with the exception of small and non-complex institutions as defined in point 145 of Article (1) of Regulation (EU) No 575/2013;


Amendment 313
Othmar Karas


Or. en
**Proposal for a regulation**  
**Article 3 – paragraph 1 – point 23 a (new)**

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(23 a) ‘credit institution exempted by Directive 2013/36/EU’ means a credit institution benefiting from an exemption pursuant to points (4) to (23) of Article 2(5) of Directive 2013/36/EU;</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

**Amendment 314**  
Othmar Karas

**Proposal for a regulation**  
**Article 3 – paragraph 1 – point 24 a (new)**

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(24 a) ‘small and non-interconnected investment firm’ means an investment firm that meets the conditions laid out in Article 12 (1) of Regulation (EU) 2019/2033;</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

**Amendment 315**  
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Engin Eroglu

**Proposal for a regulation**  
**Article 3 – paragraph 1 – point 25 a (new)**

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(25 a) 'payment system' means a payment system as defined in Article 4(7) of Directive (EU) 2015/2366, with the exception of payment systems subject to ECB Regulation (EU) 795/2014.</td>
<td>Or. en</td>
</tr>
</tbody>
</table>
Amendment 316
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 25 a (new)

Text proposed by the Commission

Amendment

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

Or. en

Amendment 317
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 26 a (new)

Text proposed by the Commission

Amendment


Or. en

Amendment 318
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 36

Text proposed by the Commission

Amendment

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

(36) ‘insurance intermediary’ means an insurance intermediary as defined in point (3) of paragraph 1 of Article 2 of Directive (EU) 2016/97, which is not a
microenterprise as defined in this Article;

Or. en

Amendment 319
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 37

Text proposed by the Commission

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

Amendment

(37) ‘ancillary insurance intermediary’ means an ancillary insurance intermediary as defined in point (4) of Article 2 of Directive (EU) 2016/97, which is not a microenterprise as defined in this Article;

Or. en

Amendment 320
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 38

Text proposed by the Commission

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

Amendment

(38) ‘reinsurance intermediary’ means a reinsurance intermediary as defined in point (5) of paragraph 1 of Article 2 of Directive (EU) 2016/97, which is not a microenterprise as defined in point (50) of this Article;

Or. en

Amendment 321
Markus Ferber

Proposal for a regulation
Article 3 – paragraph 1 – point 41
(41) ‘statutory auditor’ means statutory auditor as defined in point (2) of Article 2 of Directive 2006/43/EC; 

Amendment 322
Markus Ferber

Proposal for a regulation
Article 3 – paragraph 1 – point 42

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

Amendment 323
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 3 – paragraph 1 – point 44 a (new)

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

Amendment 324
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 3 – paragraph 1 – point 45 a (new)
Text proposed by the Commission

Amendment

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

Or. en

Amendment 325
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 3 – paragraph 1 – point 46 a (new)

Text proposed by the Commission

Amendment

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

Or. en

Amendment 326
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 3 – paragraph 1 – point 50

Text proposed by the Commission

Amendment

(50) ‘microenterprise’ means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC.

(50) ‘micro, small and medium-sized enterprise’ means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC.

Or. en

Amendment 327
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 3 – paragraph 1 – point 50

Text proposed by the Commission

(50) ‘microenterprise’ means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC.

Amendment

(50) ‘micro, small and medium-sized enterprise’ means a financial entity as defined in Article 2 of the Annex to Recommendation 2003/361/EC.

Or. en

Amendment 328
Othmar Karas

Proposal for a regulation
Article 3 – paragraph 1 – point 50

Text proposed by the Commission

(50) ‘microenterprise’ means a financial entity as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC.

Amendment

(50) ‘microenterprise’ means a financial entity as defined in Article 2(2) of the Annex to Recommendation 2003/361/EC.

Or. en

Amendment 329
Markus Ferber

Proposal for a regulation
Article 3 – paragraph 1 – point 50 a (new)

Text proposed by the Commission

(50 a) 'small and medium sized enterprises' means companies below the thresholds set out in the definition of medium-sized undertakings in Article 3(3) of Directive 2013/34/EU;

Amendment

(50 a) 'small and medium-sized enterprises' means companies below the thresholds set out in the definition of medium-sized undertakings in Article 3(3) of Directive 2013/34/EU;

Or. en

Amendment 330
Alfred Sant

Proposal for a regulation
Article 3 – paragraph 1 – point 50 a (new)

Text proposed by the Commission

Amendment

(50 a) ‘small enterprise’ means a financial entity as defined in Article 2(2) of the Annex to Recommendation 2003/361/EC.

Or. en

Amendment 331
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 3 – paragraph 1 – point 50 a (new)

Text proposed by the Commission

Amendment

(50 a) 'competent authorities' means national competent authorities in accordance with Article 41 or, for credit institutions considered to be significant, the ECB pursuant to Regulation (EU) No 1024/2013.

Or. en

Amendment 332
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 3 – paragraph 1 – point 50 a (new)

Text proposed by the Commission

Amendment

(50 a) 'Lead Overseer' means the European Banking Authority.

Or. en
Text proposed by the Commission

(50 b) 'service' means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, and where: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; and (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

Justification

Definition from Directive EU 2015/1535 – art. 1 (1) (b).

Text proposed by the Commission

(50 c) 'function' means the identification, protection and prevention, detection, response and recovery, learning and evolution and communication in the use and management of ICT systems.
Amendment 335
Othmar Karas

Proposal for a regulation
Article 3 a (new)

Text proposed by the Commission

Amendment

Article 3 a

Proportionality principle

Financial entities other than those referred to in Article 14a shall implement the rules on ICT risk management foreseen in this Chapter in accordance with the principle of proportionality, by taking into account the size of their undertaking, the nature, scale and complexity of their services, activities and operations, and their overall risk profile.

Justification

This article aims to ensure a more proportionate application of the rules on ICT risk management foreseen in this chapter taking into account the size, nature, scale, complexity and overall risk profile of the financial entities. This has been implemented in a similar way in Article 29(3) of the Solvency II Directive.

Amendment 336
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 4 – paragraph 1

Text proposed by the Commission

Amendment

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

1. Financial entities shall have in place an effective internal governance and control framework that ensures an effective and prudent management of all ICT risks, which is proportionate to the nature, scale and complexity of the entity, with a view to achieving a high level of
digital operational resilience.

Amendment 337
Markus Ferber

Proposal for a regulation
Article 4 – paragraph 1

1. Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. Those frameworks shall be proportionate to the financial entity’s size, nature, scale, complexity and overall risk profile.

Amendment 338
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point a

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

Amendment

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

Amendment 339
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point a a (new)

(a a) put in place procedures and
policies that aim to ensure the resilience, continuity and availability of ICT systems and maintain high standards of security, confidentiality and integrity of data;

Amendment 340
Bogdan Rzońca

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point d

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>(d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan which may be prepared as a independent section of the broader Business Continuity Policy and Disaster Recovery Plan respectively, in order to manage and mitigate risks that could have a harmful effect on the financial entity's ICT systems and ICT services and to facilitate their swift recovery if necessary.</td>
</tr>
</tbody>
</table>

Amendment 341
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point f

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>(f) allocate and periodically review appropriate budget to fulfil the financial entity’s digital operational resilience needs in respect of all types of resources, including relevant training on ICT risks and skills for all staff;</td>
</tr>
</tbody>
</table>
Amendment 342
Bogdan Rzońca

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point i

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

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

Or. en

Amendment 343
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 4 – paragraph 2 – subparagraph 1 – point i

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

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

Or. en

Amendment 344
Markus Ferber

Proposal for a regulation
Article 4 – paragraph 3

Text proposed by the Commission
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

Amendment
3. Financial entities other than small and medium-sized enterprises 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
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.

Amendment 345
Alfred Sant

Proposal for a regulation
Article 4 – paragraph 3

Text proposed by the Commission
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.

Amendment
3. Financial entities other than microenterprises shall establish a role to monitor the arrangements within the entity especially those 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.

Amendment 346
Bogdan Rzońca

Proposal for a regulation
Article 4 – paragraph 4

Text proposed by the Commission
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.

Amendment
4. Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date general knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.
Amendment 347
Frances Fitzgerald

Proposal for a regulation
Article 4 a (new)

Text proposed by the Commission

Amendment

Article 4 a

Proportionality principle

Financial entities shall implement the rules on ICT risk management foreseen in this Chapter in accordance with the principle of proportionality, by taking into account the size of their undertaking, the nature, scale and complexity of their activities and their overall risk profile.

Or. en

Amendment 348
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission

Amendment

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.

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, complexity and risk profile. Such ICT risk management framework shall be based on the three lines of defense model.

Or. en

Amendment 349
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework, which enables them to address and manage ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience that is commensurate to their size, nature, complexity and risk profile.

Or. en

Amendment 350
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 5 – paragraph 3

Text proposed by the Commission

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.

Amendment

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 their ICT risk management framework as requested by the competent authorities in accordance with this Regulation.

Or. en

Amendment 351
Markus Ferber

Proposal for a regulation
Article 5 – paragraph 4
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.

4. As part of the ICT risk management framework referred to in paragraph 1, financial entities other than small and medium-sized enterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance and shall regularly review it.

Or. en

Amendment 352
Alfred Sant

Proposal for a regulation
Article 5 – paragraph 4

Text proposed by the Commission

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.

Amendment

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 where already available in accordance with supervisory guidance as laid out in guidelines established for that purpose by the ESAs and shall regularly review it.

Or. en

Amendment 353
Markus Ferber

Proposal for a regulation
Article 5 – paragraph 5

Text proposed by the Commission

5. Financial entities other than microenterprises shall ensure appropriate segregation of ICT management functions, control functions, and internal audit

Amendment

5. Financial entities other than small and medium-sized enterprises shall ensure appropriate segregation of ICT management functions, control functions,
functions, according to the three lines of defense model, or an internal risk management and control model. Those provisions shall be in line with the financial entity's size, nature, scale, complexity and overall risk profile.

Amendment 354
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 5

Amendment
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.

Text proposed by the Commission
5. Financial entities other than microenterprises shall ensure appropriate independence 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.

Amendment 355
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 5 – paragraph 5

Amendment
5. Financial entities other than microenterprises shall assign the responsibility for managing and overseeing ICT-related risks to a control function and ensure the independence and objectivity of that control function to avoid conflicts of interest. They 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.

Amendment 356
Alfred Sant

Proposal for a regulation
Article 5 – paragraph 5

Text proposed by the Commission

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.

Amendment

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, in coherence and conformity with the guidelines established prior to the entry into force of this Regulation and subsequently further developed and, where applicable, amended, by their respective ESAs in accordance with this Regulation.

Amendment 357
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 7

Text proposed by the Commission

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

Amendment

7. The ICT risk management framework referred to in paragraph 1 shall be audited on a regular basis by internal ICT auditors possessing sufficient knowledge, skills and expertise in ICT risk. The frequency and focus of the internal ICT audits shall be commensurate to the
ICT risks of the financial entity.  

Additionally, at least every three years the internal auditing team shall be accompanied by an external audit firm possessing sufficient knowledge, skills and expertise in ICT risks, to develop an independent opinion on the financial entity's ICT risk management framework.

Amendment 358  
Frances Fitzgerald, Isabel Benjumea Benjumea  

Proposal for a regulation  
Article 5 – paragraph 7

Text proposed by the Commission

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.

Amendment

7. As regards financial entities other than microenterprises, 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.

Amendment 359  
Bogdan Rzońca

Proposal for a regulation  
Article 5 – paragraph 9 – introductory part

Text proposed by the Commission

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:

Amendment

9. The ICT risk management framework referred to in paragraph 1 shall include a 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:
Amendment 360
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 9 – point b

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

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

Amendment 361
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 5 – paragraph 9 – point d

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

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

Amendment 362
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 9 – point d

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

Amendment
(d) explaining the ICT architecture and any changes needed to reach specific business objectives;
Amendment 363
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 9 – point g

Text proposed by the Commission Amendment
(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 deleted

Or. en

Amendment 364
Markus Ferber

Proposal for a regulation
Article 5 – paragraph 9 – point g

Text proposed by the Commission Amendment
(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 deleted

Or. en

Amendment 365
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 5 – paragraph 9 – point g

Text proposed by the Commission Amendment
(g) defining a holistic ICT multi-assessing the need for a multi-

PE693.603v01-00 110/294 AM\1232471EN.docx
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

vendor strategy and, if applicable, and depending on the risk profile of the financial institution, defining a holistic ICT multi-vendor strategy at group level showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of third-party and intra-group service providers. Upon the request of the competent authorities, the multi-vendor strategy may be defined at entity level. A multi-vendor strategy shall be defined at entity level for ICT third-party service providers from third countries.

Amendment 366
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 5 – paragraph 9 – point g

Text proposed by the Commission

(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

Amendment

(g) explaining key dependencies in relation to the use of ICT third-party service providers, where relevant;

Amendment 367
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 5 – paragraph 9 – point h

Text proposed by the Commission

(h) implementing digital operational resilience testing;

Amendment

(h) implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;
Amendment 368
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 9 – point i

Text proposed by the Commission
(i) outlining a communication strategy in case of ICT-related incidents.

Amendment
(i) outlining a communication strategy in case of ICT-related incidents for the purpose of the requirements set out in Article 13.

Amendment 369
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 9 – point i a (new)

Text proposed by the Commission
(i a) reflecting on other available technology tools and solutions that could enhance the continuity and resilience of the financial entity's critical operations.

Amendment

Amendment 370
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 5 – paragraph 10

Text proposed by the Commission
10. Upon approval of competent authorities, financial entities may delegate the tasks of verifying compliance with the ICT risk management requirements to

Amendment
10. Upon notification to, and approval of, competent authorities, financial entities may outsource the tasks of verifying compliance with the ICT risk management requirements to intra-group or external
intra-group or external undertakings. Where such outsourcing occurs, the financial entity shall remain fully accountable for the verification of compliance with ICT risk management requirements.

Or. en

Amendment 371
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 5 – paragraph 10

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.

Text proposed by the Commission

Amendment

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. Where such outsourcing occurs, the financial entity shall remain fully accountable for the verification of compliance with ICT risk management requirements.

Or. en

Amendment 372
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 5 – paragraph 10

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

Text proposed by the Commission

Amendment

Upon notification to competent authorities, financial entities may delegate the task of verifying compliance with the
ICT risk management requirements to intra-group undertakings.

Amendment 373
Bogdan Rzońca

Proposal for a regulation
Article 5 – paragraph 10

Text proposed by the Commission

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.

Amendment

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

Amendment 374
Alfred Sant

Proposal for a regulation
Article 5 – paragraph 10 a (new)

Text proposed by the Commission

10 a. Any processing of personal data that takes place by financial entities and ICT service providers operating on their behalf under Chapters II and III of this Regulation shall be necessary for compliance with a legal obligation in accordance with Article 6(1)(c) of Regulation (EU)2016/679.

Amendment

10 a. Any processing of personal data that takes place by financial entities and ICT service providers operating on their behalf under Chapters II and III of this Regulation shall be necessary for compliance with a legal obligation in accordance with Article 6(1)(c) of Regulation (EU)2016/679.

Amendment 375
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 6 – paragraph 1 – introductory part

**Text proposed by the Commission**

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

**Amendment**

1. **In accordance with their risk profile**, financial entities shall use and maintain updated ICT systems, protocols and tools, **in order to address and manage ICT risk**, which fulfil the following conditions:

Or. en

Amendment 376
Markus Ferber

Proposal for a regulation
Article 6 – paragraph 1 – point a

**Text proposed by the Commission**

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

**Amendment**

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

Or. en

Amendment 377
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 7 – paragraph 1

**Text proposed by the Commission**

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.

