European Parliament
2019-2024

Committee on Economic and Monetary Affairs

2020/0266(COD)

17.3.2021

***I
DRAFT REPORT

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

Committee on Economic and Monetary Affairs

Rapporteur: Billy Kelleher

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2020)0595),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0304/2020),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of ...[1],

– having regard to the opinion of the European Central Bank of ...[2],

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the report of the Committee on Economic and Monetary Affairs (A9-0000/2021),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

---

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

Amendment 1

Proposal for a regulation
Recital 17

Text proposed by the Commission	*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.	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. ***Moreover, this Regulation should ensure that the CSIRTs network established by Directive (EU) No 2016/1148 is provided with the details of major ICT-related incidents.***

Or. en

Amendment 2

Proposal for a regulation
Recital 20

Text proposed by the Commission	*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	(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 ***and ICT intra-group*** risk. The digital operational resilience bar for the financial system

a proportionate application of requirements for financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC[32] .	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] .
[32] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[32] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Or. en

Amendment 3

Proposal for a regulation
Recital 33

Text proposed by the Commission	*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 ***and*** business profile, while competent authorities should continue to assess and review the approach of such distribution.	(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***,*** business ***profile, and relative risk*** profile, while competent authorities should continue to assess and review the approach of such distribution.

Or. en

Amendment 4

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.	(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 ***significant*** ICT disruptions***, major ICT-related incidents*** and the results of post-incident reviews after significant ICT disruptions.

Or. en

Amendment 5

Proposal for a regulation
Recital 36 – introductory part

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

commitment to respect a strict cyber hygiene at all levels.

of awareness over cyber risks and a commitment to respect a strict cyber hygiene at all levels. ***Members of the management body of all financial entities, including of microenterprises, should actively keep their knowledge up to date and follow specific training where necessary.***

Or. en

Amendment 6

Proposal for a regulation
Recital 40

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

Or. en

Amendment 7

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) In order to achieve robust digital operational resilience, and in line with international standards (e.g. the G7	(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.

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.

The methodology for TLPT should not be mandated but the use of the existing TIBER-EU framework should be considered as complying with the TLPT framework in this Regulation.

Based upon the success of this Regulation and market developments, the Commission should consider as part of the review process, the introduction of a testing accreditation scheme.

Or. en

Amendment 8

Proposal for a regulation
Recital 49

Text proposed by the Commission	*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	(49) To address the systemic impact of ICT third-party concentration risk, a balanced solution through a flexible and gradual approach should be promoted since rigid caps or strict limitations may hinder business conduct and contractual freedom. Financial entities should thoroughly assess contractual arrangements to identify the

likelihood for such risk to emerge, including by means of in-depth analyses of sub-outsourcing arrangements***, notably when concluded with ICT third-party service providers established in a third country***. At this stage, and with a view to strike a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to provide for strict caps and limits to ICT third-party exposures. The ***ESA designated to conduct*** the oversight for each critical ICT third-party provider ***("the Lead Overseer")*** should in the exercise of oversight tasks pay particular attention to fully grasp the magnitude of interdependences and discover specific instances where a high degree of concentration of critical ICT third-party service providers in the Union is likely to put a strain on the Union financial system's stability and integrity and should provide instead for a dialogue with critical ICT third-party service providers where that risk is identified.[38]

likelihood for such risk to emerge, including by means of in-depth analyses of sub-outsourcing arrangements. 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 Executive Body conducting*** the oversight for each 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.[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.

[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.

Or. en

Amendment 9

Proposal for a regulation
Recital 51

Text proposed by the Commission	*Amendment*
(51) Contractual arrangements should in particular provide for a specification of	(51) Contractual arrangements should in particular provide for a specification of

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

Or. en

Amendment 10

Proposal for a regulation
Recital 52

Text proposed by the Commission	*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 at no additional cost or at a cost that is determined ex-ante.	(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 ***in line with the agreed service levels***, including the provision of assistance by the latter in case of an ICT-related incident ***related to the service provider*** at no additional cost or at a cost that is determined ex-ante. ***Under this Regulation, the term 'critical or important function' also encompasses critical***

functions as defined under point 35 of Article 2(1) of the Directive 2014/59/EU of the European Parliament and of the Council[1a].

[1a] Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

Or. en

Amendment 11

Proposal for a regulation
Recital 53

Text proposed by the Commission	*Amendment*
(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.	(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 ***Joint Oversight Executive Body overseeing the ICT third-party service provider and 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 ***and whilst exercising caution not to disrupt the services provided to other customers of the ICT third-party service provider***.

Or. en

Amendment 12

Proposal for a regulation
Recital 54

Text proposed by the Commission	*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.	(54) Contractual arrangements should provide for clear termination rights***, to be exercised in the event that all other remedies have been exhausted,*** 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 ***in-house*** solutions, consistent with the complexity of the provided service.

Or. en

Amendment 13

Proposal for a regulation
Recital 58

Text proposed by the Commission	*Amendment*
(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.	(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. ***The requirement to have a legal entity 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.

Or. en

Amendment 14

Proposal for a regulation
Recital 60

Text proposed by the Commission	*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, 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.	(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 ***Joint*** Oversight ***Executive Body*** carrying out preparatory work for both decisions ***and recommendations*** addressed to critical ICT third-party service providers, 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 15

Proposal for a regulation
Recital 61

Text proposed by the Commission	*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, one of the ESAs ***should be designated as Lead Overseer for each critical*** ICT third-party service provider.	(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 Executive Body should be responsible for day to day oversight and should appoint*** one of the ESAs ***as having the responsibility to adopt formal decisions or recommendations addressed to the*** ICT third-party service provider.

Or. en

Amendment 16

Proposal for a regulation
Recital 62 – introductory part

Text proposed by the Commission	*Amendment*
(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 Joint Oversight Executive 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

Amendment 17

Proposal for a regulation
Recital 62 – point 1

Text proposed by the Commission	*Amendment*
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.	Entrusting the ***Joint Oversight Executive Body*** with the 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 ***service*** providers facing such numerous requests.

Or. en

Amendment 18

Proposal for a regulation
Recital 63

Text proposed by the Commission	*Amendment*
(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.	(63) In addition, ***the Joint Oversight Executive Body*** should be able to ***prepare*** recommendations***, for adoption by the ESAs,*** 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 ***Joint Oversight Executive Body*** should be duly taken into account by national competent authorities as part of their function relating to the prudential supervision of financial entities.

Or. en

Amendment 19

Proposal for a regulation
Recital 64

Text proposed by the Commission	*Amendment*
(64) The Oversight Framework shall not replace, or in any way nor for any part substitute the management by financial entities of the risk entailed by the use of ICT third-party service providers, including the obligation of ongoing monitoring of their contractual arrangements concluded with critical ICT third-party service providers, and shall not affect the full responsibility of the financial entities in complying with, and discharging of, all requirements under this Regulation and relevant financial services legislation. To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring the critical ICT third-party service provider's risks ***Any such measures should be previously coordinated and agreed in in the context of the Oversight Framework***.	(64) The Oversight Framework shall not replace, or in any way nor for any part substitute the management by financial entities of the risk entailed by the use of ICT third-party service providers, including the obligation of ongoing monitoring of their contractual arrangements concluded with critical ICT third-party service providers, and shall not affect the full responsibility of the financial entities in complying with, and discharging of, all requirements under this Regulation and relevant financial services legislation. To avoid duplications and overlaps, competent authorities should refrain from individually taking any measures aimed at monitoring the critical ICT third-party service provider's risks.

