Council of the European Union

Brussels, 17 January 2022
(OR. en)

5297/22

Interinstitutional File:
2020/0266 (COD)

EF 9
ECOFIN 37
TELECOM 10
CYBER 13
CODEC 38

COVER NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	DORA Regulation - Three-column table to commence trilogues

Delegations will find attached the three-column table on the above-mentioned draft Regulation.

Encl.

Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

(Text with EEA relevance)

2020/0266(COD)

[3 CT: Commission Proposal, EP Mandate and Council Mandate]

	Commission Proposal	EP Mandate	Council Mandate
Formula			
1	2020/0266 (COD)	2020/0266 (COD)	2020/0266 (COD)
Proposal Title			
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (Text with EEA relevance)
Formula			
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Citation 1			
4			

	Commission Proposal	EP Mandate	Council Mandate
	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Citation 2			
5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,
Citation 3			
6	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,
Citation 4			
7	Having regard to the opinion of the European Central Bank,[1] _____ 1. [add reference] OJ C , , p. .	Having regard to the opinion of the European Central Bank~~,~~[1]**.** _____ 1. [add reference] OJ C , , p. .	Having regard to the opinion of the European Central Bank,[1] _____ 1. [add reference] OJ C , , p. .
Citation 5			
8	Having regard to the opinion of the European Economic and Social Committee,[1] _____ 1. [add reference] OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee~~,~~[1]**.** _____ 1. [add reference] OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee~~,~~[1]**,** _____ 1. [add reference] OJ C , , p. .
Citation 6			
9	Acting in accordance with the ordinary	Acting in accordance with the ordinary	Acting in accordance with the ordinary

	Commission Proposal	EP Mandate	Council Mandate
	legislative procedure,	legislative procedure,	legislative procedure,
Formula			
10	Whereas:	Whereas:	Whereas:
Recital 1			
11	(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are nowadays core features of all activities of Union financial entities, digital resilience is not yet sufficiently built in their operational frameworks.	(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are nowadays core features of all activities of Union financial entities, digital resilience ~~*is not yet*~~***has yet to be*** sufficiently built in their operational frameworks.	(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalisation and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are nowadays core features of all activities of Union financial entities, digital resilience is not ~~yet~~ sufficiently built in their operational frameworks **yet**.
Recital 2			
12	(2) The use of ICT has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments,	(2) The use of ICT has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments,	(2) The use of ICT has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments,

	Commission Proposal	EP Mandate	Council Mandate
	which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, insurance underwriting, claim management and back-office operations. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.	which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, ~~insurance underwriting,~~ claim management and back-office operations***. The insurance sector has also been transformed by the use of ICT, from the emergence of digital insurance intermediaries operating with InsurTech, to digital insurance underwriting and contract distribution***. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.	which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, insurance underwriting, claim management and back-office operations. Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers.
Recital 3			
13	(3) The European Systemic Risk Board (ESRB) has reaffirmed in a 2020 report addressing systemic cyber risk[1] how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities[2] to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches occurring in finance do	(3) The European Systemic Risk Board (ESRB) has reaffirmed in a 2020 report addressing systemic cyber risk[1] how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities[2] to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches occurring in finance do	(3) The European Systemic Risk Board (ESRB) has reaffirmed in a 2020 report addressing systemic cyber risk[1] how the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, and particularly the interdependencies of their ICT systems, may potentially constitute a systemic vulnerability since localised cyber incidents could quickly spread from any of the approximately 22 000 Union financial entities[2] to the entire financial system, unhindered by geographical boundaries. Serious ICT breaches occurring in finance do

	Commission Proposal	EP Mandate	Council Mandate
	not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union’s financial system, generating liquidity runs and an overall loss of confidence and trust in financial markets. __________ 1. ESRB report Systemic Cyber Risk from February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf. 2. According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are around 5,665 credit institutions, 5,934 investment firms, 2,666 insurance undertakings, 1,573 IORPS, 2,500 investment management companies, 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs), 45 CRAs and 2,500 authorised payment institutions and electronic money institutions. This sums up to approx. 21.233 entities and does not include crowd funding entities, statutory auditors and audit firms, crypto assets service providers and benchmark administrators.	not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union’s financial system, generating liquidity runs and an overall loss of confidence and trust in financial markets. __________ 1. ESRB report Systemic Cyber Risk from February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf. 2. According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are around 5,665 credit institutions, 5,934 investment firms, 2,666 insurance undertakings, 1,573 IORPS, 2,500 investment management companies, 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs), 45 CRAs and 2,500 authorised payment institutions and electronic money institutions. This sums up to approx. 21.233 entities and does not include crowd funding entities, statutory auditors and audit firms, crypto assets service providers and benchmark administrators.	not merely affect financial entities taken in isolation. They also smooth the way for the propagation of localised vulnerabilities across the financial transmission channels and potentially trigger adverse consequences for the stability of the Union’s financial system, generating liquidity runs and an overall loss of confidence and trust in financial markets. __________ 1. ESRB report Systemic Cyber Risk from February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf. 2. According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are around 5,665 credit institutions, 5,934 investment firms, 2,666 insurance undertakings, 1,573 IORPS, 2,500 investment management companies, 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs), 45 CRAs and 2,500 authorised payment institutions and electronic money institutions. This sums up to approx. 21.233 entities and does not include crowd funding entities, ~~statutory auditors and audit firms,~~ crypto assets service providers and benchmark administrators.
Recital 4			
14	(4) In recent years, ICT risks have attracted the attention of national, European and international policy makers, regulators and standard-setting bodies in an attempt to enhance resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Markets Infrastructures, the Financial Stability Board,	(4) In recent years, ICT risks have attracted the attention of national, European and international policy makers, regulators and standard-setting bodies in an attempt to enhance resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Markets Infrastructures, the Financial Stability Board,	(4) In recent years, ICT risks have attracted the attention of national, European and international policy makers, regulators and standard-setting bodies in an attempt to enhance resilience, set standards and coordinate regulatory or supervisory work. At international level, the Basel Committee on Banking Supervision, the Committee on Payments and Markets Infrastructures, the Financial Stability Board,

	Commission Proposal	EP Mandate	Council Mandate
	the Financial Stability Institute, as well as the G7 and G20 groups of countries aim to provide competent authorities and market operators across different jurisdictions with tools to bolster the resilience of their financial systems.	the Financial Stability Institute, as well as the G7 and G20 groups of countries aim to provide competent authorities and market operators across different jurisdictions with tools to bolster the resilience of their financial systems. ***Consequently, it is necessary to consider ICT risk in the context of a highly interconnected global financial system in which the consistency of international regulation and cooperation between competent authorities globally needs to be prioritised.***	the Financial Stability Institute, as well as the G7 and G20 groups of countries aim to provide competent authorities and market operators across different jurisdictions with tools to bolster the resilience of their financial systems.
Recital 5			
15	(5) Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed at safeguarding the Union's competitiveness and stability from economic, prudential and market conduct perspectives. Though ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-crisis regulatory agenda, and have only developed in some areas of the Union's financial services policy and regulatory landscape, or only in a few Member States.	(5) Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed at safeguarding the Union's competitiveness and stability from economic, prudential and market conduct perspectives. Though ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-crisis regulatory agenda, and have only developed in some areas of the Union's financial services policy and regulatory landscape, or only in a few Member States.	(5) Despite national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and stability of the Union financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the Union financial sector and aimed at safeguarding the Union's competitiveness and stability from economic, prudential and market conduct perspectives. Though ICT security and digital resilience are part of operational risk, they have been less in the focus of the post-crisis regulatory agenda, and have only developed in some areas of the Union's financial services policy and regulatory landscape, or only in a few Member States.
Recital 6			

	Commission Proposal	EP Mandate	Council Mandate
16	(6) The Commission’s 2018 Fintech action plan[1] highlighted the paramount importance of making the Union financial sector more resilient also from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling financial services to be effectively and smoothly delivered across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence. __________ 1. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.	(6) The Commission’s 2018 Fintech action plan[1] highlighted the paramount importance of making the Union financial sector more resilient also from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling financial services to be effectively and smoothly delivered across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence. __________ 1. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.	(6) The Commission’s 2018 Fintech action plan[1] highlighted the paramount importance of making the Union financial sector more resilient also from an operational perspective to ensure its technological safety and good functioning, its quick recovery from ICT breaches and incidents, ultimately enabling financial services to be effectively and smoothly delivered across the whole Union, including under situations of stress, while also preserving consumer and market trust and confidence. __________ 1. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.
Recital 7			
17	(7) In April 2019, the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) (jointly called “European Supervisory Authorities” or “ESAs”) jointly issued two pieces of technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a Union sector-specific initiative.	(7) In April 2019, the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) (jointly called “European Supervisory Authorities” or “ESAs”) jointly issued two pieces of technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a Union sector-specific initiative.	(7) In April 2019, the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) (jointly called “European Supervisory Authorities” or “ESAs”) jointly issued two pieces of technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through a Union sector-specific initiative.