**Amendment**

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 **that could pose ICT risks**, the information assets supporting these functions, and the ICT system configurations and interconnections with
Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.

Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.

Amendment 378
Bogdan Rzońca

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all critical or important 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.

Amendment 379
Markus Ferber

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission

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

Amendment

1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all critical ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and
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.

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.

Amendment 380
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Financial entities shall on a regular basis monitor and assess 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.

Or. en

Amendment 381
Bogdan Rzońca

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission

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

Amendment

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.

Or. en

Amendment 382
Markus Ferber

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Financial entities shall on a regular 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.

Justification

Continuous ICT risk implies disproportionate administrative efforts, a regular assessment should be sufficient.

Amendment 383
Markus Ferber

Proposal for a regulation
Article 7 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. Financial entities other than small and medium-sized enterprises 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.
**Amendment 384**  
Bogdan Rzońca  

Proposal for a regulation  
Article 7 – paragraph 3  

*Text proposed by the Commission*  

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.  

*Amendment*  

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. **Subject to supervisory assessment, it shall be for the financial entity in each case to determine whether a major change for the purposes of this paragraph has occurred.**

Or. en

---

**Amendment 385**  
Bogdan Rzońca  

Proposal for a regulation  
Article 7 – paragraph 4  

*Text proposed by the Commission*  

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.  

*Amendment*  

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 **critical or important** ICT assets **having regard to their purpose** and the links and interdependencies between **those** different ICT assets.  

Or. en
Amendment 386  
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation  
Article 7 – paragraph 5

Text proposed by the Commission

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.

Amendment

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

Or. en

Amendment 387  
Alfred Sant

Proposal for a regulation  
Article 7 – paragraph 7

Text proposed by the Commission

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.

Amendment

7. Financial entities other than microenterprises shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment **and classification in terms of the level of criticality of all ICT systems that were in use for a period of at least six years prior to the date of entry into force of this Regulation and of all ICT systems that have been in use for a period of more than six years since that date.**

Or. en

Justification

*Six years is an objective period of time, whereas referring to "old and new technologies" is subjective and can be interpreted differently among stakeholders.*

Amendment 388  
Markus Ferber
Proposal for a regulation
Article 7 – paragraph 7

Text proposed by the Commission

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.

Amendment

7. Financial entities other than small and medium-sized enterprises shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems in relation to critical ICT-related business functions, especially before and after connecting old and new technologies, applications or systems.

Amendment 389
Bogdan Rzońca

Proposal for a regulation
Article 7 – paragraph 7

Text proposed by the Commission

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.

Amendment

7. Following a risk-based approach, financial entities other than microenterprises shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on relevant legacy ICT systems, especially before and after connecting old and new technologies, applications or systems.

Amendment 390
Bogdan Rzońca

Proposal for a regulation
Article 8 – paragraph 2

Text proposed by the Commission

2. Financial entities shall design, procure and implement ICT security

Amendment

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.

Amendment 391
Alfred Sant

Proposal for a regulation
Article 8 – paragraph 3 – introductory part

Text proposed by the Commission
Amendment

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

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

Amendment 392
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 8 – paragraph 3 – introductory part

Text proposed by the Commission
Amendment

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

3. To achieve the objectives referred to in paragraph 2, financial entities shall use ICT technology and processes, in accordance with their risk profile, which:

Amendment 393
Bogdan Rzońca

Proposal for a regulation
Article 8 – paragraph 3 – introductory part

Text proposed by the Commission

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

Amendment

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

Or. en

Amendment 394
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 8 – paragraph 3 – introductory part

Text proposed by the Commission

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

Amendment

3. To achieve the objectives referred to in paragraph 2, financial entities shall use state-of-the-art ICT technology and processes that are proportionate to the risks identified and the size and client base of the relevant financial entity, which:

Or. en

Amendment 395
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 8 – paragraph 3 – point a

Text proposed by the Commission

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

Amendment

(a) minimize the risk for the security of the means of transfer of information;

Or. en

Amendment 396
Bogdan Rzońca
Proposal for a regulation
Article 8 – paragraph 3 – point a

Text proposed by the Commission Amendment

(a) guarantee the security of the means of transfer of information;
(a) keep at a minimum the security of the means of transfer of information;

Amendment 397
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 8 – paragraph 3 – point a

Text proposed by the Commission Amendment

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

Amendment 398
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 8 – paragraph 3 – point c

Text proposed by the Commission Amendment

(c) prevent information leakage;
(c) prevent breach of confidentiality;

Amendment 399
Bogdan Rzońca

Proposal for a regulation
Article 8 – paragraph 4 – introductory part

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

4. Following a risk-based approach and taking into account the financial entity's risk profile, as part of the ICT risk management framework referred to in Article 5(1), financial entities shall:

Amendment 400
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 8 – paragraph 4 – point a

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of their ICT resources, data and information assets while ensuring full protection of customers’ ICT resources, data and information assets within financial entities’ own ICT systems</td>
</tr>
</tbody>
</table>

Justification

Firms can protect against customers’ ICT impacting on the security of the financial entity, but it is disproportionate to ask them to be responsible for ensuring the protection of customers’ own devices.

Amendment 401
Alfred Sant

Proposal for a regulation
Article 8 – paragraph 4 – point b

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(b) following a risk-based approach, establish a sound network and infrastructure management using appropriate techniques, methods and protocols including implementing</td>
<td>(b) following a risk-based approach, establish a sound network and infrastructure management;</td>
</tr>
</tbody>
</table>
automated mechanisms to isolate affected information assets in case of cyber-attacks;

Or. en

Justification

The COM text is overly prescriptive.

Amendment 402
Bogdan Rzońca

Proposal for a regulation
Article 8 – paragraph 4 – point b

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>(b) establish a sound network and infrastructure management using appropriate techniques, methods and protocols and which may consist of implementing automated mechanisms to isolate affected information assets in case of cyber-attacks;</td>
</tr>
</tbody>
</table>

Or. en

Amendment 403
Alfred Sant

Proposal for a regulation
Article 8 – paragraph 4 – point c

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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;</td>
<td>(c) implement policies, procedures and controls 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;</td>
</tr>
</tbody>
</table>

Or. en
Amendment 404
Alfred Sant

Proposal for a regulation
Article 8 – paragraph 4 – point d

Text proposed by the Commission

(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;

Amendment

(d) implement policies and protocols for strong authentication mechanisms, and protection of cryptographic keys, based on relevant standards and dedicated controls systems;

Or. en

Amendment 405
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 8 – paragraph 4 – subparagraph 1

Text proposed by the Commission

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.

Amendment

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

Or. en

Amendment 406
Christophe Hansen

Proposal for a regulation
Article 8 – paragraph 4 – subparagraph 1
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.

**Amendment**

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

Or. en

---

**Amendment 407**

*Isabel Benjumea Benjumea, Frances Fitzgerald*

**Proposal for a regulation**

**Article 9 – paragraph 1 – introductory part**

**Text proposed by the Commission**

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.

**Amendment**

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 *and monitor the* potential material single points of failure.

Or. en

---

**Amendment 408**

*Bogdan Rzońca*

**Proposal for a regulation**

**Article 9 – paragraph 1 – introductory part**

**Text proposed by the Commission**

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.

**Amendment**

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 if technologically available,
material single points of failure.

to identify all potential material single points of failure.

Amendment 409
Bogdan Rzońca

Proposal for a regulation
Article 9 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. The detection mechanisms referred to in paragraph 1 shall trigger ICT-related incident detection and ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.

Amendment 410
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 9 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. Financial entities shall devote sufficient resources and capabilities, appropriate to their size, nature, complexity, business and risk profiles, to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.
Proposal for a regulation
Article 9 – paragraph 3

Text proposed by the Commission

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.

Amendment

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

Proposal for a regulation
Article 10 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Based on the identification requirements set out in Article 7, financial entities shall put in place dedicated and comprehensive business continuity and disaster recovery plans, which could be prepared as a dedicated ICT Business Continuity Policy. Financial entities shall implement those dedicated, appropriate and documented arrangements, plans, procedures and mechanisms. Financial entities shall specifically consider risks that could have a harmful impact on ICT services and ICT systems. The plans shall support objectives to protect, and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets.

The plans shall further aim to:

a) activate without delay dedicated plans that enable containment measures, processes and technologies suited to each
type of ICT-related incident and prevent further damage, as well as tailored responses and recovery methods established in accordance with Article 11;
b) estimate preliminary impacts, damages and losses;

Financial entities shall coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

Or. en

Amendment 413
Bogdan Rzońca

Proposal for a regulation
Article 10 – paragraph 2 – introductory part

Text proposed by the Commission

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:

Amendment

2. The overseeing authority, in cooperation with the Platform on Cybersecurity of Financial Sector, shall develop guidelines containing best practices and recommendations concerning the business continuity and disaster recovery plans referred to in paragraph 1 by [PO: insert date 1 year after the date of entry into force of this Regulation]. Those guidelines shall be reviewed at least once a year, or whenever deemed necessary by the Platform on Cybersecurity of Financial Sector.

Or. en

Amendment 414
Bogdan Rzońca

Proposal for a regulation
Article 10 – paragraph 2 – point a

Text proposed by the Commission

Amendment
(a) recording all ICT-related incidents; deleted

Amendment 415
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 2 – point b

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

Amendment 416
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 2 – point c

(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; deleted

Amendment 417
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 2 – point d

Text proposed by the Commission Amendment
(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;

Amendment 418
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 2 – point e

Text proposed by the Commission
Amendment

(e) estimating preliminary impacts, damages and losses;

Amendment 419
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 2 – point f

Text proposed by the Commission
Amendment

(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.

Amendment 420
Bogdan Rzońca
Proposal for a regulation
Article 10 – paragraph 3

Text proposed by the Commission

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.

Amendment

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 small and medium-sized enterprises, shall be subject to independent audit reviews.

Amendment 421
Markus Ferber

Proposal for a regulation
Article 10 – paragraph 3

Text proposed by the Commission

4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably

4. Financial entities shall put in place, maintain and periodically test appropriate ICT Response and Recovery plans, notably

Amendment

Amendment 422
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni
with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.

**Amendment 423**

**Bogdan Rzońca**

**Proposal for a regulation**

**Article 10 – paragraph 4**

*Text proposed by the Commission*

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.

*Amendment*

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

**Amendment 424**

**Christophe Hansen**

**Proposal for a regulation**

**Article 10 – paragraph 5 – point a**

*Text proposed by the Commission*

(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least *yearly and after* substantive changes to the ICT systems;

*Amendment*

(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least *every three years and, if* substantive changes to the ICT systems *occurred, in the year thereafter*;

**Amendment 425**

**Bogdan Rzońca**
Proposal for a regulation
Article 10 – paragraph 5 – point a

*Text proposed by the Commission*

(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after *substantive* changes to the ICT systems;

*Amendment*

(a) test the Business Continuity Policy and the Disaster Recovery Plan at least yearly and after *major* changes to *critical or important* ICT systems;

Or. en

Amendment 426
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 10 – paragraph 5 – point a

*Text proposed by the Commission*

(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to the ICT systems;

*Amendment*

(a) test the ICT business continuity policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to the ICT systems *following a risk-based approach*;

Or. en

Amendment 427
Markus Ferber

Proposal for a regulation
Article 10 – paragraph 5 – subparagraph 1

*Text proposed by the Commission*

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.

*Amendment*

For the purposes of point (a), financial entities other than *small and medium-sized enterprises* 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.
Amendment 428
Markus Ferber

Proposal for a regulation
Article 10 – paragraph 6

Text proposed by the Commission

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.

Amendment

6. Financial entities other than small and medium-sized enterprises 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.

Or. en

Amendment 429
Alfred Sant

Proposal for a regulation
Article 10 – paragraph 6

Text proposed by the Commission

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.

Amendment

6. Financial entities other than microenterprises shall have a crisis management function, which may be nested under functions responsible for incident response and management or be a dedicated function and 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.

Or. en
Amendment 430
Bogdan Rzońca

Proposal for a regulation
Article 10 – paragraph 7

Text proposed by the Commission

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.

Amendment

7. Financial entities shall keep records of relevant activities during disruption events when their ICT Business Continuity Policy or ICT Disaster Recovery Plan is activated. Such records shall be readily available to the relevant competent authority if requested.

Or. en

Amendment 431
Bogdan Rzońca

Proposal for a regulation
Article 10 – paragraph 9

Text proposed by the Commission

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

Amendment

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

deleted

Or. en

Amendment 432
Markus Ferber

Proposal for a regulation
Article 10 – paragraph 9

Text proposed by the Commission

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

Amendment

9. Financial entities other than small and medium-sized enterprises shall report to competent authorities all substantial costs and losses caused by ICT disruptions.
and ICT-related incidents.

Amendment 433
Alfred Sant

Proposal for a regulation
Article 10 – paragraph 9

*Text proposed by the Commission*

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

*Amendment*

9. Financial entities other than microenterprises shall report to competent authorities a yearly review of costs and losses caused by ICT disruptions and ICT-related incidents.

Amendment 434
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 10 – paragraph 9

*Text proposed by the Commission*

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

*Amendment*

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

Amendment 435
Bogdan Rzońca

Proposal for a regulation
Article 11 – paragraph 1 – introductory part

*Text proposed by the Commission*

*Amendment*
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:

Amendment 436
Christophe Hansen

Proposal for a regulation
Article 11 – paragraph 2

*Text proposed by the Commission*

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.*

*Amendment*

2. Financial entities shall establish backup systems *that operate in accordance with the backup policies.*

Amendment 437
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 11 – paragraph 2

*Text proposed by the Commission*

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.*

*Amendment*

2. In accordance with the backup policies specified in paragraph 1(a), financial entities shall ensure that backup systems are operating adequately according to the backup processes. The activation of backup systems shall *not* jeopardize the security of the network and information systems or the integrity or confidentiality of data.
Amendment 438
Bogdan Rzońca

Proposal for a regulation
Article 11 – paragraph 4

Text proposed by the Commission  

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

Amendment

4. Financial entities shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure the financial entity is capable to ensure its resilience objectives for critical and important functions.

Or. en

Amendment 439
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 11 – paragraph 4

Text proposed by the Commission  

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

Amendment

4. Financial entities other than small and microenterprises shall assess the need to maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.

Or. en

Amendment 440
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 11 – paragraph 5 – introductory part

Text proposed by the Commission  

5. Financial entities referred to in point (f) of Article 2(1) shall maintain or

Amendment

5. Financial entities referred to in point (f) of Article 2(1) shall maintain at
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.

Amendment 441
Alfred Sant

Proposal for a regulation
Article 11 – paragraph 5 – introductory part

Text proposed by the Commission

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.

Amendment

5. Financial entities referred to in point (f) of Article 2(1) shall maintain at least one secondary processing site endowed with resources, capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.

Amendment 442
Bogdan Rzońca

Proposal for a regulation
Article 11 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission

(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;

Amendment

(a) located, designed or capable, in order to ensure a distinct risk profile as compared to the primary site, and to prevent it from being affected by the incident which has affected the primary site;
Amendment 443
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 11 – paragraph 5 – subparagraph 1 – point a

Text proposed by the Commission
(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;

Amendment
(a) located, designed or equipped 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;

Amendment 444
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 11 – paragraph 6

Text proposed by the Commission
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.

Amendment
6. In determining the recovery time and point objectives for each function, financial entities shall take into account the potential overall impact on digital operational resilience and critical or important functions. Such time objectives shall ensure that, in severe scenarios, the agreed service levels are met.