Or. en

Amendment 20

Proposal for a regulation
Recital 66

Text proposed by the Commission	*Amendment*
(66) To leverage technical expertise of competent authorities' experts on operational and ICT risk management, ***Lead Overseers*** should draw on national supervisory experience and set up dedicated examination teams for each individual critical ICT third-party service	(66) To leverage technical expertise of competent authorities' experts on operational and ICT risk management, ***the Joint Oversight Executive Body*** should draw on national supervisory experience and set up dedicated examination teams for each individual critical ICT third-party

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.	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.

Or. en

Amendment 21

Proposal for a regulation
Recital 67

Text proposed by the Commission	*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 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.	(67) ***The Joint Oversight Executive Body and*** 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. ***The Single Resolution Board, although not a competent authority for the purposes of this Regulation, should nevertheless be involved in the mechanisms for the mutual exchange of information for entities that fall within the scope of Regulation (EU) No 806/2014 of the European Parliament and of the Council[39a].***

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

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

[39a] ***Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 (OJ L 225, 30.7.2014, p. 1).***

Or. en

Amendment 22

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

Text proposed by the Commission	*Amendment*
(m) insurance and reinsurance undertakings,	(m) insurance and reinsurance undertakings, ***unless they are micro, small or medium-sized enterprises and do not rely on systematised insurance intermediation,***

Or. en

Amendment 23

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

Text proposed by the Commission	*Amendment*
(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,	(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, ***unless they are micro, small or medium-sized enterprises***

and do not rely on systematised insurance intermediation,

Or. en

Amendment 24

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

Text proposed by the Commission	*Amendment*
(q) statutory auditors and audit firms,	(q) statutory auditors and audit firms, ***unless they are micro, small or medium-sized enterprises,***

Or. en

Amendment 25

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

Text proposed by the Commission	*Amendment*
	(ua) ICT intra-group service providers, with the exception of Section II of Chapter V of this Regulation that is not applicable to such providers,

Or. en

Amendment 26

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

Text proposed by the Commission	*Amendment*
	2a. For the purposes of this Regulation, with the exception of Section II of Chapter V, entities referred to in points (u) and (ua) of paragraph 1 shall

be collectively referred to as 'ICT third-party service providers'.

Or. en

Amendment 27

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

Text proposed by the Commission	*Amendment*
(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***;	(4) 'ICT risk' means any circumstance which, if materialised, may compromise the security of ***or adversely affect*** the network and information systems, any technology-dependant tool or process, the operation and process' running, or the provision of services;

Or. en

Amendment 28

Proposal for a regulation
Article 3 – paragraph 1 – point 14

Text proposed by the Commission	*Amendment*
(14) 'ICT third-party risk' means ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers ***or*** by further sub-contractors of the latter;	(14) 'ICT third-party risk' means ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers***,*** by further sub-contractors of the latter***, or by***

ICT intra-group service providers;

Or. en

Amendment 29

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

Text proposed by the Commission	*Amendment*
	(15a) 'ICT intra-group service provider' means an undertaking that provides ICT services, related to critical or important functions, exclusively to financial entities within the same group;

Or. en

Amendment 30

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

Text proposed by the Commission	*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***;	(16) 'ICT services' means digital and data services provided through the ICT systems to one or more internal or external users;

Or. en

Amendment 31

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

Text proposed by the Commission	*Amendment*
(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;	(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; ***this definition includes 'critical functions' as defined under point (35) of Article 2(1) of the Directive 2014/59/EU;***

Or. en

Amendment 32

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*** of the Annex to Recommendation 2003/361/EC.

Or. en

Amendment 33

Proposal for a regulation
Article 4 – paragraph 4

Text proposed by the Commission	*Amendment*
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***	4. Members of the management body***, including those of microenterprises,*** shall ***actively keep their*** knowledge and skills ***up to date including, where commensurate to***

understand and assess ICT risks ***and their impact on the operations of the financial entity***.	***the*** ICT risks ***being managed, following specific training on a regular basis***.

Or. en

Amendment 34

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***.

Or. en

Amendment 35

Proposal for a regulation
Article 5 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The ICT risk management framework referred to in paragraph 1 shall include strategies, policies, procedures, ICT protocols and tools which are necessary to duly and effectively protect all relevant physical components and infrastructures, including computer hardware, servers, as well as all relevant premises, data centres and sensitive designated areas, to ensure that all those physical elements are adequately protected from risks including damage and unauthorized access or usage.	2. The ICT risk management framework referred to in paragraph 1 shall include strategies, policies, procedures, ICT protocols and tools which ***are suited to the financial entity's risk profile and*** are necessary to duly and effectively protect all relevant physical components and infrastructures, including computer hardware, servers, as well as all relevant premises, data centres and sensitive designated areas, to ensure that all those physical elements are adequately protected from risks including damage and

unauthorized access or usage.

Or. en

Amendment 36

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 37

Proposal for a regulation
Article 5 – paragraph 9 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	In addition, depending on the risk profile of the financial entity, the ICT risk management framework referred to in paragraph 1 shall define 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 and intra-group service providers. Upon approval of competent authorities, the multi-vendor strategy may be defined at group level.

Or. en

Amendment 38

Proposal for a regulation
Article 6 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Financial entities shall use and maintain updated ICT systems, protocols and tools, which fulfil the following conditions:	1. Financial entities shall use and maintain updated ICT systems, protocols and tools, which ***are commensurate to their risk profile and*** fulfil the following conditions:

Or. en

Amendment 39

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission	*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, 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.	1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify ***all ICT-related business functions. For critical or important functions***, ***financial entities shall*** 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 ***criticality or importance of ICT-related business functions, as well as the*** adequacy of the classification of the information assets and of any relevant documentation.

Or. en

Amendment 40

Proposal for a regulation
Article 8 – paragraph 2

Text proposed by the Commission	*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.	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 ***supporting critical or important functions***, and maintaining high standards of security, confidentiality and integrity of data, whether at rest, in use or in transit.

Or. en

Amendment 41

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

Text proposed by the Commission	*Amendment*
(d) ensure that data is protected from poor administration ***or processing-related risks, including inadequate record-keeping***.	(d) ensure that data is protected from ***internal ICT risks including*** poor administration ***and human error***.

Or. en

Amendment 42

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

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

Or. en

Amendment 43

Proposal for a regulation
Article 8 – paragraph 4 – subparagraph 2

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

Or. en

Amendment 44

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

Text proposed by the Commission	*Amendment*
(a) recording all ICT-related incidents;	(a) recording all ICT-related incidents ***having an impact on the stability, continuity or quality of financial services, including where the incident had both an actual and potential impact on the services***;

Or. en

Amendment 45

Proposal for a regulation
Article 10 – paragraph 9

Text proposed by the Commission	*Amendment*
9. Financial entities other than microenterprises shall report to competent authorities all costs and losses caused by ICT disruptions and ICT-related incidents.	9. Financial entities other than microenterprises shall report to competent authorities all costs and losses caused by ***significant*** ICT disruptions and ***major*** ICT-related incidents. ***The European Supervisory Authorities shall, through the Joint Committee, develop a common draft regulatory technical standard further specifying the costs and losses that are considered to be relevant.***

Or. en

Amendment 46

Proposal for a regulation
Article 10 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. The ESAs shall submit the common draft regulatory technical standard referred to in paragraph 9 of this Article to the Commission by [PO: insert date 1 year after the date of entry into force of this Regulation].
	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standard referred to in paragraph 9, in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.