	Commission Proposal	EP Mandate	Council Mandate
Recital 8			
18	(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than for example common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this component, by enlarging the mandates of financial supervisors tasked to monitor and protect financial stability and market integrity.	(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than for example common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this component, by ~~*enlarging*~~***strengthening*** the mandates of financial supervisors ~~*tasked to monitor and protect*~~***to manage ICT risks in the*** financial ~~*stability and*~~ ***sector, to protect the integrity and efficiency of the single*** market***, and to facilitate its orderly functioning*** ~~*integrity*~~.	(8) The Union financial sector is regulated by a harmonised Single Rulebook and governed by a European system of financial supervision. Nonetheless, provisions tackling digital operational resilience and ICT security are not fully or consistently harmonised yet, despite digital operational resilience being vital for ensuring financial stability and market integrity in the digital age, and no less important than for example common prudential or market conduct standards. The Single Rulebook and system of supervision should therefore be developed to also cover this component, by enlarging the mandates of financial supervisors tasked to monitor and protect financial stability and market integrity.
Recital 9			
19	(9) Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities operating in	(9) Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities operating in	(9) Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities

	Commission Proposal	EP Mandate	Council Mandate
	different Member States may equally be distorted. Notably for areas where Union harmonisation has been very limited - such as the digital operational resilience testing - or absent - such as the monitoring of ICT third-party risk - disparities stemming from envisaged developments at national level could generate further obstacles to the functioning of the single market to the detriment of market participants and financial stability.	different Member States may equally be distorted. Notably for areas where Union harmonisation has been very limited - such as the digital operational resilience testing - or absent - such as the monitoring of ICT third-party risk - disparities stemming from envisaged developments at national level could generate further obstacles to the functioning of the single market to the detriment of market participants and financial stability.	operating in different Member States may equally be distorted. Notably for areas where Union harmonisation has been very limited - such as the digital operational resilience testing - or absent - such as the monitoring of ICT third-party risk - disparities stemming from envisaged developments at national level could generate further obstacles to the functioning of the single market to the detriment of market participants and financial stability.
Recital 10			
20	(10) The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user like finance since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, every single one issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risks and mitigating adverse	(10) The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user like finance since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, every single one issued by a different competent authority in one or several Member States) face operational challenges in addressing ICT risks and mitigating adverse	(10) The partial way in which the ICT-risk related provisions have until now been addressed at Union level shows gaps or overlaps in important areas, such as ICT-related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user ~~like finance~~**such as the financial sector** since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union. Individual financial entities operating on a cross-border basis or holding several authorisations (e.g. one financial entity can have a banking, an investment firm, and a payment institution licence, every single one issued by a different competent authority in one or several

	Commission Proposal	EP Mandate	Council Mandate
	impacts of ICT incidents on their own and in a coherent cost-effective way.	impacts of ICT incidents on their own and in a coherent cost-effective way.	Member States) face operational challenges in addressing ICT risks and mitigating adverse impacts of ICT incidents on their own and in a coherent cost-effective way.
Recital 10a			
20a		***(10a) Establishing and maintaining adequate network and information system infrastructures is also a fundamental precondition for effective risk data aggregation and risk reporting practices, which are in turn an essential requisite for the sound and sustainable risk management and decision-making processes of credit institutions. In 2013, the Basel Committee on Banking Supervision (BCBS) published a set of principles for effective risk data aggregation and risk reporting (BCBS 239) based on two overarching principles of governance and IT infrastructure, to be implemented by the beginning of 2016. In accordance with the Report of the European Central Bank (ECB) of May 2018 on the Thematic Review on effective risk data aggregation and risk reporting of May 2018 and the BCBS Progress Report of April 2020, the implementation progress made by global systemically important banks was unsatisfactory and a source of concern. In order to facilitate compliance and alignment with international standards, the Commission, in close cooperation with the ECB and after consulting EBA and ESRB, should produce a report in***	

	Commission Proposal	EP Mandate	Council Mandate
		order to assess how the BCBS 239 principles interact with the provisions of this Regulation and, if appropriate, how those principles should be incorporated into Union law.	
Recital 11			
21	(11) As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework further harmonisation of key digital operational resilience requirements for all financial entities is required. The capabilities and overall resilience which financial entities, based on such key requirements, would develop with a view to withstand operational outages, would help preserving the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims at contributing to the smooth functioning of the single market it should be based on the provisions of Article 114 TFEU as interpreted in accordance with the consistent case law of the Court of Justice of the European Union.	(11) As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework further harmonisation of key digital operational resilience requirements for all financial entities is required. The capabilities and overall resilience which financial entities, based on such key requirements, would develop with a view to withstand operational outages, would help preserving the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims at contributing to the smooth functioning of the single market it should be based on the provisions of Article 114 TFEU as interpreted in accordance with the consistent case law of the Court of Justice of the European Union.	(11) As the Single Rulebook has not been accompanied by a comprehensive ICT or operational risk framework**,** further harmonisation of key digital operational resilience requirements for all financial entities is required. The capabilities and overall resilience which financial entities, based on such key requirements, would develop with a view to withstand operational outages, would help preserving the stability and integrity of the Union financial markets and thus contribute to ensuring a high level of protection of investors and consumers in the Union. Since this Regulation aims at contributing to the smooth functioning of the single market it should be based on the provisions of Article 114 TFEU as interpreted in accordance with the consistent case law of the Court of Justice of the European Union.
Recital 12			
22	(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements addressed so far separately in the different Regulations and Directives. While those Union	(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements addressed so far separately in the different Regulations and Directives. While those Union	(12) This Regulation aims first at consolidating and upgrading the ICT risk requirements **as part of the operational risk requirements** addressed so far separately in the different

	Commission Proposal	EP Mandate	Council Mandate
	legal acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they could not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk requirements, when further developed in these Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through requirements aiming at the protection, detection, containment, recovery and repair capabilities against ICT-related incidents or through setting out reporting and digital testing capabilities. Those Directives and Regulations were primarily meant to cover essential rules on prudential supervision, market integrity or conduct. Through this exercise, which consolidates and updates rules on ICT risk, all provisions addressing digital risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This initiative should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via targeted rules on ICT risk management capabilities, reporting and testing and third party risk monitoring.	legal acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they could not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk requirements, when further developed in these Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through requirements aiming at the protection, detection, containment, recovery and repair capabilities against ICT-related incidents or through setting out reporting and digital testing capabilities. Those Directives and Regulations were primarily meant to cover essential rules on prudential supervision, market integrity or conduct. Through this exercise, which consolidates and updates rules on ICT risk, all provisions addressing digital risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This initiative should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via targeted rules on ICT risk management capabilities, reporting and testing and third party risk monitoring. ***This initiative also intends to raise awareness of ICT risks and acknowledges that ICT***	Regulations and Directives. While those Union legal acts covered the main categories of financial risk (e.g. credit risk, market risk, counterparty credit risk and liquidity risk, market conduct risk), they could not comprehensively tackle, at the time of their adoption, all components of operational resilience. The operational risk requirements, when further developed in these Union legal acts, often favoured a traditional quantitative approach to addressing risk (namely setting a capital requirement to cover ICT risks) rather than enshrining targeted qualitative requirements to boost capabilities through requirements aiming at the protection, detection, containment, recovery and repair capabilities against ICT-related incidents or through setting out reporting and digital testing capabilities. Those Directives and Regulations were primarily meant to cover essential rules on prudential supervision, market integrity or conduct. Through this exercise, which consolidates and updates rules on ICT risk, all provisions addressing digital risk in finance would for the first time be brought together in a consistent manner in a single legislative act. This initiative should thus fill in the gaps or remedy inconsistencies in some of those legal acts, including in relation to the terminology used therein, and should explicitly refer to ICT risk via– targeted rules on ICT risk management capabilities, **incident** reporting**, operational resilience** ~~and~~ testing and third party risk

	Commission Proposal	EP Mandate	Council Mandate
		incidents and a lack of operational resilience might jeopardise the financial soundness of financial entities.	monitoring.
Recital 13			
23	(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of overuse of ICT systems, platforms and infrastructures, which entails increased digital risk. The respect of a basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.	(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk ***according to their size, nature, complexity and risk profile***. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of ~~overuse of~~***high reliance on*** ICT systems, platforms and infrastructures, which entails increased digital risk. The respect of a basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.	(13) Financial entities should follow the same approach and the same principle-based rules when addressing ICT risk. Consistency contributes to enhancing confidence in the financial system and preserving its stability especially in times of overuse of ICT systems, platforms and infrastructures, which entails increased digital risk. The respect of a basic cyber hygiene should also avoid imposing heavy costs on the economy by minimising the impact and costs of ICT disruptions.
Recital 14			
24	(14) The use of a regulation helps reducing regulatory complexity, fosters supervisory convergence, increases legal certainty, while also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions. The choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities appears therefore the most appropriate way to	(14) The use of a regulation helps reducing regulatory complexity, fosters supervisory convergence, increases legal certainty, while also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions. The choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities appears therefore the most appropriate way to	(14) The use of a regulation helps reducing regulatory complexity, fosters supervisory convergence, increases legal certainty, while also contributing to limiting compliance costs, especially for financial entities operating cross-border, and to reducing competitive distortions. The choice of a Regulation for the establishment of a common framework for the digital operational resilience of financial entities appears therefore the most appropriate way to

	Commission Proposal	EP Mandate	Council Mandate
	guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.	guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.	guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.
Recital 14a			
24a		***(14a) However, the implementation of this Regulation should not hamper innovation with regard to how financial entities deal with digital operational resilience issues while complying with its provisions, nor with regard to the services they offer or the services offered by ICT third-party service providers.***	
Recital 15			
25	(15) Besides the financial services legislation, Directive (EU) 2016/1148 of the European Parliament and of the Council[1] is the current general cybersecurity framework at Union level. Among the seven critical sectors, that Directive also applies to three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 sets out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties identified by the Member States are in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements laid down in it.	(15) Besides the financial services legislation, Directive (EU) 2016/1148 of the European Parliament and of the Council[1] is the current general cybersecurity framework at Union level. Among the seven critical sectors, that Directive also applies to three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 sets out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties identified by the Member States are in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements laid down in it.	(15) Besides the financial services legislation, Directive (EU) 2016/1148 of the European Parliament and of the Council[1] is the current ~~general~~**horizontal** cybersecurity framework at Union level. Among the seven critical sectors, that Directive also applies to– three types of financial entities, namely credit institutions, trading venues and central counterparties. However, since Directive (EU) 2016/1148 sets out a mechanism of identification at national level of operators of essential services, only certain credit institutions, trading venues and central counterparties identified by the Member States are in practice brought into its scope and thus required to comply with the ICT security and incident notification requirements laid down in it.