Amendment 445
Markus Ferber

Proposal for a regulation
Article 11 – paragraph 6

Text proposed by the Commission
6. In determining the recovery time and point objectives for each function, financial entities shall take into account the

Amendment
6. In determining the recovery time and point objectives for each function,
potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.
<table>
<thead>
<tr>
<th>Amendment 448</th>
<th>Markus Ferber</th>
</tr>
</thead>
</table>
| **Proposal for a regulation**  
**Article 12 – paragraph 1**  
*Text proposed by the Commission*  
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. |
| **Amendment**  
1. Financial entities shall have in place capabilities and staff, suited to their size, *complexity*, business and *overall* 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. |
| Or. en |

<table>
<thead>
<tr>
<th>Amendment 449</th>
<th>Bogdan Rzońca</th>
</tr>
</thead>
</table>
| **Proposal for a regulation**  
**Article 12 – paragraph 2 – introductory part**  
*Text proposed by the Commission*  
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. |
| **Amendment**  
2. Financial entities shall put in place post *major* 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 Business Continuity Policy referred to in Article 10. |
| Or. en |

<table>
<thead>
<tr>
<th>Amendment 450</th>
<th>Markus Ferber</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proposal for a regulation</strong></td>
<td></td>
</tr>
</tbody>
</table>
Article 12 – paragraph 2 – subparagraph 1

Text proposed by the Commission

Amendment

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

Or. en

Amendment 451
Alfred Sant

Proposal for a regulation
Article 12 – paragraph 2 – subparagraph 1

Text proposed by the Commission

Amendment

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

When implementing changes to their ICT operations, financial entities other than microenterprises shall communicate all such significant changes to the competent authorities.

Or. en

Amendment 452
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 12 – paragraph 2 – subparagraph 1

Text proposed by the Commission

Amendment

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

When implementing changes related to addressing ICT-risk, financial entities other than microenterprises shall communicate those changes to the competent authorities.

Or. en

Amendment 453
Alfred Sant

Proposal for a regulation
Article 12 – paragraph 2 – subparagraph 2 – introductory part

Text proposed by the Commission
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:

Amendment
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, namely, where deemed relevant, in relation to:

Amendment 454
Markus Ferber

Proposal for a regulation
Article 12 – paragraph 6 – introductory part

Text proposed by the Commission
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.

Amendment
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 operating critical ICT systems and to senior management staff.

Justification
Not every member of staff needs to do ICT security awareness programs.

Amendment 455
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 12 – paragraph 6 – subparagraph 1

Text proposed by the Commission
Financial entities shall monitor relevant

Amendment
Financial entities, other than
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.

Amendment 456
Alfred Sant

Proposal for a regulation
Article 13 – paragraph 1

Text proposed by the Commission

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.

Amendment

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 major ICT-related incidents to clients and counterparts when, where and as appropriate.

Amendment 457
Bogdan Rzońca

Proposal for a regulation
Article 13 – paragraph 1

Text proposed by the Commission

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

Amendment

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 major ICT-related incidents to clients and counterparts
and counterparts as well as to the public, as appropriate.

Amendment 458
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 13 – paragraph 1

Text proposed by the Commission

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.

Amendment

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 major ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.

Or. en

Amendment 459
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 13 – paragraph 3

Text proposed by the Commission

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.

Amendment

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

Or. en

Amendment 460
Alfred Sant
Proposal for a regulation
Article 14 – paragraph 1 – point a

Text proposed by the Commission

(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;

Amendment

(a) specify structural and supplementary 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 and undue delays;

Or. en

Amendment 461
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 14 – paragraph 1 – point b

Text proposed by the Commission

(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;

Amendment

deleted

(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;

Or. en

Amendment 462
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 14 – paragraph 1 – point b a (new)
Text proposed by the Commission

Amendment

(b a) incorporate security controls into systems from inception (security by design)

Or. en

Amendment 463
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 14 – paragraph 1 – point c

Text proposed by the Commission

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

deleted

Or. en

Amendment 464
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 14 – paragraph 1 a (new)

Text proposed by the Commission

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

Amendment 465
Othmar Karas

Proposal for a regulation
Article 14 a (new)
Article 14 a

Proportionate ICT risk management framework

1. Articles 4 to 14 of this Regulation shall not apply to small and non-interconnected investment firms or payment institutions exempted by Directive (EU) 2015/2366, to credit institutions exempted by Directive 2013/36/EU, to electronic money institutions exempted by Directive 2009/110/EC or to small institutions for occupational retirement pensions.

2. Small and non-interconnected investment firms, payment institutions exempted by Directive (EU) 2015/2366, credit institutions exempted by Directive 2013/36/EU, electronic money institutions exempted by Directive 2009/110/EC and small institutions for occupational retirement pensions shall implement an ICT risk management framework in accordance with the principle of proportionality, by taking into account the size of their undertaking, the nature, scale, complexity of their services, activities and operations and their overall risk profile and shall:

(a) put in place and maintain a sound and documented ICT risk management framework which details the mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, including for the protection of relevant physical components and infrastructures.

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

(c) minimise the impact of ICT risks through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate for supporting the performance of their activities and the provision of services;

(d) adequately protect confidentiality, integrity and availability of data network...
and information systems;
(e) allow sources of risk and anomalies in the network and information systems to be promptly identified and detected and ICT incidents to be swiftly handled.

Or. en

Justification


Amendment 466
Bogdan Rzońca

Proposal for a regulation
Article 15 – paragraph 2

Text proposed by the Commission

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.

Amendment

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 addressed in order to prevent the occurrence of such incidents.

Or. en

Amendment 467
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 15 – paragraph 2

Text proposed by the Commission

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

Amendment

2. As part of the ICT-incident management process, financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and
and eradicated to prevent the occurrence of such incidents.

follow-up of ICT-related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents.

Amendment 468
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 15 – paragraph 3 – point d

Text proposed by the Commission
(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;

Amendment
(d) ensure that at least 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 major ICT-related incidents;

Amendment 469
Bogdan Rzońca

Proposal for a regulation
Article 15 – paragraph 3 – point d

Text proposed by the Commission
(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;

Amendment
(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 major ICT-related incidents;

Amendment 470
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 15 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. The requirements laid down in the paragraphs 1, 2 and 3 shall apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern financial entities referred to in points (a), (b) and (c) of Article 2(1).

Or. en

Amendment 471
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 15 a (new)

Text proposed by the Commission

Amendment

Article 15 a

Operational or security payment-related incidents concerning financial entities referred to in points (a), (b) and (c) of Article 2(1)

The requirements laid down in Chapter III of this Regulation shall apply to operational or security payment-related incidents and to major operational or security payment-related incidents where they concern financial entities referred to in points (a), (b) and (c) of Article 2(1).

Or. en

Amendment 472
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 16 – paragraph 1 – point a
Text proposed by the Commission

(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;

Amendment

(a) the number of users or financial counterparts affected by the disruption caused by the ICT-related incident;

Or. en

Amendment 473
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 16 – paragraph 1 – point c

Text proposed by the Commission

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

Amendment

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

Or. en

Amendment 474
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 16 – paragraph 1 a (new)

Text proposed by the Commission

1 a. The classification requirements laid down in paragraph 1 shall apply to operational or security payment-related incidents and major operational or security payment-related incidents in cases where they concern financial entities referred to in points (a), (b) and (c) of Article 2(1).

Amendment

Or. en
Amendment 475
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 16 – paragraph 1 b (new)

Text proposed by the Commission

1 b. 1b. Financial entities shall classify significant cyber threats based on the following criteria:

(a) the number or relevance of clients or financial counterparts targeted and, where applicable, the amount or number of transactions targeted by the significant cyber threat;

(b) the duration or the frequency of the significant cyber threat;

(c) the geographical spread with regard to the areas targeted by the significant cyber threat, particularly if it affects more than two Member States;

(d) the criticality of the services targeted, including the financial entity’s transactions and operations;

Amendment

Or. en

Amendment 476
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Article 16 – paragraph 2 – introductory part

Text proposed by the Commission

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:

Amendment

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

Or. en
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:

Or. en

(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

Amendment 478
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 16 – paragraph 2 – point b

(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.

Amendment 480
Bogdan Rzońca

Proposal for a regulation
Article 16 – paragraph 2 – point b

Text proposed by the Commission

(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.

Amendment

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

Or. en

Amendment 481
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 16 – paragraph 2 – point b

Text proposed by the Commission

(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.

Amendment

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

related incidents reports to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.

Amendment 482
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 16 – paragraph 2 – point b a (new)

Text proposed by the Commission

Amendment

(b a) the criteria set out in paragraph 1b, including high materiality thresholds for determining significant cyber threats which are subject to the reporting obligation laid down in Article 17 (1a);

Amendment 483
Alfred Sant

Proposal for a regulation
Article 16 – paragraph 3 – introductory part

Text proposed by the Commission

Amendment

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.

3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities, as well as international standards and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. The ESAs shall further take into account that the timely and efficient management of an incident by small and microenterprises is not constricted by the need to respect the classification requirements set out in this Article.
**Amendment 484**
Markus Ferber

Proposal for a regulation
Article 16 – paragraph 3 – introductory part

*Text proposed by the Commission*

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.

*Amendment*

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 also take into consideration the nature, size and complexity of the financial entities concerned.*

**Amendment 485**
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 16 – paragraph 3 – subparagraph 1

*Text proposed by the Commission*

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].

*Amendment*

The ESAs shall submit those common draft regulatory technical standards to the Commission by [PO: insert date 3 years after the date of entry into force].

**Amendment 486**
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 16 – paragraph 3 – subparagraph 1
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].

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

Amendment 487
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 17 – title

Text proposed by the Commission
Amendment

17 Reporting of major ICT-related incidents

17 Reporting of major ICT-related incidents and significant cyber threats

Amendment 488
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 1 – introductory part

Text proposed by the Commission
Amendment

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.

1. Financial entities shall report major operational incidents to the single EU hub as referred to in Article 19, within the time-limits laid down in paragraph 3. Where the major operational incident also amounts to a personal data breach, financial entities shall notify it to the relevant data protection authority and to the affected data subjects, where relevant, in line with Article 33 of Regulation 2016/679.
Amendment 489
Billy Kelleher, Engin Eroglu, Gilles Boyer, Caroline Nagtegaal, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 17 – paragraph 1 – introductory part

Text proposed by the Commission

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.

Amendment

1. Financial entities shall report major ICT-related incidents to the single EU Hub as referred to in Article 19, within the time-limits laid down in paragraph 3.

Or. en

Amendment 490
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 17 – paragraph 1 – subparagraph 1

Text proposed by the Commission

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.

Amendment

For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, an incident report using the single EU Hub.

Or. en

Amendment 491
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 1 – subparagraph 1

Text proposed by the Commission

For the purpose of the first subparagraph, financial entities shall produce, after

Amendment

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**.

collecting and analysing all relevant information, an incident report using the template referred to in Article 18 and submit it to the **single EU hub**.

Amendment 492
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 17 – paragraph 1 a (new)

**Text proposed by the Commission**

1 a. Financial entities shall notify significant cyber threats without undue delay to the relevant competent authority as referred to in Article 41.

**Amendment**

1 a. Financial entities shall notify significant cyber threats without undue delay to the relevant competent authority as referred to in Article 41.

Amendment 493
Alfred Sant

Proposal for a regulation
Article 17 – paragraph 2

**Text proposed by the Commission**

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.

2. Where a major ICT-related incident has or may have a material impact on the financial interests of service users and clients, financial entities shall, without undue delay after having become aware of it, 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.

Or. en
Amendment 494
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Where a major ICT-related incident **occurs and has a material** 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 **pertinent** measures which have been taken to mitigate the adverse effects of such incident.

Or. en

Amendment 495
Bogdan Rzońca

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Where a major ICT-related incident has 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 **relevant** measures which have been taken to mitigate the adverse effects of such incident.

Or. en

Amendment 496
Markus Ferber

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission

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.

Amendment

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. Where no harm to service users and clients materialises due to the countermeasures taken by the financial entity, the requirement to inform service users and clients shall not apply.

Or. en

Amendment 497
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation

Article 17 – paragraph 2

Text proposed by the Commission

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.

Amendment

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. Where such incident materialises, the financial entities shall release a public statement, in addition to individually informing their service users and clients.

Or. en
Amendment 498
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 17 – paragraph 2 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 a. Where a significant cyber threat could adversely impact the financial interests of clients, financial entities shall inform their clients, without undue delay, of the significant cyber threat and of the measures which the financial entity intends to take to mitigate the adverse effects of such threat. Where appropriate, the financial entity shall also advise its clients on the measures they can take to mitigate the adverse effects of the threat.</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

Amendment 499
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 2 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 a. Where the risk of a major ICT-related incident emerges but does not materialise due to the counter measures adopted, financial entities may release a public statement instead of individually informing their service users and clients.</td>
<td>Or. en</td>
</tr>
</tbody>
</table>

Amendment 500
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 2 b (new)
2 b. Where a major operational incident causes financial losses to their service users and clients, financial entities shall be liable for the compensation of the proven losses incurred by those service users and clients.

Amendment 501
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 3 – introductory part

Text proposed by the Commission

Amendment

3. Financial entities shall submit to the competent authority as referred to in Article 41:

3. Financial entities shall submit to the single EU hub as referred to in Article 19:

Amendment 502
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 17 – paragraph 3 – introductory part

Text proposed by the Commission

Amendment

3. Financial entities shall submit to the competent authority as referred to in Article 41:

3. Financial entities shall submit to the single EU Hub as referred to in Article 19:

Amendment 503
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 3 – point a

Text proposed by the Commission

(a) an initial notification, without delay, but no later than 24 hours after the operational incident is classified as major by the financial entity;

Amendment

(a) an initial notification, without undue delay, but no later than the end of the next business day, or, where reporting channels are not available, as soon as they become available;

Or. en

Amendment 504
Markus Ferber

Proposal for a regulation
Article 17 – paragraph 3 – point a

Text proposed by the Commission

(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;

Amendment

(a) an initial notification, without delay, but no later than the end of the next business day, or, where reporting channels are not available, as soon as they become available;

Or. en

Amendment 505
Bogdan Rzońca

Proposal for a regulation
Article 17 – paragraph 3 – point a
(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;

(a) an initial notification, without delay and in any event within 24 hours of becoming aware of the incident, or, where reporting channels are not available, as soon as they become available;

Or. en

Amendment 506
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 17 – paragraph 3 – point a

Text proposed by the Commission

(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;

(a) in case of a major ICT-related incident, a notification from critical ICT third-party providers to the competent authority of the major ICT-related incident, without undue delay and not later than 72 hours after becoming aware of it;

Or. en

Amendment 507
Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 17 – paragraph 3 – point a

Text proposed by the Commission

(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;

(a) an initial notification, without delay, but no later than 24 hours after 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;

ICT-related incident is classified as major by the financial entity, or, where reporting channels are not available, as soon as they become available;

Or. en

**Justification**

Aligns the timing requirements for incident reporting with the NIS 2.0 proposal, thus harmonising the EU incident reporting regime further.

**Amendment 508**

Alfred Sant

**Proposal for a regulation**

**Article 17 – paragraph 3 – point a**

**Text proposed by the Commission**

(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;

**Amendment**

(a) an initial notification, without delay, after becoming aware of a major ICT-incident and making best efforts to do so no later than the end of the business day, or, in case of a major ICT-related incident that the financial entity became aware of 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;

Or. en

**Amendment 509**

Frances Fitzgerald, Isabel Benjumea Benjumea

**Proposal for a regulation**

**Article 17 – paragraph 3 – point a**

**Text proposed by the Commission**

**Amendment**
(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 initial report, to be updated as soon as possible after a financial entity becomes aware that the status of the original incident has changed significantly or new information has come to light that could have a major impact on how the incident is addressed by the competent authority;
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; becomes available following the initial notification or, if expressly required by the competent authority, 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;

Amendment 512
Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 17 – paragraph 3 – point c

Text proposed by the Commission

(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

Amendment

(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 day of sending the initial report. In duly justified cases, and following agreement with the competent authority, financial entities may deviate from the deadline laid down in this point.