Or. en

Amendment 47

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

Text proposed by the Commission	*Amendment*
(c) ***immediately*** accessible to the financial entity's staff to ensure continuity of critical services in case the primary processing site has become unavailable.	(c) accessible to the financial entity's staff to ensure continuity of critical services in case the primary processing site has become unavailable.

Or. en

Amendment 48

Proposal for a regulation
Article 11 – paragraph 6

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

Or. en

Amendment 49

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, financial entities other than microenterprises shall communicate those changes to the competent authorities***, detailing the required improvements and how those aim to prevent or mitigate disruption in***

the future.

Or. en

Amendment 50

Proposal for a regulation
Article 12 – paragraph 4

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

Or. en

Amendment 51

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

Text proposed by the Commission	*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 and to senior management staff.	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 ***with rights of direct access to the ICT systems*** and to senior management staff.

Or. en

Amendment 52

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

Text proposed by the Commission	*Amendment*
(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;	***deleted***

Or. en

Amendment 53

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

Text proposed by the Commission	*Amendment*
(c) specify further the appropriate techniques, methods and protocols referred to in point (b) of Article 8(4);	***deleted***

Or. en

Amendment 54

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

Text proposed by the Commission	*Amendment*
(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring	***deleted***

anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;

Or. en

Amendment 55

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

Text proposed by the Commission	*Amendment*
	1a. In order to determine whether a major ICT-related incident has occurred, at least the following parameters shall be taken into account:
	(a) the number of users affected by the disruption of a critical or important function;
	(b) the duration of the incident;
	(c) the geographical spread with regard to the area affected by the incident.

Or. en

Amendment 56

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission	*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	2. Where a major ICT-related incident ***occurs***, 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.

of such incident.

Or. en

Amendment 57

Proposal for a regulation
Article 17 – paragraph 2 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	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.

Or. en

Amendment 58

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

Text proposed by the Commission	*Amendment*
	(ba) the Single Resolution Board (SRB), in cases where the reporting entity falls within the scope of Regulation (EU) No 806/2014;

Or. en

Amendment 59

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

Text proposed by the Commission	*Amendment*
	(ca) the CSIRTs network established by Article 12 of Directive (EU) 2016/1148, in

	cases where the reporting entity falls within the scope of that Directive.

Or. en

Amendment 60

Proposal for a regulation
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Financial entities identified in accordance with paragraph ***4*** shall carry out at least every 3 years advanced testing by means of threat led penetration testing.	1. Financial entities identified in accordance with ***second subparagraph of*** paragraph ***3*** shall carry out at least every 3 years advanced testing by means of threat led penetration testing.

Or. en

Amendment 61

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
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.	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***, where possible, or pre-production systems with the same security configuration***. 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 62

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*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 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 testing could have an impact on the quality, confidentiality or security of the ICT third-party provider's services to other customers not falling within the scope of this Regulation, 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. ICT third-party service providers may enter into such arrangements on behalf of all their financial entity customers in order to conduct pooled testing.***

Or. en

Amendment 63

Proposal for a regulation
Article 23 – paragraph 2 – subparagraph 4

Text proposed by the Commission	*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 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.	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 Joint Oversight Executive Body*** the documentation confirming that

	the threat led penetration testing has been conducted in accordance with the requirements. Competent authorities ***or the Joint Oversight Executive Body*** shall validate the documentation and issue an attestation.

Or. en

Amendment 64

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***, or in the case of ICT third-party service providers conducting testing directly,*** shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.

Or. en

Amendment 65

Proposal for a regulation
Article 23 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) the criteria used for the purpose of the application of paragraph ***6*** of this Article;	(a) the criteria used for the purpose of the application of ***the second subparagraph of*** paragraph ***3*** of this Article;

Or. en

Amendment 66

Proposal for a regulation
Article 23 – paragraph 4 – point c

Text proposed by the Commission	*Amendment*
(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..	(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 ***and testing undertaken directly by ICT third-party service providers***, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets..

Or. en

Amendment 67

Proposal for a regulation
Article 24 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Financial entities shall only use testers for the deployment of threat led penetration testing, which:	1. Financial entities ***and ICT third-party service providers for the purposes of Article 23(2)*** shall only use testers for the deployment of threat led penetration testing, which:

Or. en

Amendment 68

Proposal for a regulation
Article 24 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Financial entities shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report,	2. Financial entities ***and ICT third-party service providers, for the purposes of Article 23(2),*** shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any

communication or destruction, do not create risks to the financial entity.	processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.

Or. en

Amendment 69

Proposal for a regulation
Article 25 – paragraph 1 – point 3

Text proposed by the Commission	*Amendment*
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.	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 ***subparagraph 1a*** 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.

Or. en

Amendment 70

Proposal for a regulation
Article 25 – paragraph 1 – point 4 – subparagraph 1

Text proposed by the Commission	*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	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.	of ***critical or important*** ICT services provided by ICT third-party service providers.

Or. en

Amendment 71

Proposal for a regulation
Article 25 – paragraph 1 – point 4 – subparagraph 2

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

Or. en

Amendment 72

Proposal for a regulation
Article 25 – paragraph 1 – point 4 – subparagraph 3

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

Or. en

Amendment 73

Proposal for a regulation
Article 25 – paragraph 1 – point 6

Text proposed by the Commission	*Amendment*
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.	6. Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the ***up-to-date*** information security standards.

Or. en

Amendment 74

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 are ***able to be*** terminated***, after all other remedies have been exhausted,*** at least under the following circumstances:

Or. en

Amendment 75

Proposal for a regulation
Article 25 – paragraph 1 – point 8 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) in accordance with a recommendation issued by the Joint Oversight Executive Body pursuant to Article 37 to a critical ICT third-party service provider;

Or. en

Amendment 76

Proposal for a regulation
Article 25 – paragraph 1 – point 9 – subparagraph 1

Text proposed by the Commission	*Amendment*
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.	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 ***providers***, in particular ***in the event of termination of contractual arrangements with ICT third-party service providers in any of the circumstances listed in point 8,*** 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 77

Proposal for a regulation
Article 26 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
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:	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 ***critical or important*** ICT services would lead to any of the following:

Or. en

Amendment 78

Proposal for a regulation
Article 26 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
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***.	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.

Or. en

Amendment 79

Proposal for a regulation
Article 26 – paragraph 2 – subparagraph 2 – introductory part

Text proposed by the Commission	*Amendment*
Where contractual arrangements on the use of ICT services are concluded with an ICT third-party service provider ***established in a third-country***, financial entities shall consider relevant, at least the following factors:	Where contractual arrangements on the use of ICT services are concluded with an ICT third-party service provider, financial entities shall consider relevant, at least the following factors:

Or. en

Amendment 80

Proposal for a regulation
Article 26 – paragraph 2 – subparagraph 3

Text proposed by the Commission	*Amendment*
Financial entities shall assess whether and	***Where such contractual arrangements***

how potentially long or complex chains of sub-contracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

include the sub-contracting of critical or important functions, financial entities shall assess whether and how potentially long or complex chains of sub-contracting may impact their ability to fully ***assess the factors listed in points (a) to (d), to*** monitor the contracted functions***,*** and the ability of the competent authority to effectively supervise the financial entity in that respect.