	Commission Proposal	EP Mandate	Council Mandate
	_____ 1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).	_____ 1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).	_____ 1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
Recital 16			
26	(16) As this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in respect to those laid down in the current Union financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, this Regulation constitutes lex specialis to Directive (EU) 2016/1148. It is crucial to maintain a strong relation between the financial sector and the Union horizontal cybersecurity framework would ensure consistency with the cyber security strategies already adopted by Member States, and allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by Directive (EU) 2016/1148.	(16) As this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in respect to those laid down in the current Union financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, ***for financial entities,*** this Regulation– constitutes lex specialis to Directive (EU) 2016/1148. It is crucial to maintain a strong relation between the financial sector and the Union horizontal cybersecurity framework ~~*would*~~***to*** ensure consistency with the cyber security strategies already adopted by Member States, and allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by Directive (EU) 2016/1148.	(16) As this Regulation raises the level of harmonisation on digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in respect to those laid down in the current Union financial services legislation, this constitutes an increased harmonisation also by comparison to requirements laid down in Directive (EU) 2016/1148. Consequently, this Regulation constitutes lex specialis to Directive (EU) 2016/1148. It is crucial to maintain a strong relation between the financial sector and the Union horizontal cybersecurity framework ~~would~~**in order to** ensure consistency with the cyber security strategies already adopted by Member States~~,~~ and allow financial supervisors– to be made aware of cyber incidents affecting other sectors covered by Directive (EU) 2016/1148.
Recital 16a			
26a			

	Commission Proposal	EP Mandate	Council Mandate
			(16a) In accordance with Article 4(2) of the Treaty on the European Union and without prejudice to the judicial review of the European Court of Justice, this Regulation should not affect the responsibility of Member States regarding essential State functions concerning public security, defence and the safeguarding of national security, for example concerning the supply of information which would be contrary to the safeguarding of national security.
Recital 17			
27	(17) To enable a cross-sector learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (EU) 2016/1148 should remain part of the 'ecosystem' of that Directive (e.g. NIS Cooperation Group and CSIRTs). ESAs and national competent authorities, respectively should be able to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, exchanges information and further cooperate with the single points of contact designated under Directive (EU) 2016/1148. The competent authorities under this Regulation should also consult and cooperate with the national CSIRTs designated in accordance with Article 9 of Directive (EU) 2016/1148.	(17) To enable a cross-sector learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (EU) 2016/1148 should remain part of the 'ecosystem' of that Directive (e.g. NIS Cooperation Group and CSIRTs). ESAs and national competent authorities, respectively should be able to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, exchanges information and further cooperate with the single points of contact designated under Directive (EU) 2016/1148. The ***Joint Oversight Body, the Lead Overseers and 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.	(17) To enable a cross-sector learning process and effectively draw on experiences of other sectors in dealing with cyber threats, financial entities referred to in Directive (EU) 2016/1148 should remain part of the 'ecosystem' of that Directive (e.g. NIS Cooperation Group and CSIRTs). **The** ESAs and national competent authorities, respectively should be able to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, 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. **The**

	Commission Proposal	EP Mandate	Council Mandate
		Moreover, this Regulation should ensure that the CSIRTs network established by Directive (EU) 2016/1148 is provided with the details of major ICT-related incidents.	**competent authorities may also request technical advice from the authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 and establish cooperation arrangements that should ensure effective and fast-response coordination mechanisms.**
Recital 18			
28	(18) It is also important to ensure consistency with the European Critical Infrastructure (ECI) Directive, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructures against non-cyber related threats, with possible implications for the financial sector. [1] 1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).	(18) It is also important to ensure consistency with the European Critical Infrastructure (ECI) Directive, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructures against non-cyber related threats, ***and the Directive on Resilience of Critical Entities***[1] with possible implications for the financial sector. [1] 1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).	(18) ~~It is also important to ensure consistency with the European Critical Infrastructure (ECI) Directive, which is currently being reviewed in order to enhance the protection and resilience of critical infrastructures against non-cyber related threats, with possible implications for the financial sector.~~ [1]**Strong interlinkages between the digital resilience and the physical resilience of financial entities call for a coherent approach by this Regulation and the Directive (EU) XXX/XXX of the European Parliament and the Council on the resilience of critical entities [CER Directive[1]].** 1. ~~Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of~~ **Proposal for a Directive of the** European ~~critical infrastructures and the assessment~~ **Parliament and** of the ~~need to improve their protection (OJ L 345, 23.12.2008, p. 75)~~**Council on the resilience of critical entities [Please insert full reference]**.
Recital 19			
29	(19) Cloud computing service providers are one	(19) Cloud computing service providers are one	(19) Cloud computing service providers are

	Commission Proposal	EP Mandate	Council Mandate
	category of digital service providers covered by Directive (EU) 2016/1148. As such they are subject to ex-post supervision carried out by the national authorities designated according to that Directive, which is limited to requirements on ICT security and incident notification laid down in that act. Since the Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities, it should be considered complementary to the supervision that is taking place under Directive (EU) 2016/1148. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority.	category of digital service providers covered by Directive (EU) 2016/1148. As such they are subject to ex-post supervision carried out by the national authorities designated according to that Directive, which is limited to requirements on ICT security and incident notification laid down in that act. Since the Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities, it should be considered complementary to the supervision that is taking place under Directive (EU) 2016/1148***, and both substantive and procedural requirements applicable to critical ICT third-party service providers under this Regulation should be coherent and seamless with those applicable under that Directive***. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority.	one category of digital service providers covered by Directive (EU) 2016/1148. As such they are subject to ex-post supervision carried out by the national authorities designated according to that Directive, which is limited to requirements on ICT security and incident notification laid down in that act. Since the Oversight Framework established by this Regulation applies to all critical ICT third-party service providers, including cloud computing service providers, when they provide ICT services to financial entities, it should be considered complementary to the supervision that is taking place under Directive (EU) 2016/1148. Moreover, the Oversight Framework established by this Regulation should cover cloud computing service providers in the absence of a Union horizontal sector-agnostic framework establishing a Digital Oversight Authority.
Recital 20			
30	(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	(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	(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 **handling all** ICT-related ~~incident~~**incidents and** reporting **major ones. Likewise**, **financial entities**

	Commission Proposal	EP Mandate	Council Mandate
	managing ICT third-party risk. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements for financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC[1]. _____ 1. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	managing ICT third-party ***and ICT intra-group*** risk. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements ~~*for financial entities which are micro enterprises as defined in Commission Recommendation 2003/361/EC*~~[1] ***taking into account their nature, scale, complexity and overall risk profile***. _____ ~~*1. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).*~~	**should have policies for** testing of ICT systems, controls and processes, as well as for managing ICT third-party risk. The digital operational resilience bar for the financial system should be raised while allowing for a proportionate application of requirements for **certain** financial entities**, particularly those** which are ~~micro enterprises as defined in Commission Recommendation 2003/361/EC~~[1] **microenterprises, as well as financial entities subject to a proportionate ICT Risk Management framework. To facilitate an efficient supervision of institutions for occupational retirement provision that duly takes into account both the application the principle of proportionality, as well as the need to reduce administrative burdens for the competent authorities, the relevant national supervisory arrangements in respect to such entities should fully take into account the specific nature, scale, complexity of the services, activities and operations and the overall risk profile of these entities even when exceeding relevant thresholds established in Article 5 of Directive 2016/2341. In particular, supervisory activities could primarily focus on the need to address serious risks associated with the ICT risk management of a particular entity. Competent authorities should also maintain a vigilant, but proportionate approach in relation to the supervision of institutions for occupational retirement provision which, in accordance with Article 31 of Directive 2016/2341,**

	Commission Proposal	EP Mandate	Council Mandate
			outsource a significant part of core business, such as asset management, actuarial calculations, accounting and data management, to service providers operating on their behalf, in result of which the proportionate application is considered appropriate. _____ ~~1. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).~~
Recital 21			
31	(21) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through relevant work undertaken by the European Union Agency for Cybersecurity (ENISA)[1] and the NIS Cooperation Group for the financial entities under Directive (EU) 2016/1148, divergent approaches on thresholds and taxonomies still exist or can emerge for the remainder of financial entities. This entails multiple requirements that financial entities must abide to, especially when operating across several Union jurisdictions and when part of a financial group. Moreover, these divergences may hinder the creation of further Union uniform or centralised mechanisms speeding up the reporting process and supporting a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risks in case of large scale attacks with potentially systemic consequences.	(21) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through relevant work undertaken by the European Union Agency for Cybersecurity (ENISA)[1] and the NIS Cooperation Group for the financial entities under Directive (EU) 2016/1148, divergent approaches on thresholds and taxonomies still exist or can emerge for the remainder of financial entities. This entails multiple requirements that financial entities must abide to, especially when operating across several Union jurisdictions and when part of a financial group. Moreover, these divergences may hinder the creation of further Union uniform or centralised mechanisms speeding up the reporting process and supporting a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risks in case of large scale attacks with potentially systemic consequences.	(21) ICT-related incident reporting thresholds and taxonomies vary significantly at national level. While common ground may be achieved through relevant work undertaken by the European Union Agency for Cybersecurity (ENISA)[1] and the NIS Cooperation Group for the financial entities under Directive (EU) 2016/1148, divergent approaches on thresholds and taxonomies still exist or can emerge for the remainder of financial entities. This **diversity** entails multiple requirements ~~that~~**which** financial entities must abide to, especially when operating across several Union jurisdictions and when part of a financial group. Moreover, these divergences may hinder the creation of further Union uniform or centralised mechanisms speeding up the reporting process and supporting a quick and smooth exchange of information between competent authorities, which is crucial for addressing ICT risks in case of large scale attacks with potentially systemic