Amendment 513
Alfred Sant

Proposal for a regulation
Article 17 – paragraph 3 – point c

Text proposed by the Commission

(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

Amendment

(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

actual impact figures are available to replace estimates and at the latest one month from the date of resolution of the incident

Amendment 514
Bogdan Rzońca

Proposal for a regulation
Article 17 – paragraph 3 – subparagraph 1 (new)

Text proposed by the Commission

Amendment

The relevant competent authority as referred to in Article 41 shall provide that, in duly justified cases, a financial entity is permitted to deviate from the deadlines set out in points (a), (b) and (c) of this paragraph.

Amendment 515
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 17 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. Due consideration shall be given to the ability of financial entities to provide accurate and meaningful information in relation to major ICT-related incidents within the timeframes set out in points (a) and (b) of paragraph 3.

Amendment 516
Mikuláš Peksa
on behalf of the Greens/EFA Group
Proposal for a regulation
Article 17 – paragraph 4

Text proposed by the Commission  

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.

Amendment

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.

Or. en

Proposal for a regulation
Article 17 – paragraph 4

Text proposed by the Commission  

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.

Amendment

4. Financial entities may only delegate the reporting obligations under this Article to a third-party service provider after agreeing a contractual provision with the ICT third-party service provider concerned, upon approval of the delegation by the relevant competent authority referred to in Article 41.

Or. en

Proposal for a regulation
Article 17 – paragraph 4

Text proposed by the Commission  

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.

Amendment

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.
Amendment 519
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 17 – paragraph 4

Text proposed by the Commission

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.

Amendment

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. In cases of such delegation, the financial entity shall
remain fully accountable for the fulfilment of the incident reporting requirements.

Or. en

Amendment 520
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer,
Stéphanie Yon-Courtin

Proposal for a regulation
Article 17 – paragraph 5

Text proposed by the Commission

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

Amendment
deleted

(a) EBA, ESMA or EIOPA, as
(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.

Amendment 521
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 5

Text proposed by the Commission

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.

Amendment 522
Bogdan Rzońca

Proposal for a regulation
Article 17 – paragraph 5 – introductory part

Text proposed by the Commission

5. Upon receipt of the report referred to in paragraph 1, the competent authority

Or. en
shall, without undue delay, provide details of the incident to:

shall, without undue delay and while respecting high security standards and after assessing potential risks, provide relevant information on the incident to:

Amendment 523
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 17 – paragraph 5 – introductory part

Text proposed by the Commission

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

Amendment

5. Upon receipt of the report referred to in paragraph 1 or the notification referred to in paragraph 1a, the competent authority shall, without undue delay, provide details of the major ICT-related incident or significant cyber threat to:

Amendment 524
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 17 – paragraph 5 – point c a (new)

Text proposed by the Commission

(c a) the Single Resolution Board for entities referred to in Article 7(2) of Regulation EU 806/2014, and national resolution authorities in relation to entities referred to in Article 7(3) of Regulation EU 806/2014. National resolution authorities should provide to the SRB, on a six monthly basis, a summary of the report received under this Article.

Amendment

Or. en
Amendment 525
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 17 – paragraph 6

Text proposed by the Commission

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.

Amendment

6. EBA, ESMA or EIOPA and the ECB, in cooperation with ENISA, 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.

Or. en

Amendment 526
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 18 – paragraph 1 – introductory part

Text proposed by the Commission

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

Amendment

1. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB and national supervisory authorities, shall develop:

Or. en

Amendment 527
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 18 – paragraph 1 – introductory part
1. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop:

Amendment

Or. en

Amendment 528
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 18 – paragraph 1 – point a – point 1 a (new)

(1 a) establish the content of the notification for significant cyber threats;

Or. en

Amendment 529
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 18 – paragraph 1 – point b

(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and notify a significant cyber threat.

Or. en

Amendment 530
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 18 – paragraph 1 – subparagraph 1
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].

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 2 years after the date of entry into force].

Amendment 531
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 19 – paragraph 1

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.

1. ESAs shall establish and operate a single EU Hub for major ICT-related incident reporting by financial entities.

Justification
There is widespread recognition that a single EU reporting hub would provide more certainty and clarity for financial entities as well as greater efficiency to the reporting system as a whole. The ESAs have indicated that they are willing to establish a single centralised reporting Hub in the near term, rather than develop individual systems pending the outcome of the feasibility study proposed in Article 19 of the Commission proposal.
Amendment 532
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. The ESAs shall establish and operate a single EU Hub for major operational incident reporting by financial entities.

Or. en

Amendment 533
Bogdan Rzońca

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. The ESAs, through the Joint Committee and in cooperation with ECB, ENISA and the Platform on Cybersecurity of Financial Sector, 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.
Amendment 534
Alfred Sant

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission
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.

Amendment
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 that would replace all pre-existing 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.

Amendment 535
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission
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

Amendment
1. The ESAs, through the Joint Committee and in consultation with ECB, ENISA and national supervisory authorities, 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
view to enhancing supervisory convergence.
and underpin thematic analyses with a view to enhancing supervisory convergence.

Amendment 536
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 19 – paragraph 2

Text proposed by the Commission

Amendment

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

Or. en

Amendment 537
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin

Proposal for a regulation
Article 19 – paragraph 2

Text proposed by the Commission

Amendment

2. The report referred to in the paragraph 1 shall comprise at least the

PE693.603v01-00 184/294 AM\1232471EN.docx
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.

Amendment 538
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru, Stéphanie Yon-Courtin, Gilles Boyer

Proposal for a regulation
Article 19 – paragraph 2 – introductory part

Text proposed by the Commission
2. The report referred to in the paragraph 1 shall comprise at least the following elements:

Amendment
2. The EU Hub shall collect and maintain incident data and shall ensure that the entities referred to in paragraph 3 have direct and immediate access to the relevant information.

Amendment 539
Bogdan Rzońca

Proposal for a regulation
Article 19 – paragraph 2 – point b a (new)

Text proposed by the Commission
(b a) capability to establish the interoperability and assess its added value with regard to other relevant reporting

Amendment
schemes, such as in Directive (EU) 2016/1148.

Amendment 540
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 19 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. The EU Hub shall collect and maintain incident data and shall ensure that the entities referred to in paragraph 3 have direct and immediate access to the relevant information.

Amendment 541
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 19 – paragraph 3

Text proposed by the Commission

Amendment

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].

3. The EU Hub shall make the necessary information available to the following entities to enable them to fulfil their respective responsibilities and mandates:

(a) Competent authorities as referred to in Article 41;

(b) EBA, ESMA or EIOPA, as appropriate;

(c) the ECB, as appropriate, in the case of financial entities referred to in points (a), (b) and (c) of Article 2(1);
(d) the single point of contact designated under Article 8 of Directive (EU) 2016/1148;

(e) the Single Resolution Board (SRB), for entities referred to in Article 7(2) of Regulation (EU) No 806/2014, and national resolution authorities in relation to entities referred to in Article 7(3) of Regulation (EU) No 806/2014; and

(f) the relevant national CSIRT belonging to the CSIRTs network as established by Article 12 of Directive (EU) 2016/1148, in cases where the reporting entity falls within the scope of that Directive.

Justification

Replaces Amendments 58 and 59.

Amendment 542
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 19 – paragraph 3

Text proposed by the Commission

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].

Amendment

3. The EU Hub shall make the necessary information available to the following entities to enable them to fulfil their respective responsibilities and mandates:

(a) competent authorities as referred to in Article 41;

(b) EBA, ESMA or EIOPA, as appropriate;

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

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

(e) the Single Resolution Board (SRB), for entities referred to in Article 7(2) of Regulation (EU) No 806/2014, and national resolution authorities in relation to entities referred to in Article 7(3) of Regulation (EU) No 806/2014.

Amendment 543
Mikuláš Peksa on behalf of the Greens/EFA Group

Proposal for a regulation
Article 19 – paragraph 3 a (new)

_text proposed by the Commission_

3 a. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop common draft regulatory technical standards specifying the following:

(a) modalities and operational standards for the collection and aggregation of incident reporting information and for the entities referred to in paragraph 3 to access that information;

(b) the terms and conditions, the arrangements and the required documentation under which access to the EU Hub is granted to the entities referred to in paragraph 3;

(c) the conditions for membership of financial entities.

Or. en

Amendment 544
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Gilles Boyer, Stéphanie Yon-Courtin, Dragoș Pîslaru

Proposal for a regulation
Article 19 – paragraph 3 a (new)

Text proposed by the Commission

3 a. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop common draft regulatory technical standards specifying the following:

(a) modalities and operational standards for the entities referred to in paragraph 3 to access the EU Hub;

(b) the terms and conditions, the arrangements and the required documentation under which access to the EU Hub is granted to the entities referred to in paragraph 3;

(c) the conditions for membership of financial entities.

Amendment

3 a. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop common draft regulatory technical standards specifying the following:

(a) modalities and operational standards for the entities referred to in paragraph 3 to access the EU Hub;

(b) the terms and conditions, the arrangements and the required documentation under which access to the EU Hub is granted to the entities referred to in paragraph 3;

(c) the conditions for membership of financial entities.

Or. en

Amendment 545

Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation

Article 20 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Upon receipt of a report as referred to in Article 17(1) and (1a), 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 and also provide appropriately anonymised feedback, insight and intelligence to all relevant financial entities where it could be beneficial, based on any major incident reports they receive.

Or. en
Justification

To support broader industry preparedness for incidents, addition of the obligation for the authorities to provide appropriately anonymised feedback to all relevant financial entities.

Amendment 546
Alfred Sant

Proposal for a regulation
Article 20 – paragraph 2 – introductory part

Text proposed by the Commission

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.

Amendment

2. The ESAs shall, through the Joint Committee, report *every six months* on an anonymised and aggregated basis on the ICT-related incident and cyber threat notifications received from competent authorities *in accordance with Article 17(1) and 17(1.1)*, setting out at least the number of ICT-related major incidents and significant cyber threats, their nature, impact on the operations of financial entities or customers, costs and remedial actions taken.

Or. en

Amendment 547
Bogdan Rzońca

Proposal for a regulation
Article 20 – paragraph 2 – introductory part

Text proposed by the Commission

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.

Amendment

2. The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the major 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, *estimated* costs and remedial actions taken.
Proposal for a regulation
Article 21 – paragraph 1

Text proposed by the Commission

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.

Amendment

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, other than microenterprises, shall establish, maintain and review, in accordance with their size, nature, complexity 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.

Amendment 549
Markus Ferber

Proposal for a regulation
Article 21 – paragraph 1

Text proposed by the Commission

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

Amendment

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, that are not small and medium-sized enterprises, shall establish, maintain and review, with due consideration to their nature, size, complexity, business and overall risk profiles, a sound and comprehensive digital
risk management framework referred to in Article 5.

operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.

Amendment 550
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 21 – paragraph 2

Text proposed by the Commission

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.

Amendment

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. Where Union legislation requires financial entities to carry out any digital operational or resilience testing and monitoring, the financial entities may pool such programmes and activities, provided they meet the requirements of any applicable legislation.

Or. en

Amendment 551
Alfred Sant

Proposal for a regulation
Article 21 – paragraph 3

Text proposed by the Commission

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

Amendment

3. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme as defined 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.

services provided, as well as any other factor the financial entity deems appropriate.

Or. en

**Amendment 552**
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

**Proposal for a regulation**
**Article 21 – paragraph 4**

*Text proposed by the Commission*

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

*Amendment*

4. Financial entities shall ensure that tests, including threat led penetration testing, are undertaken by independent parties, whether internal or external. In the case of an internal tester, an adequate analysis and identification of the proper resources to be allocated in the design and execution phases of the tests shall be performed, in order to avoid any conflicts of interest and other potential managerial issues.

Or. en

**Amendment 553**
Bogdan Rzońca

**Proposal for a regulation**
**Article 21 – paragraph 5**

*Text proposed by the Commission*

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.

*Amendment*

5. Financial entities shall establish procedures and policies to prioritise, classify and address 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.

Or. en
Amendment 554
Bogdan Rzońca

Proposal for a regulation
Article 21 – paragraph 6

Text proposed by the Commission

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

Amendment

6. Following a risk-based approach, financial entities shall ensure that appropriate tests are performed on critical ICT systems and applications at least yearly.

Or. en

Amendment 555
Alfred Sant

Proposal for a regulation
Article 22 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, on the basis of guidelines already developed and implemented by the ESAs and national competent authorities in their respective areas of competence, as well as new and updated guidelines developed after the entry into force of this Regulation.

Or. en

Amendment 556
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 22 – paragraph 1

*Text proposed by the Commission*

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, scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.

*Amendment*

1. The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, *according to a risk-based approach, which may include* vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.

Or. en

**Amendment 557**
Bogdan Rzońca

Proposal for a regulation
Article 23 – paragraph 2 – introductory part

*Text proposed by the Commission*

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.

*Amendment*

2. Threat led penetration testing shall cover at least the critical or important functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities. *Numerous tests may be required to cover all of the critical functions and services of financial entities.*

Or. en

**Amendment 558**
Markus Ferber

Proposal for a regulation
Article 23 – paragraph 2 – introductory part

Text proposed by the Commission

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.

Amendment

2. Threat led penetration testing shall cover 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.

Or. en

Amendment 559
Bogdan Rzońca

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 2

Text proposed by the Commission

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.

Amendment

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.

Where the involvement of an ICT third-party service provider in the threat led penetration testing could have an impact on the quality, confidentiality or security of the provision of the ICT third-party service provider's services to other customers that do not fall within the scope of this Regulation or on the overall integrity of the ICT third-party service provider's operations, the financial entity and the ICT third-party service provider may contractually agree that the ICT third party service provider is permitted to directly enter into contractual arrangements with an external tester to
conduct pooled testing for its financial entity customers.

Amendment 560
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 2

Text proposed by the Commission
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.

Amendment
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. Participation means that ICT third-party service providers shall conduct separate TLPT or join with the financial entity in the financial entity's TLPT. Those ICT third-party service providers shall not be required to communicate information or provide any details in relation to items which are not relevant to the risk management controls of the relevant critical or important services of the relevant financial entities.

Amendment 561
Mikuláš Peksa on behalf of the Greens/EFA Group

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 2

Text proposed by the Commission
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.

Amendment
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. Such
testing shall not adversely impact other users of the ICT third-party service providers.

Amendment 562
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 2

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Where <strong>critical</strong> 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.</td>
</tr>
</tbody>
</table>

Amendment 563
Bogdan Rzońca

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 3

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial entities shall apply effective risk management controls to <strong>reduce</strong> 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.</td>
<td>Financial entities shall apply effective risk management controls to <strong>mitigate</strong> the risks of any potential impact to data, damage to assets and disruption to critical <strong>or important</strong> services or operations at the financial entity itself, its counterparties or to the financial sector.</td>
</tr>
</tbody>
</table>

Amendment 564
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 4

Text proposed by the Commission

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.

Amendment

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 or, in the case of ICT third-party service providers entering into contractual arrangements with external testers directly, to the Lead Overseers, a confidential summary of the test results and the documentation confirming that the threat led penetration testing has been conducted in accordance with the requirements. Competent authorities shall issue an attestation confirming that the test was performed in accordance with the requirements based on the documentation in order to allow for mutual recognition of threat led penetration tests between competent authorities.

Or. en

Justification

TLPT can reveal sensitive information, their details and techniques should thus not be widely disclosed. For the sake of cross-border seamlessness, tests should also be mutually recognised by competent authorities.