Or. en

Amendment 81

Proposal for a regulation
Article 27 – paragraph 1

Text proposed by the Commission	*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 one written document*** available to the parties on paper or in a downloadable and accessible format.	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 ***and*** available to the parties on paper or in a downloadable and accessible format.

Or. en

Amendment 82

Proposal for a regulation
Article 27 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(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	(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;	entity in the case of insolvency, resolution***,*** discontinuation of the business operations of the ICT third-party service provider***, or in the case of termination of the contractual arrangements***;

Or. en

Amendment 83

Proposal for a regulation
Article 27 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(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;	***deleted***

Or. en

Amendment 84

Proposal for a regulation
Article 27 – paragraph 2 – point f

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

Or. en

Amendment 85

Proposal for a regulation
Article 27 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:	***deleted***
i) rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	
ii) the right to agree alternative assurance levels if other clients' rights are affected;	
iii) the commitment to fully cooperate during the onsite inspections performed by the financial entity and details on the scope, modalities and frequency of remote audits;	

Or. en

Amendment 86

Proposal for a regulation
Article 27 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. The contractual arrangements for the provision of critical or important functions shall, in addition to the provisions set out in paragraph 2, include at least the following:
	(a) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development which might have a material impact on the ICT

third-party service provider's ability to effectively carry out critical or important functions in line with agreed service levels;

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

i) rights of access, inspection and audit by the financial entity or by an appointed third party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;

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

iii) the commitment to fully cooperate during the onsite inspections performed by the financial entity and details on the scope, modalities and frequency of remote audits;

By way of derogation from point (b), the ICT third-party service provider and the financial entity may agree that the rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.

Or. en

Amendment 87

Proposal for a regulation
Article 27 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2b. The contractual arrangements for the provision of ICT services by an ICT

third-party service provider established in a third country 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, in the event the ICT third-party service provider is designated as critical pursuant to Article 28(9), 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.

Or. en

Amendment 88

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 ESAs, upon recommendation from the ***Joint*** Oversight ***Executive Body*** established pursuant to Article 29(1) shall:

Or. en

Amendment 89

Proposal for a regulation
Article 28 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) designate the ICT third-party service providers that are critical for financial entities, taking into account the criteria specified in paragraph 2***;***	(a) designate the ICT third-party service providers that are critical for financial entities, taking into account the criteria specified in paragraph 2***. Critical ICT third-party service providers shall be subject to oversight by the Joint Oversight***

Executive Body.

Or. en

Amendment 90

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***, ***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***.	(b) appoint either EBA, ESMA or EIOPA 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***.

Or. en

Amendment 91

Proposal for a regulation
Article 28 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	6. The ***Joint Oversight Executive Body***, through the Joint Committee, shall establish, publish and yearly update the list of critical ICT third-party service providers at Union level.

Or. en

Amendment 92

Proposal for a regulation
Article 28 – paragraph 7

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

Or. en

Amendment 93

Proposal for a regulation
Article 28 – paragraph 7 a (new)

Text proposed by the Commission	*Amendment*
	7a. The draft recommendation of criticality by the Joint Oversight Executive Body, referred to in paragraph 1, shall be communicated to the ICT third-party service provider prior to the decision on designation by the ESAs.
	On receipt of the draft recommendation, the ICT third-party service provider shall have six weeks to review and comment upon it. The ESAs shall take due consideration of those comments and may request further information or evidence from the ICT third-party service provider prior to taking a decision on designation.

Or. en

Amendment 94

Proposal for a regulation
Article 28 – paragraph 8 – subparagraph 2

Text proposed by the Commission	*Amendment*
For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to ***EBA, ESMA or EIOPA***, which, ***through*** the Joint ***Committee***, shall decide whether to include that ICT third-party service provider in that list in accordance with point (a) of paragraph 1.	For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to ***the ESAs***, which, ***upon recommendation from*** the Joint ***Oversight Executive Body***, shall decide whether to include that ICT third-party service provider in that list in accordance with point (a) of paragraph 1.

Or. en

Amendment 95

Proposal for a regulation
Article 28 – paragraph 9

Text proposed by the Commission	*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 it were established*** in the Union.	9. Financial entities shall not make use of an ICT third-party service provider established in a third country ***for a*** critical ***or important function unless that ICT third-party service provider has a legal entity in the Union and has concluded contractual arrangements in accordance with Article 27(2b).*** ***The Joint Oversight Executive Body shall, in a recommendation, consider the criticality of third-country ICT third-party service providers in accordance with paragraphs 1 and 2 of this Article.*** ***The recommendation of the Joint Oversight Executive Body shall be communicated to the legal entity in the Union of the ICT third-party service provider. That legal entity shall have the right to comment on the recommendation***

in accordance with the second subparagraph of paragraph ***7a.***

Upon designation as critical, all correspondence from the Joint Oversight Executive Body shall be with the legal entity in the Union ***of the ICT third-party service provider***.

Or. en

Amendment 96

Proposal for a regulation
Article 28 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. The ESAs shall notify the ICT third-party service provider of its designation as critical. The ICT third-party service provider shall have 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.

Or. en

Amendment 97

Proposal for a regulation
Article 29 – paragraph 1 – subparagraph 1

Text proposed by the Commission	*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 referred to in point (b) of Article 28(1) in the area of*** ICT third-party risk	1. The Joint Oversight ***Executive Body shall be established*** for the purposes of ***overseeing*** ICT third-party risk across financial sectors ***and direct*** oversight ***of ICT third-party service providers designated as critical pursuant to Article 28. The Joint Oversight Executive Body*** shall prepare the draft ***decisions, recommendations and other acts for***

across financial sectors***.*** ***The*** Oversight ***Forum*** shall prepare the draft ***joint positions and common acts of the Joint Committee in that area***.	***adoption by the ESA appointed pursuant to paragraph 1(b) of Article 28***.

Or. en

Amendment 98

Proposal for a regulation
Article 29 – paragraph 1 – subparagraph 2

Text proposed by the Commission	*Amendment*
The Oversight ***Forum*** shall regularly discuss relevant developments on ICT risks and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union scale.	The ***Joint*** Oversight ***Executive Body*** shall regularly discuss relevant developments on ICT risks and vulnerabilities and promote a consistent approach in the monitoring of ICT third-party risk at Union scale.

Or. en

Amendment 99

Proposal for a regulation
Article 29 – paragraph 2

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

Or. en

Amendment 100

Proposal for a regulation
Article 29 – paragraph 3

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

Or. en

Amendment 101

Proposal for a regulation
Article 29 – paragraph 4

Text proposed by the Commission	*Amendment*
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.	4. The ***Joint*** Oversight ***Executive Body*** shall be composed of the ***Executive Directors*** of the ESAs, one high-level representative from the current staff of ***each of the ESAs, and one high-level representative from at least five of the national*** competent ***authorities***. One representative from the European Commission, from the ESRB, from ECB and from ENISA shall participate in the ***Joint*** Oversight ***Executive Body*** as observers. ***Following each designation of critical ICT third-party service providers pursuant to Article 28(6), the Joint Committee shall decide which national competent authorities are to be members of the Joint Oversight Executive Body, taking into account the following factors:*** ***- the number of critical ICT third-party service providers established or providing***

services in a Member State;

- the reliance of the financial entities in a Member State on critical ICT third-party service providers;

- the relative expertise of a national competent authority;

- the available resources and capacity of a national competent authority;

- the need for the operation and decision making of the Joint Oversight Executive Body to be streamlined, lean, and efficient.