	Commission Proposal	EP Mandate	Council Mandate
	_____ 1. ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.	_____ 1. ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.	consequences. _____ 1. ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.
Recital 21a			
31a		***(21a) In order to reduce the administrative burden and avoid complexity and duplicative reporting requirements for payment service providers that fall within the scope of this Regulation, the incident reporting requirements under Directive (EU) 2015/2366 should cease to apply. As such, credit institutions, e-money institutions and payment institutions should report, under this Regulation, all operational or security payment-related and non-payment-related incidents that were previously reported under Directive (EU) 2015/2366, irrespective of whether the incidents are ICT-related or not.***	**(22a) To reduce the administrative burden and potentially duplicative reporting obligations, for payment service providers that fall within the scope of this regulation, the incident reporting under Directive (EU) 2015/2366 should cease to apply.** **As such, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of Directive (EU) 2015/2366, should report under this regulation all operational or security payment-related incidents previously reported under Directive (EU) 2015/2366, irrespective of whether such incidents are ICT-related or not.**
Recital 22			
32	(22) To enable competent authorities to fulfil their supervisory roles by obtaining a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to enhance the exchange of information between relevant public authorities, including law	(22) To enable competent authorities to fulfil their supervisory roles by obtaining a complete overview of the nature, frequency, significance and impact of ICT-related incidents and to enhance the exchange of information between relevant public authorities, including law	(22) To enable competent authorities to fulfil their supervisory roles by obtaining a complete overview of the nature, frequency, significance and impact of ICT-related incidents **[and cyber threats]** and to enhance the exchange of information between relevant public authorities,

	Commission Proposal	EP Mandate	Council Mandate
	enforcement authorities and resolution authorities, it is necessary to lay down rules in order to complete the ICT-related incident reporting regime with the requirements that are currently missing in financial subsector legislation and remove any existing overlaps and duplications to alleviate costs. It is therefore essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities only. In addition, the ESAs should be empowered to further specify ICT-related incident reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds.	enforcement authorities and resolution authorities, it is necessary to lay down rules in order to ~~complete the~~***achieve a robust*** ICT-related incident reporting regime with the requirements that ~~are currently missing in~~ ***address the gaps in sectoral*** financial ~~subsector~~***services*** legislation and remove any existing overlaps and duplications to alleviate costs. It is therefore essential to harmonise the ICT-related incident reporting regime by requiring all financial entities to report to their competent authorities ~~only~~***through a single streamlined framework as set out in this Regulation***. In addition, the ESAs should be empowered to further specify ICT-related incident reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds.	including law enforcement authorities and resolution authorities, it is necessary to lay down rules in order to complete the ICT-related incident **[and cyber threats]**[1] reporting ~~regime with the requirements that are~~**regimes with a set of requirements** currently missing in **the various subsectors of the** financial ~~subsector~~**services Union** legislation**,** and remove any existing overlaps and duplications to alleviate costs. It is therefore essential to harmonise the ICT-related incident **[and cyber threats]** reporting ~~regime~~**regimes** by requiring all financial entities to report to their competent authorities only. In addition, the ESAs should be empowered to further specify ICT-related incident **[and cyber threats]** reporting elements such as taxonomy, timeframes, data sets, templates and applicable thresholds. **1. Taking into consideration the views expressed by Member States on the matter of the handling of significant cyber threats (classification and reporting requirements in relation to significant cyber threats), the Presidency is of the view that ensuring full consistency between DORA Proposal and the Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2) would best preserve the lex specialis approach endorsed by MS in DORA and could thus constitute a possible compromise in this regard. Discussions on NIS 2 in this area are ongoing and it is not entirely clear yet how the final Council position on NIS 2 will evolve. In light of this uncertainty, the fact that these proposals are moving targets and with a view to ensure consistency with NIS 2, the Presidency therefore proposes to include the relevant provisions on significant cyber threats reporting in DORA in [square brackets] for the time**

	Commission Proposal	EP Mandate	Council Mandate
			being. If a mandate is granted for DORA, this way of proceeding would allow the trilogues on DORA to move ahead while the issue of significant cyber threats would be dealt with at a later stage: once the outcome of negotiations under NIS 2 becomes clear, it could then also be reflected under DORA. In case such an approach is considered acceptable by MS, this reasoning would also be explained in the note to Coreper.
Recital 23			
33	(23) Digital operational resilience testing requirements have developed in some financial subsectors within several and uncoordinated, national frameworks addressing the same issues in a different way. This leads to duplication of costs for cross-border financial entities and makes difficult the mutual recognition of results. Uncoordinated testing can therefore segment the single market.	(23) Digital operational resilience testing requirements have developed in some financial subsectors within several and ***sometimes*** uncoordinated, national frameworks addressing the same issues in a different way. This leads to duplication of costs for cross-border financial entities and ~~*makes difficult*~~***could hamper*** the mutual recognition of results. Uncoordinated testing can therefore segment the single market.	(23) Digital operational resilience testing requirements have developed in some financial subsectors ~~within~~**with** several**, some of them uncoordinated**~~ and uncoordinated, national~~ frameworks addressing the same issues in a different way **although with the same goals**. This leads to **a potential** duplication of costs for cross-border financial entities and makes ~~difficult~~ the mutual recognition of **digital operational resilience testing** results~~. Uncoordinated testing can therefore~~ **complex which in turn can** segment the single market.
Recital 24			
34	(24) In addition, where no testing is required, vulnerabilities remain undetected putting the financial entity and ultimately the financial sector's stability and integrity at higher risk. Without Union intervention, digital operational resilience testing would continue to be patchy and there would be no mutual recognition of testing results across different jurisdictions.	(24) In addition, where no testing is required, vulnerabilities remain undetected putting the financial entity and ultimately the financial sector's stability and integrity at higher risk. Without Union intervention, digital operational resilience testing would continue to be patchy and there would be no mutual recognition of testing results across different jurisdictions.	(24) In addition, where no **ICT** testing is required, vulnerabilities remain undetected ~~putting the~~**thus exposing a** financial entity **to ICT risk** and ultimately **creating higher risk to** the financial sector's stability and integrity~~ at higher risk~~. Without Union intervention, digital operational resilience testing would continue to be ~~patchy~~**inconsistent across jurisdictions** and

	Commission Proposal	EP Mandate	Council Mandate
	Also, as it is unlikely that other financial subsectors would adopt such schemes on a meaningful scale, they would miss out on the potential benefits, such as revealing vulnerabilities and risks, testing defence capabilities and business continuity, and increased trust of customers, suppliers and business partners. To remedy such overlaps, divergences and gaps, it is necessary to lay down rules aiming at coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition of advanced testing for significant financial entities.	Also, as it is unlikely that other financial subsectors would adopt such schemes on a meaningful scale, they would miss out on the potential benefits, such as revealing vulnerabilities and risks, testing defence capabilities and business continuity, and increased trust of customers, suppliers and business partners. To remedy such overlaps, divergences and gaps, it is necessary to lay down rules aiming at coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition of advanced testing for significant financial entities.	there would be no mutual recognition of **ICT** testing results across different jurisdictions. Also, as it is unlikely that other financial subsectors would adopt ~~such~~**testing** schemes on a meaningful scale, they would miss out on the potential benefits **of a testing framework**, such as revealing **ICT** vulnerabilities and risks, testing defence capabilities and business continuity, and ~~increased~~**thus contributing to increase** trust of customers, suppliers and business partners. To remedy such overlaps, divergences and gaps, it is necessary to lay down rules aiming at coordinated testing by financial entities and competent authorities, thus facilitating the mutual recognition of advanced testing for significant financial entities.
Recital 25			
35	(25) Financial entities' reliance on ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in the past years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.	(25) Financial entities' reliance on ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in the past years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.	(25) Financial entities' reliance on ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in the past years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.
Recital 26			

	Commission Proposal	EP Mandate	Council Mandate
36	(26) This extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements they are subject to, or otherwise in enforcing specific rights, such as access or audit rights, when the latter are enshrined in the agreements. Moreover, many such contracts do not provide for sufficient safeguards allowing for a fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess these associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors.	(26) This extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements they are subject to, or otherwise in enforcing specific rights, such as access or audit rights, when the latter are enshrined in the agreements. Moreover, many such contracts do not provide for sufficient safeguards allowing for a fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess these associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors.	(26) This extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements they are subject to, or otherwise in enforcing specific rights, such as access or audit rights, when the latter are enshrined in the agreements. Moreover, many such contracts do not provide for sufficient safeguards allowing for a fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess these associated risks. In addition, as ICT third-party service providers often provide standardised services to different types of clients, such contracts may not always adequately cater for the individual or specific needs of the financial industry actors.
Recital 27			
37	(27) Despite some general rules on outsourcing in some of the Union's financial services pieces of legislation, the monitoring of the contractual dimension is not fully anchored into Union legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities'	(27) Despite some general rules on outsourcing in some of the Union's financial services pieces of legislation, the monitoring of the contractual dimension is not fully anchored into Union legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities'	(27) ~~Despite some general rules on outsourcing in some of the Union's financial services pieces of legislation~~**Even though the Union financial services legislation contains certain general rules on outsourcing**, the monitoring of the contractual dimension is not fully anchored into Union legislation. In the absence of clear and bespoke Union standards applying to the contractual arrangements concluded with ICT third-party service providers, the external source of ICT risk is not comprehensively