Amendment 565
Bogdan Rzońca

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 4

Text proposed by the Commission

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.

Amendment

At the end of the test, after reports and remediation plans have been agreed, the financial entity with the support of the external testers shall provide to the competent authority the documentation required to confirm that the threat led penetration testing has been conducted in accordance with the requirements. Competent authorities may request further details concerning the outcome of the test.
and any risk discovered, and shall validate the documentation and issue an attestation at the end of the process.

Or. en

Amendment 566
Frances Fitzgerald

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 4 a (new)

Text proposed by the Commission

Amendment

Competent authorities shall issue an attestation confirming, based on the documentation referred to in the fifth subparagraph, that the test was performed in accordance with the requirements in order to allow - where applicable - for mutual recognition of threat led penetration tests between competent authorities.

Without prejudice to such attestation, financial entities shall remain at all times fully responsible for the impacts of the tests referred to in this paragraph.

Or. en

Amendment 567
Alfred Sant

Proposal for a regulation
Article 23 – paragraph 3 – introductory part

Text proposed by the Commission

Amendment

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

3. Financial entities shall either contract testers in accordance with Article 24 or use internal testing teams, provided they operate at arms' length and are independent from the rest of the financial entity, for the purposes of undertaking threat led penetration testing.
Amendment 568
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 23 – paragraph 3 – introductory part

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

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

Amendment 569
Alfred Sant

Proposal for a regulation
Article 23 – paragraph 3 – subparagraph 1 – introductory part

**Text proposed by the Commission**
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:

**Amendment**
*Without prejudice to their ability to delegate tasks and competences under this Article to one other competent authority, or more, in charge of 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:

Amendment 570
Markus Ferber

Proposal for a regulation
Article 23 – paragraph 3 – subparagraph 1 – introductory part
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:

Amendment 571
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Article 23 – paragraph 4 – introductory part

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:

Amendment 572
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 23 – paragraph 4 – introductory part

4. **The ESAs** shall, after consulting the ECB, **ENISA and the national supervisory authorities**, and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further:

4. The ESAs shall, in coordination with ENISA and after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop one set of draft regulatory technical standards to specify further:
Amendment 573
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 23 – paragraph 4 – introductory part

Text proposed by the Commission

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:

Amendment

4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to threat led penetration tests, including the TIBER-EU framework, develop draft regulatory technical standards to specify further:

Amendment 574
Bogdan Rzońca

Proposal for a regulation
Article 23 – paragraph 4 – introductory part

Text proposed by the Commission

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:

Amendment

4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to threat led penetration tests, develop draft regulatory technical standards to specify further:

Amendment 575
Alfred Sant

Proposal for a regulation
Article 23 – paragraph 4 – introductory part

Text proposed by the Commission

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:

Amendment
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:

Amendment 576
Alfred Sant, Jonás Fernández, Carmen Avram, Niels Fuglsang

Proposal for a regulation
Article 23 – paragraph 4 – point c

Text proposed by the Commission
(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.

Amendment
(c) the type of supervisory cooperation needed for the implementation and to facilitate full mutual recognition 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.

Amendment 577
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 23 – paragraph 4 – subparagraph 1

Text proposed by the Commission
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].

Amendment
The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 6 months before the date of entry into force].
**Amendment 578**
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 23 – paragraph 4 – subparagraph 1 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Until the entry into force of this Regulation, and the development and adoption of regulatory technical standards specified in Article 23 (4), financial entities shall follow those relevant guidelines and frameworks in the Union which apply to intelligence-based penetration tests, as these will continue to apply when this Regulation comes into force.</td>
<td></td>
</tr>
</tbody>
</table>

**Amendment 579**
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 23 – paragraph 4 a (new)

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 a. Results of threat led penetration testing, including those performed under the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), shall be mutually recognized within the Union among competent authorities.</td>
<td></td>
</tr>
</tbody>
</table>

**Amendment 580**
Jonás Fernández, Niels Fuglsang
Proposal for a regulation
Article 24 – title

Text proposed by the Commission

24 Requirements for testers

Amendment

24 Requirements for external testers

Or. en

Amendment 581
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 24 – paragraph 1 – point c

Text proposed by the Commission

(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;

Amendment

(c) are certified by an accreditation body in a Member State or are certified by a well-established accreditation body in a third country or adhere to formal codes of conduct or ethical frameworks;

Or. en

Justification

This amendment ensures EU financial entities can make use of the best technology available globally in a reasonable manner.

Amendment 582
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 24 – paragraph 1 – point d

Text proposed by the Commission

(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;

Amendment

(d) are independent and 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;
Amendment 583
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 24 – paragraph 1 – point e

Text proposed by the Commission

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

Amendment

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

Amendment 584
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 25 – paragraph 1 – point 2 – point a

Text proposed by the Commission

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

Amendment

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

Amendment 585
Bogdan Rzońca

Proposal for a regulation
Article 25 – paragraph 1 – point 2 – point b a (new)

Text proposed by the Commission

(b a) whether a provider of ICT services is an ICT intra-group service provider.

Amendment

(b a) whether a provider of ICT services is an ICT intra-group service provider.
Amendment 586
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 25 – paragraph 1 – point 3

Text proposed by the Commission

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.

Amendment

3. As part of their ICT risk
management framework, financial entities,
other than microenterprises, shall adopt
and regularly review a strategy on ICT
third-party risk. 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.

Or. en

Amendment 587
Markus Ferber

Proposal for a regulation
Article 25 – paragraph 1 – point 3

Text proposed by the Commission

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.

Amendment

3. As part of their ICT risk
management framework, financial entities
shall adopt and regularly review a strategy
on ICT third-party risk. 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.
functions.

Amendment 588
Bogdan Rzońca

Proposal for a regulation
Article 25 – paragraph 1 – point 3

Text proposed by the Commission

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.

Amendment

3. As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk. 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.

Amendment 589
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 25 – paragraph 1 – point 4 – introductory part

Text proposed by the Commission

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.

Amendment

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. **Where available,**
financial entities shall follow the guidelines and other measures issued by the ESAs and competent authorities until the entry into force of the implementing technical standards referred in Article 25(10). Where relevant, the register of information may be constituted by records pursuant to Article 30 of Regulation (EU) 2016/79.

Or. en

Justification

Alignment with the records of processing activity under GDPR.

Amendment 590
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 25 – paragraph 1 – point 6

Text proposed by the Commission

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.

Amendment

6. Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with high security standards. The latest information standards shall also be considered when determining whether the information standards in place are appropriate.

Or. en

Justification

Many organisations have legacy systems in relation to which it will not be possible to implement the latest information standards and it may not in fact be appropriate to always do so. The new proposed wording is also moving towards the GDPR concept of “appropriate technical and organisational measures”.

Amendment 591
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 25 – paragraph 1 – point 7 – introductory part

Text proposed by the Commission  

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.

Amendment

7. In exercising access, inspection and audit rights over the ICT third-party service provider in relation to critical or important functions, 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.

Or. en

Amendment 592
Bogdan Rzońca

Proposal for a regulation
Article 25 – paragraph 1 – point 7 – paragraph 1

Text proposed by the Commission  

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.

Amendment

For contractual arrangements that entail a detailed 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.

Or. en

Amendment 593
Engin Eroğlu

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – introductory part

Text proposed by the Commission  

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under

Amendment

8. Financial entities shall take appropriate measures such as corrective or remedial actions or termination of
the following circumstances: outsourcing agreements if they identify any of the following circumstances:

Or. en

**Justification**

This article is not easily applicable as it questions the ability of financial entities to impose these requirements on third-party providers, particularly regarding the contract termination. The conditions for termination are too strict, without the possibility of corrective action by the third-party ICT within an acceptable period (like in the example of Article 105 of the EBA Guidelines on Outsourcing).

**Amendment 594**

Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation

Article 25 – paragraph 1 – point 8 – introductory part

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:</td>
<td>8. Financial entities shall take appropriate corrective or remedial measures, which could include terminating the contractual arrangements as a measure of last resort, in cases where at least any of the following circumstances are identified:</td>
</tr>
</tbody>
</table>

Or. en

**Amendment 595**

Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation

Article 25 – paragraph 1 – point 8 – introductory part

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:</td>
<td>8. Financial entities shall ensure that contractual arrangements on the use of ICT services allow the financial entity to terminate the arrangement under applicable law, after all other remedies have been exhausted, at least under the</td>
</tr>
</tbody>
</table>
following circumstances:

Justification

Replacing Amendment 74 to give financial entities more discretion over their ability to terminate.

Amendment 596
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – introductory part

Text proposed by the Commission
Amendment

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:

8. Financial entities shall ensure that contractual arrangements on the use of ICT services may be wholly terminated, if no rectification is possible, and partially terminated, if a rectification is possible, at least under the following circumstances:

Amendment 597
Markus Ferber

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – introductory part

Text proposed by the Commission
Amendment

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:

8. Financial entities shall ensure that contractual arrangements on the use of ICT services can be terminated as a matter of last resort at least under the following circumstances:

Amendment 598
Bogdan Rzońca
Proposal for a regulation  
Article 25 – paragraph 1 – point 8 – introductory part

**Text proposed by the Commission**

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are terminated at least under the following circumstances:

**Amendment**

8. Financial entities shall ensure that contractual arrangements on the use of ICT services are **able to be** terminated, **after all other remedies have been exhausted and after issuing a prior warning**, at least under the following circumstances:

Or. en

Amendment 599
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation  
Article 25 – paragraph 1 – point 8 – point a

**Text proposed by the Commission**

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

**Amendment**

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

Or. en

Amendment 600
Bogdan Rzońca

Proposal for a regulation  
Article 25 – paragraph 1 – point 8 – point a

**Text proposed by the Commission**

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

**Amendment**

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

Or. en

Amendment 601
Alfred Sant

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – point c

Text proposed by the Commission
(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;

Amendment
(c) ICT third-party service provider’s evidenced weaknesses pertaining to its overall ICT risk management of its contract with the financial entity and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information;

Or. en

Amendment 602
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – point d

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

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

Or. en

Amendment 603
Gunnar Beck, Maximilian Krah, Jörg Meuthen, France Jamet

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – point d a (new)

Text proposed by the Commission
(d a) ICT third-party service provider becomes or is suspected of becoming at least partially owned or controlled by foreign governments or foreign militaries;

Amendment
(d a) ICT third-party service provider becomes or is suspected of becoming at least partially owned or controlled by foreign governments or foreign militaries;
Amendment 604
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 25 – paragraph 1 – point 8 a (new)

Text proposed by the Commission

8 a. With a view to reducing the risk of disruptions at the level of the financial entity, in duly justified circumstances and in agreement with their competent authorities, financial entities may not terminate the contractual arrangement with the ICT third-party service provider until they are able to switch to another ICT third-party service provider or change to on-premises solutions consistent with the complexity of the service provided, in accordance with the exit strategy referred to in paragraph 9.

Amendment

Or. en

Amendment 605
Bogdan Rzońca

Proposal for a regulation
Article 25 – paragraph 1 – point 8 a (new)

Text proposed by the Commission

8 a. Financial entities shall not bear the cost of transferring out data from an ICT third-party service provider in cases where a contract is terminated under any of the circumstances listed in points (a) to (d) of point 8.

Amendment

Or. en
Amendment 606
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 25 – paragraph 1 – point 9 – introductory part

Text proposed by the Commission

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.

Amendment

9. For ICT services related to critical or important functions, 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.

Or. en

Amendment 607
Bogdan Rzońca

Proposal for a regulation
Article 25 – paragraph 1 – point 9 – introductory part

Text proposed by the Commission

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.

Amendment

9. For critical and important functions, 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.

Or. en
Amendment 608
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 25 – paragraph 1 – point 9 – introductory part

Text proposed by the Commission

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.

Amendment

9. Financial entities shall put in place exit strategies, to be reviewed periodically, 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.

Or. en

Amendment 609
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 25 – paragraph 1 – point 11 – paragraph 1

Text proposed by the Commission

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].

Amendment

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

Or. en

Amendment 610
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 25 – paragraph 1 – point 11 a (new)

Text proposed by the Commission

11 a. The rules of this Regulation

Amendment
concerning ICT services shall apply without prejudice to the right of financial entities to use decentralised cryptographic solutions, or to form consortia in order to deploy or use such solutions, in which case such ICT services shall not be subject to this Chapter.

Amendment 611
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 26 – title

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements</td>
<td>Preliminary assessment of ICT concentration risk and further sub-contracting arrangements</td>
</tr>
</tbody>
</table>

Amendment 612
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 26 – paragraph 1 – introductory part

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
<td>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 concerning critical or important functions would lead to any of the following:</td>
</tr>
</tbody>
</table>

Amendment 613
Amendment 614
Bogdan Rzońca

Proposal for a regulation
Article 26 – paragraph 1 – point b

Text proposed by the Commission

(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.

Amendment

(b) having in place multiple contractual arrangements in relation to the provision of ICT services concerning critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.

Or. en

Amendment 615
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 26 – paragraph 2 – introductory part

Text proposed by the Commission

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

Amendment

2. Where the contractual arrangement on the use of ICT services concerning critical or important functions includes the possibility that an ICT third-party
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.

Amendment 616
Alfred Sant

Proposal for a regulation
Article 26 – paragraph 2 – introductory part

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.

Amendment

Where contractual arrangements on the use of ICT services concerning critical or important functions 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.

Amendment 617
Alfred Sant

Proposal for a regulation
Article 26 – paragraph 2 – subparagraph 1 – introductory part

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

Amendment

Where contractual arrangements on the use of ICT services concerning critical or important functions are concluded with an ICT third-party service provider established in a third-country, financial
factors: entities shall consider relevant, at least the following factors:

Amendment 618
Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni

Proposal for a regulation
Article 26 – paragraph 2 – subparagraph 1 a (new)

Text proposed by the Commission

With regard to the respect of data protection referred to point (a), financial entities shall comply with the requirement of Chater V of Regulation (EU) 2016/679, as interpreted in the case-law of the Court of Justice of the European Union.

Justification

From the Opinion of the EDPS (European Data Protection Supervisor)

Amendment 619
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 1

Text proposed by the Commission

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.

Amendment

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 writing and be available to the parties on paper or in a downloadable and accessible format.
Justification

Technology contracts often incorporate multiple documents by reference and links so that amendments, renewals and/or statements of work are made in separate documents. Obliging the contract to consist in one single written document could be impractical.

Amendment 620
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 2 – introductory part

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. <em>The</em> contractual arrangements on the use of ICT services shall include at least the following:</td>
<td>2. <em>Financial entities and ICT third party providers shall ensure that</em> contractual arrangements on the use of ICT services shall include at least the following:</td>
</tr>
</tbody>
</table>

Or. en

Justification

The burden of implementing European regulations must not rely solely on one party.

Amendment 621
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 27 – paragraph 2 – introductory part

<table>
<thead>
<tr>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. The contractual arrangements on the use of ICT services shall include at least the following:</td>
<td>2. The contractual arrangements on the use of ICT services <em>concerning critical or important functions</em> shall include at least the following:</td>
</tr>
</tbody>
</table>

Or. en

Amendment 622
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 2 – introductory part

Text proposed by the Commission

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

Amendment

2. The contractual arrangements on the use of ICT services concerning critical and important functions shall include at least the following:

Or. en

Amendment 623
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 27 – paragraph 2 – point b

Text proposed by the Commission

(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;

Amendment

(b) the location(s), namely the regions or countries, where the contracted or sub-contracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify in advance the financial entity if it envisages changing

Or. en

Amendment 624
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 2 – point b

Text proposed by the Commission

(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;

Amendment

(b) the location(s), namely the regions or countries, where the contracted or sub-contracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify in advance the financial entity if it envisages changing
such location(s).