The documentation and decisions of the Joint Oversight Executive Body shall be shared with all non-participating national competent authorities.

Or. en

Amendment 102

Proposal for a regulation
Article 29 – paragraph 5

Text proposed by the Commission	*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 on the cooperation between the ESAs and the competent authorities for the purposes of this Section on the detailed procedures and conditions relating to the execution of tasks between competent authorities and the ESAs and details on exchanges of information needed by competent authorities to ensure the follow-up of recommendations addressed by Lead Overseers pursuant to point (d) of Article 31(1) to critical ICT third-party providers***.	5. ***The work of the Joint Oversight Executive Body shall be supported and assisted by dedicated staff from across*** the ESAs.

Or. en

Amendment 103

Proposal for a regulation
Article 29 – paragraph 7

Text proposed by the Commission	*Amendment*
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.	7. The Joint Oversight ***Executive Body***, shall present yearly to the European Parliament, the Council and the Commission a report on the application of this Section.

Or. en

Amendment 104

Proposal for a regulation
Article 30 – title

Text proposed by the Commission	*Amendment*
Tasks of the ***Lead Overseer***	Tasks of the ***Joint Oversight Executive Body***

Or. en

Amendment 105

Proposal for a regulation
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. The ***Joint Oversight Executive 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. ***The assessment shall primarily focus on the critical or important functions provided by the***

critical ICT third-party service provider to financial entities, but may also be broader if relevant to the assessment of the risks to those services.

Or. en

Amendment 106

Proposal for a regulation
Article 30 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(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;	(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;

Or. en

Amendment 107

Proposal for a regulation
Article 30 – paragraph 3

Text proposed by the Commission	*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. ***That*** plan shall be communicated ***each year*** to the critical ICT third-party service provider.	3. Based on the assessment referred to in paragraph 1, the ***Joint Oversight Executive Body*** shall ***propose*** a clear, detailed and reasoned individual Oversight plan for each critical ICT third-party service provider. ***The Oversight plan shall be adopted on a yearly basis by the ESA appointed pursuant to paragraph 1(b) of Article 28, and the plan shall be executed on a day-to-day basis by the Joint Oversight Executive Body.*** ***Prior to the adoption by the ESAs, the draft Oversight*** plan shall be communicated to the critical ICT third-party service provider. ***The critical ICT third-party service provider shall have six***

weeks to review and comment on the draft Oversight plan. Grounds for challenging a draft Oversight plan may include that there would be a disproportionate impact on or disruption to customers not subject to this Regulation, or that there is a more effective or efficient solution for managing the identified ICT risks.

The ESAs shall take due consideration of those comments and may request further information or evidence from the ICT third-party service provider prior to taking a final decision on the Oversight plan.

Or. en

Amendment 108

Proposal for a regulation
Article 30 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Once the annual Oversight plans referred to in paragraph 3 have been ***agreed*** and notified to the critical ICT third-party service providers, competent authorities may only take measures concerning critical ICT third-party service providers ***in agreement with the Lead Overseer***.	4. Once the annual Oversight plans referred to in paragraph 3 have been ***adopted*** and notified to the critical ICT third-party service providers, competent authorities may only take measures concerning critical ICT third-party service providers ***upon recommendation by the Joint Oversight Executive Body***.

Or. en

Amendment 109

Proposal for a regulation
Article 31 – title

Text proposed by the Commission	*Amendment*
Powers of the ***Lead Overseer***	Powers of the ***Joint Oversight Executive Body***

Or. en

Amendment 110

Proposal for a regulation
Article 31 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. For the purposes of carrying out the duties laid down in this Section, the ***Lead Overseer*** shall have the following powers:	1. For the purposes of carrying out the duties laid down in this Section, the ***Joint Oversight Executive Body*** shall have the following powers:

Or. en

Amendment 111

Proposal for a regulation
Article 31 – paragraph 1 – point d – point i

Text proposed by the Commission	*Amendment*
(i) the use of specific ICT security and quality requirements or processes, notably in relation to the roll-out of patches, updates, encryption and other security measures which the ***Lead Overseer*** deems relevant for ensuring the ICT security of services provided to financial entities;	(i) the use of specific ICT security and quality requirements or processes, notably in relation to the roll-out of patches, updates, encryption and other security measures which the ***Joint Oversight Executive Body*** deems relevant for ensuring the ICT security of services provided to financial entities;

Or. en

Amendment 112

Proposal for a regulation
Article 31 – paragraph 1 – point d – point ii

Text proposed by the Commission	*Amendment*
(ii) the use of conditions and terms, including their technical implementation, under which the critical ICT third-party	(ii) the use of conditions and terms, including their technical implementation, under which the critical ICT third-party

service providers provide services to financial entities, which the ***Lead Overseer*** deems relevant for preventing the generation of single points of failure, or the amplification thereof, or for minimising possible systemic impact across the Union's financial sector in case of ICT concentration risk;	service providers provide services to financial entities, which the ***Joint Oversight Executive Body*** deems relevant for preventing the generation of single points of failure, or the amplification thereof, or for minimising possible systemic impact across the Union's financial sector in case of ICT concentration risk;

Or. en

Amendment 113

Proposal for a regulation
Article 31 – paragraph 1 – point d – point iii

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

Or. en

Amendment 114

Proposal for a regulation
Article 31 – paragraph 1 – point d – point iv – indent 1

Text proposed by the Commission	*Amendment*
— the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country;	— the envisaged sub-contractor is an ICT third-party service provider or an ICT sub-contractor established in a third country ***and does not have a legal entity in the Union***;

Or. en

Amendment 115

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***.	2. ***Before finalising and issuing recommendations in accordance with point (d) of paragraph 1, the Joint Oversight Executive Body*** shall consult the ***critical ICT third-party service provider on its intentions and give an opportunity for the ICT third-party service provider to provide information which it reasonably believes should be taken into account*** before ***the recommendation is finalised or in order to challenge the intended recommendations. Grounds for challenging a recommendation may include that there would be a disproportionate impact on or disruption for customers not subject to this Regulation, or that there is a more effective or efficient solution for managing the identified risk***.

Or. en

Amendment 116

Proposal for a regulation
Article 31 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Critical ICT third-party service providers shall cooperate in good faith with the ***Lead Overseer*** and assist the ***Lead Overseer*** in the fulfilment of its tasks.	3. Critical ICT third-party service providers shall cooperate in good faith with the ***Joint Oversight Executive Body*** and assist the ***Joint Oversight Executive Body*** in the fulfilment of its tasks.

Or. en

Amendment 117

Proposal for a regulation
Article 31 – paragraph 4

Text proposed by the Commission	*Amendment*
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.	4. The ***Joint Oversight Executive Body*** 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.