	Commission Proposal	EP Mandate	Council Mandate
	management of ICT third-party risk, accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level.	management of ICT third-party risk, accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level.	addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, **particularly where financial entities resort to ICT third-party service providers to support their critical or important functions. These principles should be** accompanied by a set of core contractual rights in relation to several elements in the performance and termination of contracts with a view to enshrine certain minimum safeguards underpinning financial entities' ability to effectively monitor all risk emerging at ICT third party level. **These principles are complementary to sectorial legislation applicable to outsourcing.**
Recital 28			
38	(28) There exists a lack of homogeneity and convergence on ICT third party risk and ICT third-party dependencies. Despite some efforts to tackle the specific area of outsourcing such as the 2017 recommendations on outsourcing to cloud service providers,[1] the issue of systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed in Union legislation. This lack at Union level is compounded by the absence of specific mandates and tools allowing national supervisors to acquire a good understanding of ICT third-party dependencies and adequately monitor risks arising from concentration of such ICT third-party dependencies.	(28) There exists a lack of homogeneity and convergence on ICT third party risk and ICT third-party dependencies. Despite some efforts to tackle the specific area of outsourcing such as the 2017 recommendations on outsourcing to cloud service providers,[1] the issue of systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed in Union legislation. This lack at Union level is compounded by the absence of specific mandates and tools allowing national supervisors to acquire a good understanding of ICT third-party dependencies and adequately monitor risks arising from concentration of such ICT third-party dependencies.	(28) There ~~exists~~**is** a lack of homogeneity and convergence ~~on~~**in relation to the monitoring of** ICT third party risk and ICT third-party dependencies. Despite ~~some~~ efforts to tackle the specific area of outsourcing such as the 2017 recommendations on outsourcing to cloud service providers,[1] the **broader** issue of **counteracting** systemic risk which may be triggered by the financial sector's exposure to a limited number of critical ICT third-party service providers is barely addressed ~~in~~**by** Union legislation. This lack at Union level is compounded by the absence of specific mandates and tools allowing national **financial** supervisors to acquire a good understanding of ICT third-party dependencies and **to** adequately

	Commission Proposal	EP Mandate	Council Mandate
	_____ 1. Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), now repealed by the EBA Guidelines on outsourcing (EBA/GL/2019/02).	_____ 1. Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), now repealed by the EBA Guidelines on outsourcing (EBA/GL/2019/02).	monitor risks arising from concentration of ~~such~~ ICT third-party dependencies. _____ 1. Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), now repealed by the EBA Guidelines on outsourcing (EBA/GL/2019/02).
Recital 29			
39	(29) Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms enabling financial superiors to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Union oversight framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities.	(29) Taking into account the potential systemic risks entailed by the increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms enabling financial superiors to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, it is necessary to establish an appropriate Union oversight framework allowing for a continuous monitoring of the activities of ICT third-party service providers that ~~are~~***provide*** critical ~~*providers*~~***services*** to financial entities. ***As intra-group provision of ICT services does not carry the same risks, ICT service providers that are part of the same group or institutional protection scheme should not be defined as critical ICT third-party service providers.***	(29) Taking into account the potential systemic ~~risks~~**risk** entailed by ~~the~~ increased outsourcing practices and by the ICT third-party concentration, and mindful of the insufficiency of national mechanisms ~~enabling~~**in providing** financial ~~superiors~~**supervisors with adequate tools** to quantify, qualify and redress the consequences of ICT risks occurring at critical ICT third-party service providers, it is necessary to establish– an appropriate Union Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical providers to financial entities**, while ensuring that the confidentiality or security of customers other than financial entities is preserved**.
Recital 30			
40	(30) With ICT threats becoming more complex and sophisticated, good detection and prevention measures depend to a great extent on regular threat and vulnerability intelligence	(30) With ICT threats becoming more complex and sophisticated, good detection and prevention measures depend to a great extent on regular threat and vulnerability intelligence	(30) With ICT threats becoming more **and more** complex and sophisticated, good **measures for the** detection and prevention ~~measures~~**of ICT risks** depend to a great extent

	Commission Proposal	EP Mandate	Council Mandate
	sharing between financial entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances financial entities' capacity to prevent threats from materialising into real incidents and enables financial entities to better contain the effects of ICT-related incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules.	sharing between financial entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances financial entities' capacity to prevent threats from materialising into real incidents and enables financial entities to better contain the effects of ICT-related incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules. ***It is therefore important to strengthen cooperation arrangements and reporting amongst financial entities and the competent authorities as well as information-sharing with the public, with a view to developing an open intelligence sharing framework and a 'security by design' approach, which are essential in order to increase the operational resilience and preparedness of the financial sector with regard to ICT risks. Information-sharing arrangements should always give due consideration to potential risks related to cyber security, data protection or commercial confidentiality.***	on regular threat and vulnerability intelligence sharing between financial entities. Information sharing contributes to **creating** increased awareness on cyber threats~~, which,~~**.** In turn, **this** enhances **the capacity of** financial entities~~' capacity~~ to prevent threats from materialising into real **ICT** incidents and enables financial entities to ~~better contain the effects~~**contain more effectively the impacts** of ICT-related incidents and recover ~~more efficiently~~**faster**. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with the data protection, anti-trust and liability rules. **It is therefore important to foster cooperation arrangements, in particular with regard to information sharing, amongst competent authorities, as well as in relation to NIS competent authorities.**
Recital 31			
41	(31) In addition, hesitations about the type of information which can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead	(31) In addition, hesitations about the type of information ~~*which*~~ ***that*** can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law	(31) In addition, hesitations about the type of information which can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead

	Commission Proposal	EP Mandate	Council Mandate
	to useful information being withheld. The extent and quality of information sharing remains limited, fragmented, with relevant exchanges being done mostly locally (via national initiatives) and with no consistent Union-wide information sharing arrangements tailored to the needs of an integrated financial sector.	enforcement purposes) lead to useful information being withheld. The extent and quality of information sharing remains limited, fragmented, with relevant exchanges being done mostly locally (via national initiatives) and with no consistent Union-wide information sharing arrangements tailored to the needs of an integrated financial sector. ***It is therefore important to strengthen those communication channels and have input from non-supervisory authorities, when necessary and relevant, throughout the supervisory cycle.***	to useful information being withheld. The extent and quality of information sharing remains limited, fragmented, with relevant exchanges being done mostly locally (via national initiatives) and with no consistent Union-wide information sharing arrangements tailored to the needs of an integrated financial sector.
Recital 32			
42	(32) Financial entities should therefore be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements which, when conducted in trusted environments, would help the financial community to prevent and collectively respond to threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels. Those mechanisms should be conducted in full compliance with the applicable competition law rules of the Union[1] as well as in a way that guarantees the full respect of Union data	(32) Financial entities should ~~*therefore*~~***also*** be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements which, when conducted in trusted environments, would help the financial community to prevent and collectively respond to threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels. Those mechanisms should be conducted in full compliance with the applicable competition law rules of the Union[1] as well as in a way that guarantees the full respect of Union data	(32) Financial entities should therefore be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements which, when conducted in trusted environments, would help the financial community to prevent and collectively respond to threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels. Those mechanisms should be conducted in full compliance with the applicable competition law rules of the Union[1] as well as in a way that guarantees the full respect of Union data

	Commission Proposal	EP Mandate	Council Mandate
	protection rules, mainly Regulation (EU) 2016/679 of the European Parliament and of the Council,[2] in particular in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in point (f) of Article 6(1) of that Regulation. _____ 1. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01. 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).	protection rules, mainly Regulation (EU) 2016/679 of the European Parliament and of the Council[2],[2] in particular in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in point (f) of Article 6(1) of that Regulation. _____ 1. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01. 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).	protection rules, mainly Regulation (EU) 2016/679 of the European Parliament and of the Council[2],[2] ~~in particular~~ **based on one or more of the legal basis laid down in Article 6 of that Regulation, such as** in the context of the processing of personal data that is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, as referred to in point (f) **of Article 6(1) of that Regulation as well as in the context of the processing of personal data necessary for compliance with a legal obligation to which the controller is subject, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as referred to in points (c) and (e) respectively,** of Article 6(1) of that Regulation. _____ 1. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01. 2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(OJ L 119, 4.5.2016, p. 1).
Recital 33			
43	(33) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into consideration significant differences	(33) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules, ***including the risk management framework***	(33) Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into consideration significant differences

	Commission Proposal	EP Mandate	Council Mandate
	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.	***requirements,*** should take into consideration significant differences between financial entities in terms of size, ~~*business profiles or exposure to digital risk*~~***nature, complexity and risk profile***. As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework, financial entities should duly balance their ICT-related needs to their size***, nature, complexity,*** ~~*and*~~ business ***profile and relative risk*** profile, while competent authorities should continue to assess and review the approach of such distribution.	between financial entities in terms of size, business **and risk** 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 **the size nature, scale and complexity of** their ~~size and business~~**services, activities and operations, as well as their overall risk** profile, while competent authorities should continue to assess and review the approach of such distribution.
Recital 33a			
43a			**(33a) Account information service providers referred to in Article 33 (1) of Directive (EU) 2015/2366, are explicitly included in the scope of this Regulation, taking into account the specific nature of their activities and the risks arising therefrom.** **In addition, payment institutions and e-money institutions exempted under Article 32(1) of Directive (EU) 2015/2366 and Article 9(1) of Directive 2009/110/EC, respectively, are included in the scope of this Regulation even if they have not been granted authorisation in accordance with Directive (EU) 2015/2366 to provide and execute payment services or if they have not been granted authorisation under Directive 2009/110/EC to issue electronic money, respectively.**