Or. en

Amendment 625
Bogdan Rzońca

Proposal for a regulation
Article 27 – paragraph 2 – point b

Text proposed by the Commission

(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;

Amendment

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

Or. en

Amendment 626
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 27 – paragraph 2 – point c

Text proposed by the Commission

(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;

Amendment

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

Or. en
Amendment 627
Bogdan Rzońca

Proposal for a regulation
Article 27 – paragraph 2 – point d

*Text proposed by the Commission*

(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;

*Amendment*

(d) full service level descriptions, *if considered to be necessary by the financial entity*, 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;

Or. en

Amendment 628
Bogdan Rzońca

Proposal for a regulation
Article 27 – paragraph 2 – point e

*Text proposed by the Commission*

(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;

*Amendment*

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

Or. en

Amendment 629
Bogdan Rzońca

Proposal for a regulation
Article 27 – paragraph 2 – point g
Text proposed by the Commission

(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;

(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 provide an appropriate level of secure provision of services by the financial entity in line with its regulatory framework;

Or. en

Amendment 630
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 27 – paragraph 2 – point h – point i

Text proposed by the Commission

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;

Amendment

i) rights of access, inspection and audit by the financial entity or by an appointed third-party, in relation to the use of ICT services provided by the ICT third-party service provider concerning critical or important functions, and the right of access of relevant documentation in a way which does not compromise the security of the providers and its customers, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

Or. en

Amendment 631
Bogdan Rzońca
Proposal for a regulation
Article 27 – paragraph 2 – point h – point i

Text proposed by the Commission

i) rights of access, inspection and

Amendment

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;

audit by the financial entity or by an appointed third-party, and the right to *review* copies of relevant documentation *on-site if they are critical to the operations of the ICT third-party service provider*, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

Or. en

Amendment 632
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 27 – paragraph 2 – point h – point i

**Text proposed by the Commission**

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;

**Amendment**

i) *unrestricted* rights of access, inspection and audit by the competent authority, 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;

Or. en

Amendment 633
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 27 – paragraph 2 – point h – point i a (new)

**Text proposed by the Commission**

i a) the obligation to allow competent authorities to have access to all contractual arrangements;

**Amendment**

i a) the obligation to allow competent authorities to have access to all contractual arrangements;

Or. en
Amendment 634
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 27 – paragraph 2 – point h – point iii

Text proposed by the Commission

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;

Amendment

iii) the commitment to fully cooperate during the onsite inspections and audits performed by the competent authority, financial entity or by an appointed third party and details on the scope, modalities and frequency of such inspections and audits;

Or. en

Amendment 635
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 27 – paragraph 2 – point j

Text proposed by the Commission

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

Amendment

(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities’ expectations; where that consideration impacts an ICT intra-group third-party service provider within the same group, it shall be analysed following a risk-based approach;

Or. en

Amendment 636
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 27 – paragraph 2 – point j

Text proposed by the Commission

Amendment

AM\1232471EN.docx 229/294 PE693.603v01-00
(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities’ expectations;  
(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities’ and resolution authorities’ expectations;

Amendment 637
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 2 – point j

Text proposed by the Commission  
Amendment

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

Or. en

Amendment 638
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 27 – paragraph 2 – point k – introductory part

Text proposed by the Commission  
Amendment

(k) exit strategies, in particular the establishment of a mandatory adequate transition period:

(k) exit strategies, in particular the establishment of a mandatory adequate transition period - where that consideration impacts an ICT intra-group third-party service provider within the same group, it shall be analysed following a risk-based approach:

Or. en

Amendment 639
Alfred Sant
Proposal for a regulation
Article 27 – paragraph 2 – point k – point i

Text proposed by the Commission

(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;

Amendment

(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 or to ensure its effective resolution and restructuring;

Or. en

Amendment 640
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 27 – paragraph 2 – point k – point i

Text proposed by the Commission

(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;

Amendment

(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 or to ensure its effective resolution and restructuring;

Or. en

Amendment 641
Alfred Sant

Proposal for a regulation
Article 27 – paragraph 2 – point k a (new)

Text proposed by the Commission

(k a) the processing of personal data by the ICT-third party service provider is in conformity with Regulation (EU) 2016/679;

Amendment

(k a) the processing of personal data by the ICT-third party service provider is in conformity with Regulation (EU) 2016/679;
Amendment 642
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 27 – paragraph 2 a (new)

Text proposed by the Commission

2 a. The contractual arrangements for the provision of ICT services by an ICT third-party service provider established in a third country and designated as critical pursuant to Article 28(9), shall, in addition to the provisions set out in paragraphs 2 and 2a of this Article:

(a) be concluded with a legal entity in the Union of that ICT third-party service provider; and

(b) guarantee that the Joint Oversight Executive Body can carry out its duties specified in Article 30 on the basis of its competences set out in Article 31.

The services for which the contractual arrangements are concluded shall not be required to be performed by the legal entity located in the Union.

Justification

replacing Amendment 87 of the draft report to specify that only contractual arrangements with third-country TTPs deemed critical need to be concluded with a legal entity in the EU. Such a requirement does not extend to all third-country TTPs.

Amendment 643
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 27 – paragraph 2 a (new)

Text proposed by the Commission

Amendment
2 a. Competent authorities shall be able to access the contractual arrangements.

Amendment 644
Bogdan Rzońca

Proposal for a regulation
Article 27 – paragraph 3

Text proposed by the Commission

Amendment

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 and refrain from supplementing them in the areas set out in this Regulation or further detailed by the ESAs referred to in paragraph 4.

Amendment 645
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 27 – paragraph 4 – introductory part

Text proposed by the Commission

Amendment

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.

When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, complexity and overall risk profile of the financial
Amendment 646
Markus Ferber

Proposal for a regulation
Article 27 – paragraph 4 – introductory part

Text proposed by the Commission

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.

Amendment

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. When devising those standards, the ESAs shall take into consideration the nature, size and complexity of the financial entities concerned.

Amendment 647
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 27 – paragraph 4 – subparagraph 1

Text proposed by the Commission

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].

Amendment

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

Amendment 648
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 28 – paragraph 1 – introductory part

Text proposed by the Commission  
Amendment

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

   1. The Joint Oversight Body established pursuant to Article 29(1), after consultation with the ENISA, shall:

   Or. en

Justification

The Joint Oversight Body composed by the ESAs Executive Directors shall be the single supervisor on the CTTP with direct executive powers. It should be assisted by joint examination teams.

Amendment 649
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 28 – paragraph 1 – point a a (new)

Text proposed by the Commission  
Amendment

(a a) be responsible for the supervision and oversight of critical ICT third-party service providers in relation to the services they provide to financial entities.

Or. en

Amendment 650
Frances Fitzgerald, Isabel Benjumea Benjumea
Proposal for a regulation
Article 28 – paragraph 1 – point b

Text proposed by the Commission  
Amendment

(b) appoint either EBA, ESMA or EIOPA as Lead Overseer for each critical ICT third-party service provider, deleted

AM\1232471EN.docx  235/294  PE693.603v01-00
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.

Amendment 651
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 28 – paragraph 1 – point b

Text proposed by the Commission
(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.

Amendment
(b) adopt decisions addressed to critical ICT third-party service providers.
Proposal for a regulation

Article 28 – paragraph 1 – point b

Text proposed by the Commission

(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.

Amendment

(b) appoint either EBA, ESMA or EIOPA, on a rotational basis, to be rotated following the annual publication of the list referred to in paragraph 6, as having the responsibility to adopt formal decisions and recommendations addressed to critical ICT third-party service providers, on the basis of draft decisions and recommendations from the Joint Oversight Executive Body.

Justification

Replacing amendment 90.

Proposal for a regulation

Article 28 – paragraph 2 – introductory part

Text proposed by the Commission

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

Amendment

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

-a) on the basis of a structured risk-based approach which takes into account both
the provider and the nature of the service it provides;

Or. en

Amendment 654
Markus Ferber

Proposal for a regulation
Article 28 – paragraph 2 – point a a (new)

Text proposed by the Commission

Amendment

(a a) the services provided constitute a function within the meaning of Article 3(17) of this Regulation.

Or. en

Justification

A provider should only be designated as critical if they perform critical functions as defined in this regulation.

Amendment 655
José Gusmão

Proposal for a regulation
Article 28 – paragraph 2 – point b – introductory part

Text proposed by the Commission

Amendment

(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the Basel Committee on Banking Supervision’s standard number 239\(^{1a}\) and the following parameters:

\(^{1a}\) https://www.bis.org/publ/bcbs239.pdf

Or. en
Amendment 656
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 28 – paragraph 2 – point e

Text proposed by the Commission  
Amendment

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

Or. en

Amendment 657
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 28 – paragraph 2 – point f

Text proposed by the Commission  
Amendment

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

Or. en

Amendment 658
Alfred Sant

Proposal for a regulation
Article 28 – paragraph 2 – point f a (new)

Text proposed by the Commission  
Amendment

(f a) the materiality and importance of the relevant service provided by the ICT third-party service provider.

Or. en

Amendment 659
<table>
<thead>
<tr>
<th>Amendment</th>
<th>Author(s)</th>
<th>Proposal for a regulation</th>
<th>Article 28 – paragraph 2 a (new)</th>
<th>Text proposed by the Commission</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>660</td>
<td>Antonio Maria Rinaldi, Francesca Donato, Valentino Grant, Marco Zanni</td>
<td>Proposal for a regulation</td>
<td>Article 28 – paragraph 2 a (new)</td>
<td>Text proposed by the Commission</td>
<td>Amendment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 a. The designation shall not apply in relation to intragroup ICT third-party service providers.</td>
<td>Or. en</td>
</tr>
<tr>
<td>661</td>
<td>Bogdan Rzońca</td>
<td>Proposal for a regulation</td>
<td>Article 28 – paragraph 2 b (new)</td>
<td>Text proposed by the Commission</td>
<td>Amendment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 b. The ICT third-party service provider may, within 90 calendar days of receipt of the notification referred to in paragraph 2a, provide additional information to the Lead Overseer that is considered to be relevant to the designation referred to in point (a) of paragraph 1 and to its outcome.</td>
<td>Or. en</td>
</tr>
</tbody>
</table>
Amendment 662
Bogdan Rzońca

Proposal for a regulation
Article 28 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. The Lead Overseer shall notify the ICT third-party service provider before initiating its assessment for the purposes of the designation referred to in point (a) of paragraph 1.

Amendment 663
Bogdan Rzońca

Proposal for a regulation
Article 28 – paragraph 2 c (new)

Text proposed by the Commission

Amendment

2 c. The Lead Overseer shall make public the reason for the designation referred to in point (a) of paragraph 1 unless to do so could have a harmful impact on the designated ICT third-party service provider or on another entity subject to this Regulation.

Amendment 664
Bogdan Rzońca

Proposal for a regulation
Article 28 – paragraph 2 d (new)

Text proposed by the Commission

Amendment
2 d. Upon receipt of the draft recommendation, the ICT third-party service provider shall have a period of six weeks within which to review and comment on it, and shall communicate if an additional period of time is needed in order to make necessary adjustments as set out in this Article.

Or. en

Amendment 665
Bogdan Rzońca

Proposal for a regulation
Article 28 – paragraph 2 e (new)

*Text proposed by the Commission*

2 e. The ESAs shall notify the ICT third-party service provider of its designation as critical. The ICT third party service provider shall have at least three months to make any necessary adjustments to allow the Joint Oversight Executive Body to carry out its duties pursuant to Article 29, as well as to notify its financial entity customers. The Joint Oversight Executive Body may allow the adjustment period to be extended for a minimum period of three months, if requested by the designated ICT third-party service provider and duly justified.

Or. en

Amendment 666
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 28 – paragraph 3

*Text proposed by the Commission*

3. The Commission is empowered to adopt delegated *acts* in accordance with

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

Article 50 to **specify further** the criteria referred to in paragraph 2 by [OJ: insert date 12 months after the date of entry into force].

Or. en

**Amendment 667**  
Markus Ferber

Proposal for a regulation  
**Article 28 – paragraph 3**

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

*Amendment*  
3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement the criteria referred to in paragraph 2. **The Commission shall adopt such a delegated act within 12 months from the date of entry into force of this Regulation.**

Or. en

*Justification*

For legal certainty, a clear deadline should be specified.

**Amendment 668**  
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation  
**Article 28 – paragraph 5 a (new)**

*Text proposed by the Commission*  
5 a. The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment referred in paragraph 2 by providing a draft recommendation of criticality. Within 45 calendar days from the date of that notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement on the assessment

*Amendment*  
5 a. The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment referred in paragraph 2 by providing a draft recommendation of criticality. Within 45 calendar days from the date of that notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement on the assessment
which shall contain all relevant additional information deemed to be appropriate by the ICT third-party service provider in order to support the completeness and accuracy of the designation procedure or to challenge the draft recommendation of criticality. Prior to taking a decision on the criticality designation, the Lead Overseer shall take due consideration of the reasoned statement and may request further information or evidence from the ICT third-party service provider.

Amendment 669
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 28 – paragraph 6

Text proposed by the Commission

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.

Amendment

6. The Joint Oversight Body, in consultation with ENISA, shall establish, publish and yearly update the list of critical ICT third-party service providers at Union level.

Amendment 670
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 28 – paragraph 8 – subparagraph 1

Text proposed by the Commission

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

Amendment

For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to the **Lead Overseer**, which, through the Joint Committee, shall decide whether to include that ICT third-party service provider in that
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.

Justification

Such a determination is hard to make when it concerns third-party entities.

9. Financial entities shall not make use, for critical or important functions, of an ICT third-party service provider established in a third country unless it has established a legal entity in the Union and has entered into a contractual arrangement with a financial entity for the provision of ICT services.
Amendment 673
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel

Proposal for a regulation
Article 28 – paragraph 9

Text proposed by the Commission

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.

Amendment

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 that ICT third-party service provider has a subsidiary in the Union.

Or. en

Amendment 674
Bogdan Rzońca

Proposal for a regulation
Article 28 – paragraph 9

Text proposed by the Commission

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.

Amendment

9. Financial entities shall not make use of an ICT third-party service provider established in a third country that is designated as critical pursuant to point (a) of paragraph 1 and does not have legal representation in the Union.

Or. en

Amendment 675
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 28 – paragraph 9

Text proposed by the Commission

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.

Amendment

9. Financial entities shall refrain from using an ICT third-party service provider established in a third country designated as
designated as critical pursuant to point (a) of paragraph 1 \textit{if it were established} in the Union.

critical pursuant to point (a) of paragraph 1 \textit{does not establish a subsidiary} in the Union.

Amendment 676
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 28 – paragraph 9 a (new)

\textit{Text proposed by the Commission}

\textit{Amendment}

9 a. \textit{Financial entities shall not make use of an ICT third-party established in a third country if that third party has, or is suspected of having, ties with foreign governments or foreign militaries.}

Amendment 677
Markus Ferber

Proposal for a regulation
Article 28 – paragraph 9 a (new)

\textit{Text proposed by the Commission}

\textit{Amendment}

9 a. \textit{ICT service providers that are part of the same group of financial entities shall not be classified as critical ICT third-party service providers.}

Amendment 678
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 28 a (new)
Article 28a

Minimum requirements for critical ICT third-party providers

1. Critical ICT third-party providers shall have in place internal governance and control frameworks that ensure an effective and prudent management of all operational risks linked directly or indirectly to the services provided to financial entities.

2. Critical ICT third-party providers shall have an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling an effective ICT risk management of all ICT risks linked directly or indirectly to the services provided to financial entities.

3. The management body of the critical ICT third-party providers shall define, approve, oversee and be accountable for the implementation of all arrangements related to the operational risk management framework of all operational risks linked directly or indirectly to the services provided to financial entities.