Or. en

Amendment 118

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 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.	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 ***or, if inspections and access are in a third-country jurisdiction, the enforcement shall be governed by the rules of civil procedure of the Member State in which the critical ICT third-party service provider has its legal entity***. 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.

Or. en

Amendment 119

Proposal for a regulation
Article 31 – paragraph 9

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

Or. en

Amendment 120

Proposal for a regulation
Article 32 – paragraph 1

Text proposed by the Commission	*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.	1. The ***Joint Oversight Executive Body*** may by simple request or by decision require the critical ICT third-party ***service*** providers to provide all information that is necessary for the ***Joint Oversight Executive Body*** to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies documentation, ICT security audit reports, ***major*** ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party ***service*** provider has outsourced operational functions or activities. ***For the purpose of the first subparagraph, when the Joint Oversight Executive Body requests information concerning customers of critical ICT third-party service providers that are not the subject of this Regulation, the ICT third-party service provider may redact the information as necessary to protect the confidentiality of its customers.***

Or. en

Amendment 121

Proposal for a regulation
Article 32 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. When sending a simple request for information under paragraph 1, the ***Lead Overseer*** shall:	2. When sending a simple request for information under paragraph 1, the ***Joint Oversight Executive Body*** shall:

Or. en

Amendment 122

Proposal for a regulation
Article 32 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. When requiring to supply information under paragraph 1, the ***Lead Overseer*** shall:	3. When requiring ***by decision*** to supply information under paragraph 1, the ***Joint Oversight Executive Body*** shall:

Or. en

Amendment 123

Proposal for a regulation
Article 32 – paragraph 5

Text proposed by the Commission	*Amendment*
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.	5. The ***Joint Oversight Executive Body*** 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 ***service*** providers' services. ***If the information specified under point (c) of paragraph 3 pertains to a financial entity, that financial entity shall be notified of the decision for a request by the Joint Oversight Executive Body.***

Or. en

Amendment 124

Proposal for a regulation
Article 33 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to carry out its duties under this Regulation, the ***Lead Overseer***, assisted by the examination team referred to in Article ***34(1)***, may conduct the	1. In order to carry out its duties under this Regulation, the ***Joint Oversight Executive Body***, assisted by the examination team referred to in Article

necessary investigations of ICT third-party service providers*:*	***35(1)***, may conduct the necessary investigations of ICT third-party service providers***. When conducting the investigation, the Joint Oversight Executive Body and examination team shall exercise caution and ensure that the rights of the critical ICT third-party service provider that are not the subject of this Regulation are protected, including in relation to the impact on service levels, availability of data and confidentiality.***

Or. en

Amendment 125

Proposal for a regulation
Article 33 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The ***Lead Overseer*** shall be empowered to:	2. The ***Joint Oversight Executive Body*** shall be empowered to:

Or. en

Amendment 126

Proposal for a regulation
Article 33 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. The officials and other persons authorised by the ***Lead Overseer*** for the purposes of the investigation referred to in paragraph 1 shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the investigation.	3. The officials and other persons authorised by the ***Joint Oversight Executive Body*** for the purposes of the investigation referred to in paragraph 1 shall exercise their powers upon production of a written authorisation specifying the subject matter and purpose of the investigation.

Or. en

Amendment 127

Proposal for a regulation
Article 33 – paragraph 4

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

Or. en

Amendment 128

Proposal for a regulation
Article 33 – paragraph 5

Text proposed by the Commission	*Amendment*
5. In good time before the investigation, ***Lead Overseers*** shall inform competent authorities of the financial entities using that ICT third-party service provider of the investigation and of the identity of the authorised persons.	5. In good time before the investigation, ***Joint Oversight Executive Body*** shall inform competent authorities of the financial entities using that ICT third-party service provider of the investigation and of the identity of the authorised persons.

Or. en

Amendment 129

Proposal for a regulation
Article 34 – paragraph 1

Text proposed by the Commission	*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, such as head offices, operation centres, secondary premises, as well as to conduct off-line inspections.	1. In order to carry out its duties under this Regulation, the ***Joint Oversight Executive Body***, 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 ***service*** providers, such as head offices, operation centres, secondary premises, as well as to conduct off-line inspections. ***The power to conduct on-site inspections shall not be limited to sites in the Union, provided that the inspection of the site in a third country is necessary for the Joint Oversight Executive Body to carry out its duties under this Regulation and that the site has a direct connection to the provision of ICT services to Union financial entities.***

Or. en

Amendment 130

Proposal for a regulation
Article 34 – paragraph 2 – introductory part

Text proposed by the Commission	*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.	2. The officials and other persons authorised by the ***Joint Oversight Executive Body*** 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.

Or. en

Amendment 131

Proposal for a regulation
Article 34 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. When performing an on-site inspection, the Joint Oversight Executive Body through the examination team shall exercise caution and ensure that the rights of customers of critical ICT third-party service providers that are not the subject of this Regulation are protected, including in relation to the impact on service levels, availability of data and confidentiality.

Or. en

Amendment 132

Proposal for a regulation
Article 34 – paragraph 3

Text proposed by the Commission	*Amendment*
3. In good time before the inspection, ***Lead Overseers*** shall inform the competent authorities of the financial entities using that ICT third-party provider.	3. In good time before the inspection, ***Joint Oversight Executive Body*** shall inform the competent authorities of the financial entities using that ICT third-party ***service*** provider.

Or. en

Amendment 133

Proposal for a regulation
Article 34 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Before any planned on-site visit, ***Lead Overseers*** shall give a reasonable notice to the critical ICT third-party service	5. Before any planned on-site visit, ***Joint Oversight Executive Body*** shall give a reasonable notice to the critical ICT

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.

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.

Or. en

Amendment 134

Proposal for a regulation
Article 34 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The critical ICT third-party service provider shall submit to on-site inspections ordered by decision of the ***Lead Overseer***. The decision shall specify the subject matter and purpose of the inspection, appoint the date on which it is to begin and indicate the periodic penalty payments provided for in Article 31(4), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, as well as the right to have the decision reviewed by the Court of Justice.	6. The critical ICT third-party service provider shall submit to on-site inspections ordered by decision of the ***Joint Oversight Executive Body***. The decision shall specify the subject matter and purpose of the inspection, appoint the date on which it is to begin and indicate the periodic penalty payments provided for in Article 31(4), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, as well as the right to have the decision reviewed by the Court of Justice.

Or. en

Amendment 135

Proposal for a regulation
Article 34 – paragraph 7

Text proposed by the Commission	*Amendment*
7. Where the officials and other persons authorised by the ***Lead Overseer*** find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the ***Lead Overseer*** shall inform the critical ICT provider of the consequences of such opposition, including	7. Where the officials and other persons authorised by the ***Joint Oversight Executive Body*** find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the ***Joint Oversight Executive Body*** shall inform the critical ICT ***third-party service***

the possibility for competent authorities of the relevant financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

Or. en

Amendment 136

Proposal for a regulation
Article 35 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where conducting general investigations or on-site inspections, the ***Lead Overseers*** shall be assisted by an examination team established for each critical ICT third-party service provider.	1. Where conducting general investigations or on-site inspections, the ***Joint Oversight Executive Body*** shall be assisted by an examination team established for each critical ICT third-party service provider.