	Commission Proposal	EP Mandate	Council Mandate
			On the contrary, post office giro institutions, referred to in Article 1(1), point (c) of Directive (EU) 2015/2366, are excluded from the scope of this Regulation. **The competent authority for payment institutions exempted under Directive (EU) 2015/2366, electronic money institutions exempted under Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366, is the one designated in accordance with Article 22 of Directive (EU) 2015/2366.**
Recital 34			
44	(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities which are not micro enterprises in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining access rights policies.	(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities ~~*which*~~***that*** are not micro enterprises in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, or to adopt a human resources document comprehensively explaining access rights policies.	(34) As larger financial entities may enjoy wider resources and could swiftly deploy funds to develop governance structures and set up various corporate strategies, only financial entities which are not ~~micro enterprises~~**microenterprises** in the sense of this Regulation should be required to establish more complex governance arrangements. Such entities are better equipped in particular to set up dedicated management functions for supervising arrangements with ICT third-party service providers or for dealing with crisis management, to organise their ICT risk management according to the three lines of defence model, ~~or~~ to adopt a human resources document comprehensively explaining access

	Commission Proposal	EP Mandate	Council Mandate
	By the same token, only such financial entities should be called to perform in-depth assessments after major changes in the network and information system infrastructures and processes, to regularly conduct risk analyses on legacy ICT systems, or expand the testing of business continuity and response and recovery plans to capture switchovers scenarios between primary ICT infrastructure and redundant facilities.	By the same token, only such financial entities should be called to perform in-depth assessments after major changes in the network and information system infrastructures and processes, to regularly conduct risk analyses on legacy ICT systems, or expand the testing of business continuity and response and recovery plans to capture switchovers scenarios between primary ICT infrastructure and redundant facilities.	rights policies~~.~~ ~~By the same token, only such financial entities should be called to perform in-depth assessments after major changes in the network and information system infrastructures and processes.~~**, or** to regularly ~~conduct risk analyses on legacy ICT systems, or expand the testing of business continuity and response and recovery plans to capture switchovers scenarios between primary ICT infrastructure and redundant facilities~~**submit their ICT risk management framework to internal audits**.
Recital 34a			
44a			**(34a) Some financial entities benefit from exemptions or from a very light framework under their respective sectorial Union legislation. Such financial entities include managers of alternative investment funds referred to in Article 3 (2) of Directive 2011/61/EU, insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC, institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total, as well as insurance and reinsurance intermediaries.** **In light of the exemptions applicable to these financial entities in their respective sectorial legislation, it would not be proportionate to include them in the scope of this Regulation.**

	Commission Proposal	EP Mandate	Council Mandate
Recital 34aa			
44b			**(34aa) Since Member States may partly or fully exclude institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU from the application of all or part of the provisions in Directive (EU) 2015/2366, and Directive 2013/36/EU itself does not apply to institutions referred to in points (3) to (23) of its Article 2(5), Member States may consequently also choose to exempt institutions referred to in points (3) to (23) of Article 2(5) of Directive 2013/36/EU located within their respective territory from the application of this Regulation.**
Recital 34b			
44c			**(34b) For the same reasons, it is also appropriate to exclude form the scope of this Regulation, the persons and entities referred in Articles 2 and 3 of Directive 2014/65/EU which are allowed to provide investment services without having to obtain an authorisation under Directive 2014/65/EU. However, Article 2 of Directive 2014/65/EU also exempts from the scope of that directive entities which qualify as financial entities for the purposes of this Regulation such as, central securities depositories, collective investment undertakings or insurance and reinsurance undertakings. The exemption**

	Commission Proposal	EP Mandate	Council Mandate
			from the scope of this Regulation of the persons and entities referred in Articles 2 and 3 of Directive 2014/65/EU should not encompass these central securities depositories, collective investment undertakings or insurance and reinsurance undertakings.
Recital 34c			
44d			**(34c) Under sector specific Union legislation some financial entities are subject to lighter requirements or exemptions for reasons associated with their size or the services they provide. These categories include small and non-interconnected investment firms, small institutions for occupational retirement provision which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total as well as institutions exempted under Directive 2013/36/EU. Therefore, in accordance with the principle of proportionality and to preserve the spirit of sector specific Union legislation, it is also appropriate to subject these financial entities to a more proportionate ICT- risk framework under this Regulation. The proportionate character of the ICT-risk management framework covering these financial entities should not be altered by the**

	Commission Proposal	EP Mandate	Council Mandate
			regulatory technical standards that are to be developed by the ESAs. **Moreover, in accordance with the principle of proportionality, it is appropriate to also subject payment institutions referred to in Article 32 (1) of Directive (EU) 2015/2366 and electronic money institutions referred to in Article 9 of Directive 2009/110/EC benefiting from exemptions in accordance with national transpositions of these Union legal acts to a proportionate ICT-risk framework under this Regulation, while payment institutions and electronic money institutions which have not been exempted in accordance with their respective transposition of sectorial Union legislation should comply with the general framework laid down by this Regulation.**
Recital 34d			
44e			**(34d) In the same vein, financial entities which qualify as microenterprises or are subject to the proportionate ICT risk management framework mentioned in the previous recital, should not be required to perform in-depth assessments after major changes in their network and information system infrastructures and processes, to regularly conduct risk analyses on legacy ICT systems, or to expand the testing of business continuity and response and recovery plans to capture switchover**

	Commission Proposal	EP Mandate	Council Mandate
			scenarios between primary ICT infrastructure and redundant facilities.
Recital 35			
45	(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 ***estimated*** costs and losses caused by ***significant*** ICT disruptions***, major ICT-related incidents*** and the results of post-incident reviews after ~~*significant*~~***such*** 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 ICT disruptions and the results of post-incident reviews after significant ICT disruptions.~~
Recital 36			
46	(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	(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	(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

	Commission Proposal	EP Mandate	Council Mandate
	means to ensure the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness over cyber risks and a commitment to respect a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risks should be an overarching principle of that comprehensive approach, further translated into the continuous engagement of the management body in the control of the monitoring of the ICT risk management.	means to ensure the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness over cyber risks and a commitment to respect a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risks should be an overarching principle of that comprehensive approach, further translated into the continuous– engagement of the management body in the control of the monitoring of the ICT risk management.	means to ensure the resilience of the ICT systems, but should also cover people and processes through a set of policies which cultivate, at each corporate layer, and for all staff, a strong sense of awareness over cyber risks and a commitment to respect a strict cyber hygiene at all levels. The ultimate responsibility of the management body in managing a financial entity's ICT risks should be an overarching principle of that comprehensive approach, further translated into the continuous– engagement of the management body in the control of the monitoring of the ICT risk management.
Recital 37			
47	(37) Moreover, the management body's full accountability goes hand in hand with securing a level of ICT investments and overall budget for the financial entity to be able to achieve its digital operational resilience baseline.	(37) Moreover, the management body's full accountability goes hand in hand with– securing a level of ICT investments and overall budget for the financial entity to be able to achieve its digital operational resilience baseline.	(37) Moreover, the management body's full accountability goes hand in hand with– securing a level of ICT investments and overall budget for the financial entity to be able to achieve its digital operational resilience baseline.
Recital 38			
48	(38) Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk,[1] this Regulation promotes a set of functions facilitating the overall structuring of the ICT risk management.	(38) Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk,[1], this Regulation promotes a set of functions facilitating the overall structuring of the ICT risk management.	(38) Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk,[1] this Regulation promotes a set of functions facilitating the overall structuring of the ICT risk management.

	Commission Proposal	EP Mandate	Council Mandate
	As long as the main capabilities which financial entities put in place answer the needs of the objectives foreseen by the functions (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities remain free to use ICT risk management models that are differently framed or categorised. __________ 1. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf G7 Fundamental Elements of Cybersecurity for the Financial Sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB CIRR toolkit, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.	As long as the main capabilities which financial entities put in place answer the needs of the objectives foreseen by the functions (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities remain free to use ICT risk management models that are differently framed or categorised. __________ 1. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf G7 Fundamental Elements of Cybersecurity for the Financial Sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB CIRR toolkit, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document~~.~~	As long as the main capabilities which financial entities put in place answer the needs of the objectives foreseen by the functions (identification, protection and prevention, detection, response and recovery, learning and evolving and communication) set out in this Regulation, financial entities remain free to use ICT risk management models that are differently framed or categorised. __________ 1. CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf G7 Fundamental Elements of Cybersecurity for the Financial Sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB CIRR toolkit, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.
Recital 39			
49	(39) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and endowed with sufficient capacity not only to guarantee the processing of data as it is necessary for the performance of their services, but also to ensure technological resilience allowing financial entities to adequately deal with additional processing needs which stressed market conditions or other adverse situations may generate. While this Regulation does not entail any standardization of specific ICT systems, tools or technologies, it relies on the	(39) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and endowed with sufficient capacity not only to guarantee the processing of data as it is necessary for the performance of their services, but also to ensure technological resilience allowing financial entities to adequately deal with additional processing needs which stressed market conditions or other adverse situations may generate. While this Regulation does not entail any standardization of specific ICT systems, tools or technologies, it relies on the	(39) To keep pace with an evolving cyber threat landscape, financial entities should maintain updated ICT systems that are reliable and endowed with sufficient capacity not only to guarantee the processing of data as it is necessary for the performance of their services, but also to ensure technological resilience allowing financial entities to adequately deal with additional processing needs which stressed market conditions or other adverse situations may generate. While this Regulation ~~does not entail~~**neither entails** any standardization of specific ICT systems, tools or technologies, **nor**