4. Critical ICT third-party providers shall have a sound, comprehensive, up-to-date and well-documented operational risk management framework to address operational risk linked directly or indirectly to the services provided to financial entities quickly, efficiently and comprehensively and to ensure a maximal level of operational resilience.

5. Critical ICT third-party providers shall continually monitor and effectively identify operational risks and anomalies linked directly or indirectly to the services provided to financial entities.

6. Critical ICT third-party providers shall effectively manage and resolve all anomalies and incidents linked directly or indirectly to the services provided to financial entities, in particular cyber-
attacks.

7. Critical ICT third-party providers shall ensure that regular and thorough ICT audits of the services provided to financial entities are conducted.

8. Critical ICT third-party providers shall use reliable and resilient ICT systems, protocols and tools (including premises, facilities and data centres) to provide their services to financial entities. Those ICT systems, protocols and tools shall:
   a. guarantee data security, integrity, confidentiality and continuity; and service availability, scalability and quality;
   b. have sufficient capacity to maintain performance through peaks in usage;
   c. minimise the impact of operational risks.

9. Critical ICT third-party providers shall maintain robust mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities.

10. Critical ICT third-party providers shall use and maintain updated and state-of-the-art ICT systems, protocols and tools to provide their services to financial entities.

11. Critical ICT third-party providers shall ensure that any contracting arrangements they enter into with other ICT service providers do not create risks for the provision of services to financial entities or risks to financial stability. Critical ICT third-party providers should ensure that the Joint Oversight Body is able to obtain promptly, upon request, access to the relevant information concerning such arrangements.

12. Critical ICT third-party providers shall have in place a dedicated operational business continuity policy to enable them to quickly, appropriately and effectively respond to and resolve operational incidents linked directly or
indirectly to the services provided to financial entities. Critical ICT third-party providers should have in place an associated dedicated disaster recovery plan.

13. To minimise downtime and disruption of the service they provide to financial entities, critical ICT third-party providers shall offer comprehensive, reliable and effective backup and recovery.

14. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the specific minimum requirements applicable to critical ICT third-party service providers.

Amendment 679
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 29 – paragraph 1 – introductory part

Text proposed by the Commission

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.

Amendment

1. The Joint Oversight Body shall be established for the purposes of supporting the work of overseeing ICT third-party risk across financial sectors and conducting direct oversight of ICT third-party service providers designated as critical pursuant to Article 28.

Justification

The Joint Oversight Body should assume the functions assigned in the initial proposal to the
Lead Overseer and the Oversight Forum as well as the competences assigned to the ESAs and competent authorities as regard the oversight of critical third party providers. A single European supervisor with appropriate powers would ensure a more effective and streamlined oversight framework with respect to critical third party service providers. This change applies horizontally to the text.

Amendment 680
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 29 – paragraph 1 – introductory part

Text proposed by the Commission

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.

Amendment

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 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 role of the Oversight Forum shall be limited to supervisory and oversight responsibilities related to ICT risks concerning the ICT services provided by critical ICT third-party service providers to financial entities.

Or. en

Amendment 681
Mikuláš Peksa on behalf of the Greens/EFA Group

Proposal for a regulation
Article 29 – paragraph 4

Text proposed by the Commission

4. The Oversight Forum shall be composed of the Chairpersons of the ESAs, and one high-level representative

Amendment

4. The Joint Oversight Body shall be composed of the Executive Directors of the ESAs, and two independent members
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.

appointed on the basis of merit, skills and knowledge of ICT risks. One representative from the European Commission, from the ESRB, from ECB and from ENISA shall participate in the Joint Oversight Body as observers.

Following each designation of critical ICT third-party service providers pursuant to Article 28(6), the Joint Oversight Body shall decide, in addition to the dedicated staff from the ESAs, which national competent authorities are to be members of the joint examination team, taking into account the following factors:

(a) the number of critical ICT third-party service providers established or providing services in a Member State;

(b) the reliance of the financial entities in a Member State on critical ICT third-party service providers;

(c) the relative expertise, available resources and capacity of a national competent authority.

Amendment 682
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 29 – paragraph 4

Text proposed by the Commission

4. 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.

Amendment

4. The Joint Oversight Executive Body shall be composed of one independent director from EBA, one independent director from EIOPA, one independent director from ESMA, and one high-level representative from at least five of the national competent authorities. 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 Joint Oversight Executive Body as
observers.

Justification

References to the Joint Oversight Executive Body to be aligned throughout the Regulation

Amendment 683
Christophe Hansen

Proposal for a regulation
Article 29 – paragraph 4

Text proposed by the Commission

4. 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.

Amendment

4. The Oversight Forum shall be composed of the Chairpersons of the ESAs, and at least 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.

Or. en

Amendment 684
Stéphanie Yon-Courtin, Gilles Boyer, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 29 – paragraph 4 a (new)

Text proposed by the Commission

4 a. The independent directors from each ESA referred to in paragraph 4 shall be full-time, independent professionals.

They shall be appointed by the respective Board of Supervisors of each ESA on the basis of merit, skills, knowledge and experience relevant to digital operational resilience for the financial sector,

Amendment

4 a. The independent directors from each ESA referred to in paragraph 4 shall be full-time, independent professionals.

They shall be appointed by the respective Board of Supervisors of each ESA on the basis of merit, skills, knowledge and experience relevant to digital operational resilience for the financial sector,
following an open selection procedure.

Before the appointment of independent directors from each ESA, and up to one month after the selection by the Board of Supervisors, which shall submit its shortlist of selected candidates, respecting gender balance, to the European Parliament, the European Parliament, after having heard the selected candidates, shall approve or reject them.

Where an independent director no longer fulfil the conditions required for the performance of his or her duties or has been found guilty of serious misconduct, the Council may, on a proposal from the Commission which has been approved by the European Parliament, adopt an implementing decision to remove the independent director from office. The Council shall act by qualified majority. The European Parliament or the Council may inform the Commission that they consider the conditions for the removal of one of the independent directors to be fulfilled, to which the Commission shall respond.

The term of office of the independent directors shall be five years and may be extended once.

The independent directors shall not hold any office at national, Union, or international level. They shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.

Neither Member States, the Union institutions or bodies, nor any other public or private body shall seek to influence the independent directors in the performance of their tasks.

In accordance with the Staff Regulations referred to in Article 68 of Regulation (EU) No 1093/2010, Article 68 of Regulation (EU) No 1094/2010 and
Article 68 of Regulation (EU) No 1095/2010, the independent directors shall, after leaving service, continue to be bound by the duty to behave with integrity and discretion as regards the acceptance of certain appointments or benefits.

Or. en

Amendment 685
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 29 – paragraph 5

Text proposed by the Commission

5. 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.

Amendment

5. The Commission is empowered to adopt a delegated act in accordance with Article 50 to specify the cooperation modalities between the Joint Oversight Body 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 Joint Oversight Body and details on exchanges of information needed by competent authorities to ensure the follow-up of the decisions adopted by the Joint Oversight Body pursuant to point (d) of Article 31(1) to critical ICT third-party providers.

Or. en

Amendment 686
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 29 – paragraph 5

Text proposed by the Commission


Amendment

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.

Amendment 687
Christophe Hansen, Jessica Polfjärd

Proposal for a regulation
Article 29 – paragraph 5

Text proposed by the Commission

5. 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.

Amendment

5. 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 by [OJ: insert date 18 months after the date of entry into force] 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.

Or. en

Amendment 688
Mikuláš Peksa

PE693.603v01-00 256/294 AM\1232471EN.docx
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 29 – paragraph 7

*Text proposed by the Commission*

7. 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.

*Amendment*

7. The Joint Oversight Body shall present yearly to the European Parliament, the Council and the Commission a report on the application of this Section.

Amendment 689
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 30 – title

*Text proposed by the Commission*

Tasks of the *Lead Overseer*

*Amendment*

Tasks of the *Joint Oversight Body*

Amendment 690
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 30 – paragraph 1

*Text proposed by the Commission*

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.

*Amendment*

1. The *Joint Oversight Body* 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.
Amendment 691
Bogdan Rzońca

Proposal for a regulation
Article 30 – paragraph 2 – point e

Text proposed by the Commission

(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;

Amendment

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

Amendment 692
Bogdan Rzońca

Proposal for a regulation
Article 30 – paragraph 3

Text proposed by the Commission

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.

Amendment

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. Before publication of the Oversight plan, the Lead Overseer shall engage in dialogue with the ICT third-party service provider, specifically for the purpose of exchanging information relevant to the final Oversight plan, including the possibility for the ICT third-party service provider to challenge individual recommendations. That plan shall be communicated each year to the critical ICT third-party service provider.
Amendment 693
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru, Ondřej Kovařík

Proposal for a regulation
Article 30 – paragraph 3 a (new)

Text proposed by the Commission

3 a. When preparing the Oversight plan, the Joint Oversight Executive body shall consult all relevant competent authorities and single points of contact referred to in Article 8 of Directive (EU) 2016/1148 to ensure that there are no inconsistencies or duplications with the critical ICT third-party service provider's obligations under Directive (EU) 2016/1148.

Amendment

3 a. Prior to the finalisation of the oversight plan referred to in paragraph 2, the Lead Overseer shall consult the relevant competent authorities that have jurisdiction under Directive (EU) 2016/1148 to assess if compliance with Directive (EU) 2016/1148 satisfies one or more of the requirements set out in the oversight framework in this section.

Amendment 694
Frances Fitzgerald, Isabel Benjumea Benjumea

Amendment 695
Mikuláš Peksa
on behalf of the Greens/EFA Group
Proposal for a regulation
Article 31 – title

Text proposed by the Commission

Powers of the Lead Overseer

Amendment

Powers and responsibilities of the Joint Oversight Body

Amendment 696
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 31 – paragraph 1 – introductory part

Text proposed by the Commission

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

Amendment

1. For the purposes of carrying out the duties laid down in this Section, the Joint Oversight Body shall have the following powers in respect of the services provided by critical ICT third-party service providers to financial entities:

Amendment 697
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 31 – paragraph 1 – introductory part

Text proposed by the Commission

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

Amendment

1. For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers related to ICT risks concerning the ICT services provided by critical ICT third-party service providers to financial entities:
Amendment 698
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 31 – paragraph 1 – point d – introductory part

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

Amendment
(d) to take decisions on the areas referred to in Article 30(2), in particular concerning the following:

Or. en

Amendment 699
Gunnar Beck, Maximilian Krah, Jörg Meuthen

Proposal for a regulation
Article 31 – paragraph 1 – point d – point iv a (new)

Text proposed by the Commission  
(iv a) refraining from entering into a further subcontracting arrangement, when the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country, if this third-party has or is suspected of having ties to foreign governments or foreign militaries;

Amendment

Or. en

Amendment 700
Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 31 – paragraph 1 – subparagraph 1 (new)

Text proposed by the Commission  
The powers referred to in the first subparagraph shall primarily be used in

Amendment

The powers referred to in the first subparagraph shall primarily be used in
respect of the critical or important services provided by the critical ICT third-party service provider to financial entities, but may also be used in respect of other services provided to financial entities when necessary.

Or. en

Amendment 701
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 31 – paragraph 1 a (new)

Text proposed by the Commission Amendment

1 a. When exercising the powers referred to in paragraph 1, the Lead Overseer shall take due account of the framework established by Directive (EU) 2016/1148, in order to avoid unnecessary duplication of technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that Directive.

Or. en

Amendment 702
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 31 – paragraph 1 a (new)

Text proposed by the Commission Amendment

1 a. When exercising the powers referred to in paragraph 1, the Joint Oversight Body shall coordinate with the relevant national competent authority established by Directive (EU) 2016/1148 to avoid inconsistencies or duplication with rules established under Directive (EU) 2016/1148.
Amendment 703
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 31 – paragraph 2

Text proposed by the Commission

Amendment

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

Or. en

Amendment 704
Billy Kelleher, Engin Eroglu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 31 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. When preparing the recommendations, the Joint Oversight Executive body shall consult all relevant competent authorities and single points of contact referred to in Article 8 of Directive (EU) 2016/1148 to ensure there are no inconsistencies or duplications with the critical ICT third-party service provider's obligations under Directive (EU) 2016/1148

Or. en

Amendment 705
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 31 – paragraph 3 a (new)
3 a. For the purposes of paragraph 1(d), prior to issuing a recommendation, the Lead Overseer shall inform the critical ICT third-party service provider of its intention to issue a recommendation and shall provide an opportunity for the critical ICT third-party service provider to provide information which it reasonably believes should be taken into account before the recommendation is finalised and issued.

Amendment 706
Jonás Fernández, Niels Fuglsang
Proposal for a regulation
Article 31 – paragraph 4

Text proposed by the Commission

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.

Amendment

4. The Lead Overseer shall decide, in the case of full or partial non-compliance with the appropriate measures taken in accordance with points (a), (b) or (c), within 30 calendar days, to 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.

Amendment 707
Alfred Sant
Proposal for a regulation
Article 31 – paragraph 4

Text proposed by the Commission

4. The Lead Overseer may impose a periodic penalty payment to compel the

Amendment

4. The Lead Overseer may, in the case of whole or partial non-compliance
critical ICT third-party service provider to comply with points (a), (b) and (c) of paragraph 1.

with the appropriate measures that would need to be taken in accordance with points (a), (b) or (c) of paragraph 1, within 60 calendar days, decide to 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.

Or. en

Amendment 708
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 31 – paragraph 6

Text proposed by the Commission
Amendment

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.

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 related to services provided to financial entities covered in this regulation of the critical ICT third-party service provider in the preceding business year.

Or. en

Amendment 709
Alfred Sant

Proposal for a regulation
Article 31 – paragraph 7

Text proposed by the Commission
Amendment

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

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. Such penalty payments shall only be imposed as a last resort in the event that the ICT third-party service provider fails to comply despite other reasonable measures being taken.

Amendment 710
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 31 – paragraph 8

Text proposed by the Commission

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.

Amendment

8. The Joint Oversight Body 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.

Amendment 711
Bogdan Rzońca

Proposal for a regulation
Article 32 – paragraph 1

Text proposed by the Commission

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 information concerning ICT services delivered to a financial entity that is necessary for the Lead Overseer to carry...
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.

The Lead Overseer shall not be authorised to request information on any customers of the critical ICT third-party service provider which do not fall within the scope of this Regulation or are not using the ICT third-party service provider for critical or important functions.

Amendment 712
Alfred Sant

Proposal for a regulation
Article 32 – paragraph 1

Text proposed by the Commission

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.

Amendment

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. **ICT third-party service providers shall only be required to provide that information in respect of financial entities subject to this Regulation who use the services for critical or important functions and shall give notice to the relevant financial entity of requests specific to that financial entity.**

Or. en
Amendment 713
Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 32 – paragraph 1

Text proposed by the Commission

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.

Amendment

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. Any contractual clauses between the financial entity and the critical ICT third-party service provider restricting access to information by the Lead Overseer shall be declared null and void.

Or. en

Amendment 714
Bogdan Rzońca

Proposal for a regulation
Article 32 – paragraph 2 – point d

Text proposed by the Commission

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

Amendment

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

Or. en

Amendment 715
Jonás Fernández, Niels Fuglsang
Proposal for a regulation  
Article 32 – paragraph 3 – point e

_text proposed by the Commission_

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

_text proposed by the Commission_

(e) indicate the periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete or when such information is not provided within the time limit established in point (d);

Or. en

Amendment 716  
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation  
Article 32 – paragraph 5

_text proposed by the Commission_

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.

_text proposed by the Commission_

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. That critical ICT third-party service provider shall notify its clients about the Lead Overseer's recommendations.