Or. en

Amendment 137

Proposal for a regulation
Article 35 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The ***joint*** examination team referred to in paragraph 1 shall be composed ***of*** staff members from ***the Lead Overseer*** and from the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides services, who will join the preparation and execution of the Oversight activities, with a maximum of 10 members. All members of the ***joint*** examination shall have expertise in ICT and operational risk. The ***joint*** examination	2. The examination team referred to in paragraph 1 shall be composed ***dedicated*** staff members from ***across the ESAs*** and from the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides services, who will join the preparation and execution of the Oversight activities, with a maximum of 10 members. All members of the examination ***team*** shall have expertise in ICT and operational risk. The examination team shall work under the

team shall work under the coordination of a designated ESA staff member ***(the 'Lead Overseer coordinator')***.

coordination of a designated ESA staff member.

Or. en

Amendment 138

Proposal for a regulation
Article 35 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. The ESAs, through the Joint ***Committee***, shall develop common draft regulatory technical standards to specify further the designation of the members of the ***joint*** examination team coming from the relevant competent authorities, as well as the tasks and working arrangements of the examination team. The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force].	3. The ESAs, through the Joint ***Oversight Executive Body***, shall develop common draft regulatory technical standards to specify further the designation of the members of the examination team coming from the relevant competent authorities, as well as the tasks and working arrangements of the examination team. The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force].

Or. en

Amendment 139

Proposal for a regulation
Article 35 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Within 3 months after the completion of an investigation or on-site inspection, the ***Lead Overseer, after consultation of the*** Oversight ***Forum***, shall adopt recommendations ***to be*** addressed ***by the Lead Overseer*** to the critical ICT third-party service provider pursuant to the powers referred to in Article 31.	4. Within 3 months after the completion of an investigation or on-site inspection, the ***Joint*** Oversight ***Executive Body***, shall adopt recommendations addressed to the critical ICT third-party service provider pursuant to the powers referred to in Article 31. ***Critical ICT third-party service providers shall be afforded the opportunity to***

provide information or challenge the intended recommendation prior to its adoption in accordance with Article 31(2).

Or. en

Amendment 140

Proposal for a regulation
Article 35 – paragraph 5 – subparagraph 1

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

Or. en

Amendment 141

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

Text proposed by the Commission	*Amendment*
(d) the details of the ***competent authorities'*** assessment of measures taken by critical ICT third-party service providers based on the recommendations of ***Lead Overseers*** pursuant to Article 37(2).	(d) the details of the assessment of measures taken by critical ICT third-party service providers based on the recommendations of ***the Joint Oversight Executive Body*** pursuant to Article 37(2).

Or. en

Amendment 142

Proposal for a regulation
Article 37 – title

Text proposed by the Commission	*Amendment*
Follow-up ***by*** competent authorities	Follow-up ***and enforcement by the Joint Oversight Executive Body and*** competent authorities

Or. en

Amendment 143

Proposal for a regulation
Article 37 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	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 Lead Overseer whether they intend to follow those recommendations. ***The Joint Oversight Executive Body*** shall immediately transmit this information to competent authorities.

Or. en

Amendment 144

Proposal for a regulation
Article 37 – paragraph 2

Text proposed by the Commission	*Amendment*
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).	2. Competent authorities shall monitor whether financial entities take into account the risks identified in the recommendations addressed to critical ICT third-party ***service*** providers by the ***Joint Oversight Executive Body*** in accordance with points (d) of Article 31(1).

Or. en

Amendment 145

Proposal for a regulation
Article 37 – paragraph 3

Text proposed by the Commission	*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***.	3. ***The Joint Oversight Executive Body*** may, in accordance with Article***s 28 and 44, and after consultation with the competent authorities of the affected*** financial entities***, require the critical ICT third-party service providers*** to temporarily suspend, either in part or completely, the use or deployment of a service provided ***to financial entity customers exposed to*** the risks identified in the recommendations addressed to 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***.

Or. en

Amendment 146

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 taking ***those*** decisions***, 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:

Or. en

Amendment 147

Proposal for a regulation
Article 37 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. The decisions provided for in paragraph 3 shall only be implemented once all affected financial entity customers have been duly informed. The affected financial entity customers shall be afforded at least 30 calendar days to conclude and operationalise alternative arrangements, and to execute their exit strategies and transition plans referred to in Article 25.
	The critical ICT third-party service providers subject to the decisions provided for in paragraph 3 of this Article, shall fully cooperate with their financial entity customers.

Or. en

Amendment 148

Proposal for a regulation
Article 37 – paragraph 5

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

Or. en

Amendment 149

Proposal for a regulation
Article 38 – paragraph 1 – subparagraph 1

Text proposed by the Commission	*Amendment*
The amount of a fee charged to a critical ICT third-party service provider shall cover all ***administrative*** costs and shall be proportionate to their turnover.	The amount of a fee charged to a critical ICT third-party service provider shall cover all costs ***derived from the execution of the duties foreseen in this Chapter*** and shall be proportionate to their turnover.

Or. en

Amendment 150

Proposal for a regulation
Article 39 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. If an administrative arrangement is with a third-country regulatory and supervisory authority in accordance with paragraph 1 of this Article, that authority may form part of the examination team referred to in Article 35(1).

Or. en

Amendment 151

Proposal for a regulation
Article 43 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB and the ESRB, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance	1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB***, the SRB for information relating to entities falling under the scope of Regulation (EU) No 806/2014*** and the ESRB, may establish

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

Or. en

Amendment 152

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.	2. Competent authorities, EBA, ESMA or EIOPA, ***the ECB,*** and the ***SRB*** 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.

Or. en

Amendment 153

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.	1. ***The Joint Oversight Executive Body and*** competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.

Or. en

Amendment 154

Proposal for a regulation
Article 44 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The powers referred to in paragraph 1 shall include at least the powers to:	2. ***For the purpose of the oversight of critical ICT third-party service providers, the Joint Oversight Executive Body and relevant competent authorities,*** the powers referred to in paragraph 1 shall include at least the powers to:

Or. en

Amendment 155

Proposal for a regulation
Article 44 – paragraph 4 – introductory part

Text proposed by the Commission	*Amendment*
4. ***Member States shall confer on*** competent authorities ***the power*** to apply at least the following administrative penalties or remedial measures for breaches of this Regulation:	4. ***Powers are conferred on the Joint Oversight Executive Body and on relevant*** competent authorities to apply at least the following administrative penalties or remedial measures for breaches of this Regulation:

Or. en

Amendment 156

Proposal for a regulation
Article 50 – paragraph 6

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

period of ***two*** months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by ***two*** months at the initiative of the European Parliament or of the Council.	period of ***three*** months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by ***three*** months at the initiative of the European Parliament or of the Council.

Or. en

EXPLANATORY STATEMENT

The rapporteur welcomes the Commission's proposal for a Digital Operational Resilience Act, as a necessary step to strengthen and harmonise the regulatory framework in this area. The proposal is a robust, ambitious, and timely initiative for a sector becoming increasingly digitalised and intertwined with ICT third-party providers (ICT TPP).

Nonetheless, the rapporteur has identified certain aspects of the proposal for improvement. The amendments included in the present report are guided by three main principles:

1. Proportionality - the scope of and obligations imposed by the Regulation should be proportionate to the ICT risk posed to an entity and should not discourage the continuing digitalisation of the EU's financial services sector.