	Commission Proposal	EP Mandate	Council Mandate
	financial entities' suitable use of European and internationally recognised technical standards (e.g. ISO) or industry best practices, insofar as such use is fully compliant with specific supervisory instructions on the use and incorporation of international standards.	financial entities' suitable use of European and internationally recognised technical standards (e.g. ISO) or industry best practices, insofar as such use is fully compliant with specific supervisory instructions on the use and incorporation of international standards.	**specifically refers to any particular standard or reference which are subject to evolution over time,** it relies on the financial entities' suitable use of **the most up to date** European and internationally recognised technical standards (e.g. ISO) or industry best practices, insofar as such use is fully compliant with specific supervisory instructions on the use and incorporation of international standards.
Recital 40			
50	(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.	(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.
Recital 41			
51	(41) While this Regulation allows financial entities to determine recovery time objectives in a flexible manner and hence set such objectives by fully taking into account the nature and the criticality of the relevant function and any	(41) While this Regulation allows financial entities to determine recovery time objectives in a flexible manner and hence set such objectives by fully taking into account the nature and the criticality of the relevant function and any	(41) While this Regulation allows financial entities to determine recovery time objectives in a flexible manner and hence set such objectives by fully taking into account the nature and the criticality of the relevant function and any

	Commission Proposal	EP Mandate	Council Mandate
	specific business needs, an assessment on the potential overall impact on market efficiency should also be required when determining such objectives.	specific business needs, an assessment on the potential overall impact on market efficiency should also be required when determining such objectives.	specific business needs, an assessment on the potential overall impact on market efficiency should also be required when determining such objectives.
Recital 42			
52	(42) The significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source. To mitigate such risks and to prevent ICT systems losing integrity or becoming unavailable and confidential data being breached or physical ICT infrastructure suffering damage, the reporting of major ICT-related incidents by financial entities should be significantly improved. ICT-related incident reporting should be harmonised for all financial entities by requiring them to report to their competent authorities only. While all financial entities would be subject to this reporting, not all of them should be affected in the same manner, since relevant materiality thresholds and time frames should be calibrated to only capture major ICT-related incidents. Direct reporting would enable financial supervisors' access to information on ICT-related incidents. Nevertheless, financial supervisors should pass on this information to non-financial public authorities (NIS competent authorities, national data protection authorities and law enforcement authorities for incidents of	(42) The significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source. To mitigate such risks and to prevent ICT systems losing integrity or becoming unavailable and confidential data being breached or physical ICT infrastructure suffering damage, the reporting of major ICT-related incidents by financial entities should be significantly improved. ICT-related incident reporting should be harmonised for all financial entities by requiring them to report to their competent authorities only. While all financial entities would be subject to this reporting, not all of them should be affected in the same manner, since relevant materiality thresholds and time frames should be calibrated to only capture major ICT-related incidents. Direct reporting would enable financial supervisors' access to information on ICT-related incidents. Nevertheless, financial supervisors should pass on this information to non-financial public authorities (NIS competent authorities, national data protection authorities	(42) The significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source. To mitigate such risks and to prevent ICT systems losing integrity or becoming unavailable and confidential data being breached or physical ICT infrastructure suffering damage, the reporting of major ICT-related incidents **[and significant cyber threats]** by financial entities should be significantly improved. ICT-related incident **[and cyber threats]** reporting should be harmonised for all financial entities by requiring them to report to their competent authorities**.** **Where a financial entity is subject to the supervision of more than one national competent authority, Member States should designate a single competent authority as the receiver of such reporting. Also, credit institutions classified as significant in accordance with Article 6(4) of Regulation**

	Commission Proposal	EP Mandate	Council Mandate
	criminal nature). The ICT-related incident information should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity while the ESAs should share anonymised data on threats and vulnerabilities relating to an event to aid wider collective defence.	and law enforcement authorities for incidents of criminal nature). The ICT-related incident information should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity while the ESAs should share anonymised data on threats and vulnerabilities relating to an event to aid wider collective defence.	**(EU) No 1024/2013 should submit such reporting to the national competent authorities which should subsequently transmit the reporting to the ECB.** ~~ only.~~ While all financial entities would be subject to this reporting, not all of them should be affected in the same manner, since relevant materiality thresholds and time frames should be calibrated to only capture major ICT-related incidents **[and significant cyber threats]. In addition, credit institutions, e-money institutions, payment institutions and account information service providers, as referred to in Article 33(1) of Directive (EU) 2015/2366, will report under this Regulation all operational or security payment-related incidents, previously reported under Directive (EU) 2015/2366, irrespective of such incidents being ICT related or not**. Direct reporting would enable financial supervisors' **immediate** access to information on ICT-related incidents~~. Nevertheless,~~ **[and significant cyber threats].**Financial supervisors should **in turn** pass on this information to ~~non-financial~~ public **non-financial** authorities (NIS competent ~~authorities, national data protection~~ authorities and law enforcement authorities for **ICT-related** incidents of **a** criminal nature) **while Member States may additionally determine that competent authorities or financial entities themselves provide such information to non-financial authorities to benefit from the technical input, advice on remedies and**

	Commission Proposal	EP Mandate	Council Mandate
			subsequent follow-up from these latter authorities. The ICT-related incident **[and significant cyber threats]** information should be mutually channelled: financial supervisors should provide all necessary feedback or guidance to the financial entity while the ESAs should share anonymised data on **cyber** threats and vulnerabilities relating to an event to aid wider collective defence.
Recital 43			
53	(43) Further reflection on the possible centralisation of ICT-related incident reports should be envisaged, by means of a single central EU Hub either directly receiving the relevant reports and automatically notifying national competent authorities, or merely centralising reports forwarded by the national competent authorities and fulfilling a coordination role. The ESAs should be required to prepare, in consultation with ECB and ENISA, by a certain date a joint report exploring the feasibility of setting up such a central EU Hub.	(43) Further reflection on the possible centralisation of ICT-related incident reports should be envisaged, by means of a single ~~central~~ EU Hub ***for major ICT-related incident reporting,*** either directly receiving the relevant reports and automatically notifying national competent authorities, or merely centralising reports forwarded by the national competent authorities and fulfilling a coordination role. The ESAs should be required to prepare, in consultation with ECB and ENISA, by a certain date a joint report exploring the feasibility of setting up such a central EU Hub.	(43) Further reflection on the possible centralisation of ICT-related incident reports should be envisaged, by means of a single central EU Hub either directly receiving the relevant reports and automatically notifying national competent authorities, or merely centralising **relevant** reports forwarded by the national competent authorities and **thus** fulfilling a coordination role. The ESAs should be required to prepare, in consultation with **the** ECB and ENISA, ~~by a certain date~~ a joint report exploring the feasibility of setting up such a central EU Hub.
Recital 44			
54	(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	(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***, other***	(44) In order to achieve robust digital operational resilience, and in line with **both** international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing**) and with frameworks**

	Commission Proposal	EP Mandate	Council Mandate
	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	***than microenterprises,*** 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.	**applied in the Union, such as the TIBER-EU**, financial entities should regularly test their ICT systems and staff with **ICT - related responsibilities with** regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities. To 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~~**carry** 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~~**financial entities operating in those core** 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 **involved in cross-**

	Commission Proposal	EP Mandate	Council Mandate
	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.	TLPT) in their home Member State, and that test should include the ICT infrastructures in all jurisdictions where the cross-border group operates within the Union, thus allowing cross-border groups to incur testing costs in one jurisdiction only. ***Furthermore, in order to strengthen cooperation with trusted third countries in the field of resilience of financial entities, the Commission and competent authorities should seek to establish a framework for mutual recognition of TLPTs results.*** ***Member States should designate a single public authority to be responsible for TLPT in the financial sector at national level. The single public authority could be, inter alia, a national competent authority, or a public authority designated in accordance with Article 8 of Directive (EU) 2016/1148 (NIS). The single public authority should be responsible for issuing attestations that TLPT was undertaken in compliance with the requirements. Such attestations should facilitate mutual recognition of testing amongst competent authorities.*** ***Some financial entities have the capacity to conduct internal advanced testing, whilst others will contract external testers from within the Union or from a third country. As such, it is important that all testers are subject to the same clear requirements. In order to ensure the independence of internal testers, their use should be subject to the approval of***	**border and** 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~~**which** should include the ICT infrastructures in all jurisdictions where the cross-border **financial** group operates within the Union, thus allowing **such** cross-border **financial** groups to incur **related ICT** testing costs in one jurisdiction only.