Or. en

Amendment 717  
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation  
Article 33 – paragraph 2 – point b

_text proposed by the Commission_

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

_text proposed by the Commission_

(b) access, in a secured way, to certified copies of, or extracts from, such records, data, procedures and other material;
Amendment 718
Bogdan Rzońca

Proposal for a regulation
Article 33 – paragraph 2 – point b

*Text proposed by the Commission*

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

*Amendment*

(b) take or obtain certified copies of or review them on-site where they are deemed to be critical to the operations of the ICT third-party service provider, or extract from, such records, data, procedures and other material;

Amendment 719
Bogdan Rzońca

Proposal for a regulation
Article 33 – paragraph 2 – point e

*Text proposed by the Commission*

(e) request records of telephone and data traffic.

*Amendment*

deleted

Amendment 720
Alfred Sant, Carmen Avram

Proposal for a regulation
Article 33 – paragraph 2 – point e

*Text proposed by the Commission*

(e) request records of telephone and data traffic.

*Amendment*

(e) request records of telephone and data traffic, in accordance with the principle of proportionality.
Amendment 721
Bogdan Rzońca

Proposal for a regulation
Article 34 – paragraph 1

Text proposed by the Commission

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.

Amendment

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, which are relevant to the ongoing investigation and financial entity in question, such as head offices, operation centres, secondary premises, as well as to conduct off-line inspections.

Amendment 722
Bogdan Rzońca

Proposal for a regulation
Article 34 – paragraph 2 – introductory part

Text proposed by the Commission

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.

Amendment

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, unless it does not interrupt operations of other ICT third-party service provider customers and books or records for the period of, and to the extent necessary for, the inspection.
Amendment 723  
Isabel Benjumea Benjumea, Frances Fitzgerald  
Proposal for a regulation  
Article 34 – paragraph 2 – introductory part  

**Text proposed by the Commission**

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.

**Amendment**

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, *in a way which does not compromise the security of the provider and its customers.*

Or. en

Amendment 724  
Alfred Sant  
Proposal for a regulation  
Article 34 – paragraph 4  

**Text proposed by the Commission**

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.

**Amendment**

4. Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data *that the Lead Overseer deems appropriate and technologically relevant,* either for, or contributing to, the provision of services to financial entities.

Or. en

Amendment 725  
Alfred Sant  
Proposal for a regulation  
Article 34 – paragraph 5

PE693.603v01-00 272/294 AM\1232471EN.docx
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.

Amendment 726
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 37 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Within 30 calendar days after the receipt of the decisions issued by the Joint Oversight Body pursuant to point (d) of Article 31(1), critical ICT third-party service providers shall notify whether they have complied with the decisions. The Joint Oversight Body shall immediately transmit this information to the competent authorities of the financial entities concerned.

Amendment 727
Billy Kelleher, Engin Eroğlu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru
Proposal for a regulation
Article 37 – paragraph 1

Text proposed by the Commission

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.

Amendment

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

Or. en

Justification

Replacing Amendment 143 of the draft report.

Amendment 728
Alfred Sant

Proposal for a regulation
Article 37 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Within 30 calendar days after the receipt of the recommendations issued by Lead Overseers pursuant to point (d) of Article 31(1), which shall be simultaneously copied to the financial entities serviced by the latter critical ICT third-party service providers shall notify the Lead Overseer whether they intend to follow those critical recommendations. For non-critical recommendations, the time period may be extended by up to 45 days. Lead Overseers shall immediately transmit this information to competent authorities.

Or. en
Amendment 729
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 37 – paragraph 2

Text proposed by the Commission

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).

Amendment

2. Competent authorities shall monitor whether financial entities take into account the risks identified in the decisions addressed to critical ICT third-party providers by the Joint Oversight Body in accordance with points (d) of Article 31(1). The Joint Oversight Body shall monitor whether the critical ICT third-party providers have addressed the risks identified in those decisions.

Or. en

Amendment 730
Billy Kelleher, Engin Eroglu, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 37 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. The ESAs may decide, upon recommendation from the Joint Oversight Executive Body and after consultation with the Competent authorities of the affected financial entities, to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party service providers until those risks have been addressed. Where necessary, they may require the critical ICT third-party service providers to terminate, in part or completely, the relevant contractual arrangements concluded with the financial
entity customers exposed to the identified risks.

Justification

Replacing Amendment 145 to clarify that the decisions regarding suspension are taken by the Board of Supervisors of the ESA currently responsible for such decisions.

Amendment 731
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 37 – paragraph 3

Text proposed by the Commission

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.

Amendment

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

Amendment 732
Bogdan Rzońca

Proposal for a regulation
Article 37 – paragraph 3
3. Competent authorities may, in accordance with Article 44, require financial entities to temporarilysuspend, 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.

Amendment

3. After exhausting all other options and issuing warnings to financial entities as a result of the oversight process, and subject to the approval of the Oversight Forum, 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. Competent authorities shall notify the financial entities concerned as soon as possible and allow them sufficient time, at a minimum 30 business days, to adjust the outsourcing of relevant ICT services on an individual basis.

Or. en

Amendment 733
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 37 – paragraph 3

Text proposed by the Commission

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.

necessary, and as a measure of last resort, they may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.

**Competent authorities shall allow sufficient time to financial entities to adjust their outsourcing and contractual arrangements with critical ICT third-party service providers.**

---

**Amendment 734**

Alfred Sant, Jonás Fernández, Niels Fuglsang

**Proposal for a regulation**

**Article 37 – paragraph 3**

*Text proposed by the Commission*

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.

*Amendment*

3. Competent authorities may, in accordance with Article 44, as a measure of last resort, 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, after considering risks and mitigating measures and following the defined exit strategies put in place by the financial entity. Following the request for termination, the competent authorities shall allow sufficient time for financial entities to adjust their contractual arrangements with ICT third-party service providers in such a way as to not jeopardise digital operational resilience.
Amendment 735  
Markus Ferber

Proposal for a regulation  
Article 37 – paragraph 3

*Text proposed by the Commission*

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.

*Amendment*

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. *Competent authorities shall only require financial entities to perform any of the above actions as a matter of last resort and taking into account the involved risk and the feasibility of exiting the service in question.*

Amendment 736  
Markus Ferber

Proposal for a regulation  
Article 37 – paragraph 3 a (new)

*Text proposed by the Commission*

3 a. Where a competent authority decides to require a financial entity to terminate, in part or completely, relevant contractual arrangements concluded with a critical ICT third-party service provider

*Amendment*

3 a. Where a competent authority decides to require a financial entity to terminate, in part or completely, relevant contractual arrangements concluded with a critical ICT third-party service provider
pursuant to paragraph 3, the competent authority shall inform the financial entity at least 60 days prior to that decision being taken.

Amendment 737
Billy Kelleher, Engin Eroğlu, Ondřej Kovařík, Caroline Nagtegaal, Olivier Chastel, Dragoș Pîslaru

Proposal for a regulation
Article 37 – paragraph 4 – introductory part

Text proposed by the Commission

Amendment

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:

4. When making those recommendations, the Joint Oversight Executive Body 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:

Justification

Replacing Amendment 146.

Amendment 738
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 37 – paragraph 4 – introductory part

Text proposed by the Commission

Amendment

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

4. When taking the decisions referred to in paragraph 3, the Joint Oversight Body 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:

Amendment 739
Alfred Sant, Jonás Fernández, Niels Fuglsang

Proposal for a regulation
Article 37 – paragraph 4 – point d a (new)

Text proposed by the Commission  Amendment

(d a) whether the suspension or termination introduces a discontinuity risk for the business operations of the customer of the critical ICT third-party provider.

Or. en

Amendment 740
Isabel Benjumea Benjumea, Frances Fitzgerald

Proposal for a regulation
Article 37 – paragraph 4 – point d a (new)

Text proposed by the Commission  Amendment

(d a) whether the suspension or termination means a risk for the business operations of the customer of the critical ICT third-party service provider.

Or. en

Amendment 741
Alfred Sant

Proposal for a regulation
Article 40 – paragraph 1 – introductory part

Text proposed by the Commission  Amendment
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:

1. Financial entities shall, whenever possible and deemed appropriate, exchange amongst themselves and ICT third-party service providers 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:

Amendment 742
Alfred Sant

Proposal for a regulation
Article 40 – paragraph 1 – point a

Text proposed by the Commission

(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;

Amendment

(a) aims at enhancing the digital operational resilience of financial entities and ICT third-party service providers, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats’ ability to spread, supporting defensive capabilities, threat detection techniques, mitigation strategies or response and recovery stages;

Amendment 743
Alfred Sant

Proposal for a regulation
Article 40 – paragraph 1 – point b

Text proposed by the Commission

(b) takes places within trusted communities of financial entities;

Amendment

(b) takes places within trusted communities of financial entities and ICT third-party service providers;

Or. en
Amendment 744
Alfred Sant

Proposal for a regulation
Article 40 – paragraph 2

*Text proposed by the Commission*

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.**

*Amendment*

2. **For the purpose of paragraph 1, a database for storing information at Union level shall be created.** 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.

Or. en

Amendment 745
Bogdan Rzońca

Proposal for a regulation
Article 40 – paragraph 3

*Text proposed by the Commission*

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.**

*Amendment*

deleted

3. **delet**

Or. en

Amendment 746
Alfred Sant, Carmen Avram
Proposal for a regulation
Article 40 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. Processing of personal data for the purposes of this Article is in accordance with point (f) of Article 6(1) of Regulation (EU) 2016/679.

Or. en

Justification

Reference to the GDPR for the purposes of cybersecurity information sharing.

Amendment 747
Markus Ferber

Proposal for a regulation
Article 41 – paragraph 1 – point p

Text proposed by the Commission

Amendment

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

deleted

Or. en

Amendment 748
Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation
Article 42 – paragraph 1

Text proposed by the Commission

Amendment

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

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, shall be invited to participate
the workings of Cooperation Group.
in the work of the Cooperation Group
insofar as that work concerns supervisory and oversight activities, respectively, in relation to entities listed under point (7) of Annex II to Directive (EU) 2016/1148 which have also been designated as critical ICT third-party service providers pursuant to Article 28 of this Regulation.

Amendment 749
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 42 – paragraph 1

Text proposed by the Commission

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.

Amendment

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, shall participate in the work of the Cooperation Group as set out in Article 11 of Directive (EU) 2016/1148 in so far as that work concerns any aspect of the subject matter set out in Article 1 of this Regulation.

Amendment 750
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 42 – paragraph 2 a (new)

Text proposed by the Commission

2 a. The Joint Oversight Executive Body shall inform and cooperate with the
relevant competent authorities designated under Directive (EU) 2016/1148 before conducting general investigations and inspections in accordance with Article 31(1)(b), and Articles 33 and 34 of this Regulation.

Amendment 751
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 43 – paragraph 2

Text proposed by the Commission
Amendment

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.

Amendment 752
Bogdan Rzońca

Proposal for a regulation
Article 43 a (new)

Text proposed by the Commission
Amendment

Article 43 a

Platform on Cybersecurity of Financial Sector
1. The Commission shall establish or designate an advisory body on standards in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk (‘Platform on Cybersecurity of Financial Sector’).

2. The Platform on Cybersecurity of Financial Sector shall be composed in a balanced manner of the following groups:

(a) representatives of:

(i) the Commission;

(ii) the ESAs; ENISA and

(iii) the competent authorities;

(b) experts representing relevant private stakeholders, including financial and non-financial market participants and business sectors, representing relevant industries, and persons with accounting and reporting expertise;

(c) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation.

3. The Platform on Cybersecurity of Financial Sector shall:

(a) advise the ESAs on the drawing up of the regulatory technical standards referred to in Articles 14, 16, 18, 23, 25, 27, 35, 36 as well as on the possible need to update those standards;

(b) analyse the impact of those regulatory technical standards in terms of potential costs and benefits of their application;

(c) assist the Commission in analysing requests from stakeholders to develop or revise those regulatory technical standards;

(d) monitor and regularly report to the Commission on trends at Union and Member State level regarding developments in the areas covered by those regulatory technical standards;

(e) advise the Commission on the possible
need to amend this Regulation.

4. The Platform on Cybersecurity of Financial Sector shall be chaired by the Commission and constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context the Commission may invite experts with specific expertise on an ad hoc basis.

5. The Platform on Cybersecurity of Financial Sector shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish the minutes of the meetings of the Platform on Cybersecurity of Financial Sector and other relevant documents on the Commission website.“

Amendment 753
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission

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

Amendment

1. The Joint Oversight Body and the competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.

Amendment 754
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 44 – paragraph 4 – point e a (new)
Text proposed by the Commission

Amendment

(e a) provide an automatic compensation to their service users and clients where an operational incident hampered the use of financial services for a period of more than 48 hours;

Or. en

Amendment 755
Alfred Sant

Proposal for a regulation
Article 48 – paragraph 2

Text proposed by the Commission

Amendment

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.

Or. en

Amendment 756
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 48 – paragraph 3 – introductory part

Text proposed by the Commission

Amendment

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:

Amendment 757
Mikuláš Peksa
on behalf of the Greens/EFA Group

Proposal for a regulation
Article 48 – paragraph 3 – point c

Text proposed by the Commission
(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.

Amendment
(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.

Amendment 758
Alfred Sant

Proposal for a regulation
Article 48 – paragraph 6

Text proposed by the Commission
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

Amendment
6. Competent authorities shall ensure that any publication referred to in paragraphs 1 and 2 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.

Amendment 759
Alfred Sant

Proposal for a regulation
Article 50 – paragraph 2

Text proposed by the Commission

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].

Amendment

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 three years from [PO: insert date 3 years after the date of entry into force of this Regulation].

Amendment 760
Bogdan Rzońca

Proposal for a regulation
Article 51 – paragraph 1 a (new)

Text proposed by the Commission

1a. 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 Platform on Cybersecurity of Financial Sector, 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 desirability of setting up an optional regulatory sandbox whereby critical ICT third-party service providers would:
(a) be able to apply for permission to operate in a controlled environment provided by the Lead Overseer in order to test the application of innovative cybersecurity measures required for the purposes of this Regulation; and

(b) be temporarily exempted from some specific requirements under Union financial services legislation that could otherwise prevent them from verifying solutions for the development or application of such cybersecurity measures.

In the report referred to in the first subparagraph, the Commission shall also consider how the regulatory sandbox would best enable it, the ESAs and competent authorities to gain experience on the opportunities and specific risks created by the innovative cybersecurity measures, and by their underlying technology.

Amendment 761
Alfred Sant

Proposal for a regulation
Article 56 – paragraph 2

Text proposed by the Commission

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

Amendment

It shall apply from [PO: insert date - 36 months after the date of entry into force].

Amendment 762
Engin Eroglu

Proposal for a regulation
Article 56 – paragraph 2
Text proposed by the Commission  

**Amendment**

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

It shall apply from [PO: insert date - 24 months after the date of entry into force].

Or. en

**Justification**

Give more time for implementation, especially for small banks this timeline might be too short.

---

**Amendment 763**

Markus Ferber

Proposal for a regulation

Article 56 – paragraph 2

Text proposed by the Commission  

**Amendment**

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

It shall apply from [PO: insert date - 24 months after the date of entry into force].

Or. en

---

**Amendment 764**

Bogdan Rzońca

Proposal for a regulation

Article 56 – paragraph 2

Text proposed by the Commission  

**Amendment**

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

It shall apply from [PO: insert date - 24 months after the date of entry into force].

Or. en

---

**Amendment 765**

Frances Fitzgerald, Isabel Benjumea Benjumea

Proposal for a regulation

Article 56 – paragraph 2
Text proposed by the Commission

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

Amendment

It shall apply from [PO: insert date - 24 months after the date of entry into force].

Or. en