2. Preserving competitiveness - it is necessary to ensure that the digital operational resilience framework does not hinder the competitiveness of entities falling within scope or the attractiveness of the EU, which should position itself as a key player on the digital stage, while remaining open to collaborate with international partners.

3. Futureproof - the framework must have the necessary flexibility to address new services and business models that might emerge in the near future and must not hamper innovation.

Besides their attachment to the abovementioned principles, the amendments to the Commission proposal can be classified into the following groups:

Proportionality & scope

The draft report introduces amendments relating to the proportionality and scope, with the objective of keeping the scope of the Regulation limited to relevant companies exposed to ICT risks, while also ensuring a risk-based approach.

In order to achieve that objective, certain changes to the personal scope are introduced. Small and medium-sized insurance and reinsurance undertakings (as well as intermediaries) are excluded from the scope of the proposal, with the exception of those that rely on systematised insurance intermediation. Small and medium-sized audit firms and statutory auditors are also excluded from the scope of the Regulation. Finally, ICT intra-group service providers will fall under the scope of the Regulation with the exception of the Chapter V oversight framework.

On definitions, 'ICT risk' and 'ICT services have been simplified in order to ensure the Regulation is flexible enough to cope with the short-term evolution of ICT services. Other changes have been included to definitions so as to make them broader and more complete, such as confirming that the term 'critical or important functions' also covers critical functions as defined by BRRD, or the addition of a definition for ICT intra-group service providers.

Changes reflected in AMs 2, 10, 22-32.

ICT risk reporting

The rapporteur is overall supportive of the ICT risk-reporting regime as proposed by the Commission but has made targeted amendments, particularly on reporting requirements and the authorities involved. The criteria for determining major ICT-related incidents has been aligned with the requirements for assessing the significance of incidents under the NIS Directive.

The list of authorities that should be informed by the competent authority after receiving the report on the major ICT related incident has been modified. The SRB should be informed in the cases where the financial entity affected falls under the scope of the SRM Regulation, whereas the CSIRTs should be updated if the entities affected fall under the scope of the NIS Directive.

Changes reflected in AMs 1, 55-59.

Testing

Some targeted amendments have been tabled in order to introduce more flexibility to the framework for ICT tools testing (Chapter IV). Additionally, Article 23 has been amended in respect of ICT TPP involvement in threat led penetration testing. When the involvement of a given ICT TPP could affect the quality of the service provided to other customers, the ICT TPP will have the possibility (under certain conditions) of arranging pooled testing on behalf of all its financial entity customers. In that case, the documentation confirming that the threat led penetration testing has been conducted will be submitted to the Joint Oversight Executive Committee to be validated.

Changes reflected in AMs 7, 60-68.

ICT risk management framework

The framework has been amended to introduce more proportionality and a strengthened risk-based approach. The risk profile of financial entities has been included as an important element to be considered when building digital operational resilience.

In order to limit the extent of the burden borne by financial entities, the obligation to classify and adequately document all ICT related functions in Article 7 has been limited to critical or important functions. Moreover, the obligation to record all ICT-related incidents has been nuanced, and financial entities will only have to record them in cases when they are related to the continued provision and quality of financial services.

Small changes to the framework for ICT-related incident reviews and monitoring the effectiveness of digital resilience strategies have also been made, with the objective of further defining their scope and ensuring they are focused on risk and their potential impact on critical or important functions.

Changes reflected in AMs 3-6, 33-54.

Sound management of ICT third-party risk

In this area, the scope of certain requirements has been narrowed to introduce more proportionality. The obligation to maintain and update a Register of Information in relation to all contractual arrangements has been limited to the provision of critical or important functions. Similarly, some of the elements that had to be included in the contractual arrangements under Article 27(2), such as notice periods and reporting obligations or the right to monitor the ICT TPP's performance, have been moved to a new paragraph (2a) and will only be applicable to arrangements for the provision of critical or important functions.

Furthermore, termination of contractual arrangements with ICT TPPs will only be possible when all other possible remedies have been exhausted.

The introduction of certain requirements for the contractual arrangements for the provision of ICT services by an ICT TPP established in a third-country have also been proposed to ensure sufficient oversight can be exercised.

Changes reflected in AMs 9-10, 12, 69-87.

Oversight framework for critical TPPs

The report's objective is to enhance and simplify the oversight, while also improving the dialogue between oversight bodies, financial entities and critical ICT TPPs as a way to balance competing perspectives whilst drawing on the expertise of each party. Such an approach would give due consideration to the fact that financial supervisors have the best understanding of the potential risks; while critical ICT TPPs are likely to have leading expertise in their field and a consideration for the impact of any measures on their customers not subject to this Regulation.

The roles of the Oversight Forum and Lead Overseer have been assumed by a single Joint Oversight Executive Body, in charge of day to day oversight of critical ICT TPPs. The Joint Oversight Executive Body has assumed the role of the Oversight Forum, in that it will prepare the draft joint positions, decisions, recommendations and common other acts, including the determination of criticality, and the drafting of the annual oversight plan. One of the ESAs will be appointed as responsible for legally adopting the recommendations and decisions for each ICT TPP.

The enhanced dialogue will allow ICT TPPs to review and comment upon, prior to final adoption, their designation as critical, their oversight plan, and any recommendations issued following an inspection.

The majority of the powers conferred on the Joint Oversight Executive Body, including those to conduct onsite inspections, have been maintained. However, certain safeguards have been put in place to ensure the confidentiality of and minimal disruption to customers not subject to this Regulation.

The ability for financial entities to engage the services of third-country critical ICT TPPs has been clarified. Such arrangements would be permitted provided the third-country ICT TPP has a legal entity in the EU and the ICT TPP and financial entity have concluded contractual

agreements provisions in accordance with Article 27(2b). The purpose of this legal entity would be, inter alia, a point of contact for the oversight framework, an entity with which the oversight framework would engage and issue any recommendations, and finally as a point of access to the infrastructure located in the third-country.

Oversight fees charged to ICT TPPs will have to cover all costs derived from the execution of the duties foreseen in the present chapter, and not only administrative costs.

Changes reflected in AMs 8, 11, 13-20, 88-150.

Competent authorities

The SRB has been added as a competent authority for both financial cross-sector exercises and cooperation under Article 43. The Joint Oversight Executive Body has also been entitled with supervisory, investigatory and sanctioning powers, whereas competent authorities under Chapter VII would keep that attribution as well.

Changes reflected in AMs 21, 151-155.

Interaction with existing financial services and cyber security frameworks

As one of the main objectives of this report is to ensure consistency with the existing frameworks for cyber security and financial services, certain tweaks have been introduced in order to maintain alignment with the NIS Directive and its ongoing review. Changes on the definition of 'ICT risk' and the criteria to determine which are major ICT related incidents are good examples of this. Besides that, the definition of 'critical or important functions' has also been amended to align it with BRRD.

Lastly, the report has been prepared in close contact with the rapporteur of the Directive on the oversight framework on service providers in order to keep both reports as much aligned as possible.

Changes reflected in AMs 10, 27, 31, 55.

Delegations:

One new delegation has been introduced in order to set the threshold for reporting costs and losses caused by major ICT disruptions and ICT-related incidents. The deadline for the Parliament to object to delegated acts has been extended to three months following the notification.

Changes reflected in AMs 45-46, 156.