	Commission Proposal	EP Mandate	Council Mandate
		the competent authority. ***The methodology for TLPT should not be mandated but the use of the existing TIBER-EU framework should be considered as complying with the requirements of TLPT as set out in this Regulation.*** ***Until the entry into force of this Regulation and the development and adoption by the ESAs of the mandated regulatory technical standards in respect of TLPT, financial entities should follow the relevant Union guidelines and frameworks that apply to intelligence-based penetration tests, as those will continue to apply after this Regulation comes into force.***	
Recital 44a			
54a		***(44a) The responsibility for conducting TLPT – and for cyber security management in general and cyber-attack prevention – should remain fully with the financial entity, and attestations provided by authorities should be solely for the purpose of mutual recognition and should not preclude any follow-up action on the level of ICT risk to which the financial entity is exposed nor be seen as an endorsement of its ICT risk management and mitigation capabilities.***	
Recital 45			
55			

	Commission Proposal	EP Mandate	Council Mandate
	(45) To ensure a sound monitoring of ICT third-party risk, it is necessary to lay down a set of principle-based rules to guide financial entities' monitoring of risk arising in the context of outsourced functions to ICT third-party services providers and, more generally, in the context of ICT third-party dependencies.	(45) To ensure a sound monitoring of ICT third-party risk, it is necessary to lay down a set of principle-based rules to guide financial entities' monitoring of risk arising in the context of outsourced functions to ICT third-party services providers***, particularly regarding the provision of critical or important functions by ICT third-party service providers,*** and, more generally, in the context of ICT third-party dependencies.	(45) To ensure a sound monitoring of ICT third-party risk, it is necessary to lay down a set of principle-based rules to guide financial entities' monitoring of risk arising in the context of outsourced functions to ICT third-party services providers**, particularly in regard to the use of ICT third-party service providers in the context of ICT services concerning critical or important functions** and, more generally, in the context of ICT third-party dependencies.
Recital 45a			
55a			**(45a) In order to address the complexity posed by various sources of ICT risk, and taking into account the multitude and diversity of providers of technological solutions which enable a smooth provision of financial services, this Regulation should cover a wide range of ICT third-party service providers, including providers of cloud computing services, software, data analytics services and data centres.** **In the same vein, since financial entities should identify and manage effectively and coherently all types of risk, including in the context of ICT services procured within a financial group, undertakings that are part of a financial group and provide ICT services exclusively to their parent undertaking, or to subsidiaries or branches of their parent undertaking, as well as financial entities**

	Commission Proposal	EP Mandate	Council Mandate
			providing ICT services to other financial entities, should equally be considered as ICT third party-service providers under this Regulation. **Lastly in light of the evolving payment services market becoming increasingly dependent on complex technical solutions, and in view of emerging types of payment services and payment-related solutions, participants in the payment services ecosystem, providing payment-processing activities, or operating payment infrastructures, should be equally deemed as ICT third-party service providers under this Regulation, with the exception of central banks when operating payment systems, and of public authorities when providing ICT related services in the context of fulfilling State functions.**
Recital 46			
56	(46) A financial entity should at all times remain fully responsible for complying with obligations under this Regulation. A proportionate monitoring of risk emerging at the level of the ICT third-party service provider should be organised by duly considering the scale, complexity and importance of ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a	(46) A financial entity should at all times remain fully responsible for complying with obligations under this Regulation. A proportionate monitoring of risk emerging at the level of the ICT third-party service provider should be organised by duly considering the ***nature,*** scale, complexity and importance of ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a	(46) A financial entity should at all times remain fully responsible for complying with obligations under this Regulation. A proportionate monitoring of risk emerging at the level of the ICT third-party service provider should be organised by duly considering the scale, complexity and importance of ICT-related dependencies, the criticality or importance of the services, processes or functions subject to the contractual arrangements and, ultimately, on the basis of a

	Commission Proposal	EP Mandate	Council Mandate
	careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.	careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate, ***as well as whether the ICT services are provided by an intra-group or third-party service provider***.	careful assessment of any potential impact on the continuity and quality of financial services at individual and at group level, as appropriate.
Recital 47			
57	(47) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated strategy, rooted in a continuous screening of all such ICT third-party dependencies. To enhance supervisory awareness over ICT third-party dependencies, and with a view to further support the Oversight Framework established by this Regulation, financial supervisors should regularly receive essential information from the Registers and should be able to request extracts thereof on an ad-hoc basis.	(47) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated strategy, rooted in a continuous screening of all such ICT third-party dependencies. To enhance supervisory awareness over ICT third-party dependencies, and with a view to further support the Oversight Framework established by this Regulation, financial supervisors should regularly receive essential information from the Registers and should be able to request extracts thereof on an ad-hoc basis.	(47) The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through the adoption by the financial entity's management body of a dedicated strategy, rooted in a continuous screening of all such ICT third-party dependencies. To enhance supervisory awareness over ICT third-party dependencies, and with a view to further support the Oversight Framework established by this Regulation, financial supervisors should regularly receive essential information from the registers **of information** and should be able to request extracts thereof on an ad-hoc basis.
Recital 48			
58	(48) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, while termination of contracts should be prompted by at least a set of circumstances that show shortfalls at the ICT third-party service provider.	(48) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, while ***corrective and remedial measures, which may include partial or whole*** termination of contracts should be ***taken in the case of*** ~~*prompted by*~~ at least a set of circumstances that	(48) A thorough pre-contracting analysis should underpin and precede the formal conclusion of contractual arrangements, while termination of contracts ~~should~~**could** be prompted by at least a set of circumstances that show shortfalls at the ICT third-party service provider.

	Commission Proposal	EP Mandate	Council Mandate
		show ***severe*** shortfalls at the ICT third-party service provider.	
Recital 49			
59	(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	(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*~~***Joint Oversight Body conducting*** the oversight for each critical ICT third-party provider ***and the ESA designated to conduct day-to-day oversight*** ("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	(49) To address the systemic impact of ICT third-party concentration risk, **this Regulation promotes** a balanced solution ~~through~~**by means of** a flexible and gradual approach ~~should be promoted~~**on concentration risk** since **the imposition of any** rigid caps or strict limitations may hinder ~~business~~**the** conduct **of business and restrain the**~~and~~ contractual freedom. Financial entities should thoroughly assess **their** contractual arrangements to identify the likelihood for such risk to emerge, including by means of in-depth analyses of ~~sub-outsourcing~~**subcontracting** arrangements, notably when concluded with ICT third-party service providers established in a third country. At this stage, and with a view to strike a fair balance between the imperative of preserving contractual freedom and that of guaranteeing financial stability, it is not considered appropriate to provide for strict caps and limits to ICT third-party exposures. **In the context of** ~~The ESA designated to conduct~~ the Oversight ~~for each critical ICT third-party provider (~~"**Framework,** the Lead Overseer~~")~~ should in ~~the exercise of oversight tasks~~**respect to critical ICT third-party service providers,** pay particular attention to fully grasp the magnitude of interdependences

	Commission Proposal	EP Mandate	Council Mandate
	providers where that risk is identified.[1] 1. 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.	integrity and should provide instead for a dialogue with critical ICT third-party service providers where that risk is identified[1]. 1. 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.	~~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~~**maintain** a dialogue with critical ICT third-party service providers where that **specific** risk is identified.[1] **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.** ~~1. 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.~~
Recital 50			
60	(50) To be able to evaluate and monitor on a regular basis the ability of the ICT third-party service provider to securely provide services to the financial entity without adverse effects on the latter's resilience, there should be a harmonisation of key contractual elements throughout the performance of contracts with ICT third-party providers. Those elements only cover minimum contractual aspects considered crucial for enabling full monitoring by the	(50) To be able to evaluate and monitor on a regular basis the ability of the ICT third-party service provider to securely provide services to the financial entity without adverse effects on the latter's resilience, there should be a harmonisation of key contractual elements throughout the performance of contracts with ICT third-party providers. Those elements only cover minimum contractual aspects considered crucial for enabling full monitoring by the	(50) ~~To be able~~ To evaluate and monitor on a regular basis the ability of the ICT third-party service provider to securely provide services to the financial entity without adverse effects on the latter's ~~resilience, there should be a harmonisation of~~**digital operational resilience** key contractual elements throughout the performance of contracts with ICT third-party providers **should be harmonised. Such**~~. Those~~ elements **should** only cover minimum

	Commission Proposal	EP Mandate	Council Mandate
	financial entity from the perspective of ensuring its digital resilience reliant on the stability and security of the ICT service.	financial entity from the perspective of ensuring its digital resilience reliant on the stability and security of the ICT service.	contractual aspects considered crucial for enabling **a** full monitoring by the financial entity from the perspective of ensuring its digital resilience ~~reliant~~**dependent** on the stability and security of the ICT service.
Recital 51			
61	(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.	(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 ***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.	(51) Contractual arrangements should in particular provide for a specification of **the** complete descriptions of functions and services, of locations where such functions are provided and where data ~~are~~**is to be** 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, **other elements deemed essential to enabling a financial entity's monitoring of ICT-third party risk are those contractual** provisions ~~on~~**specifying how** accessibility, availability, integrity, security and protection of personal data **are ensured by the ICT third-party service provider, provisions laying down the relevant**~~, as well as~~ guarantees for **enabling the** access, ~~recover~~**recovery** and return **of data** 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~~**, as well as provisions requiring the ICT third-party service provider to**

	Commission Proposal	EP Mandate	Council Mandate
			cooperate in the conduct of TLPTs and to provide information on the recommendations addressed to it.
Recital 52			
62	(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*~~***that*** may impair their ICT security, notice periods and reporting obligations of the ICT third-party service provider should be set out in case of developments with a potential material impact on the ICT third-party service provider's ability to effectively carry out critical or important functions, including the provision of assistance by the latter in case of an ICT-related incident ***relevant to the services being provided by the ICT third-party service provider to the financial entity at the agreed service levels*** at no additional cost or at a cost that is determined ex-ante. ***Ancillary ICT services on which the financial entities are not operationally dependent are not covered by this Regulation.*** ***Furthermore, the definition of 'critical or important function' provided for in this Regulation should encompass the definition of 'critical functions' as provided for in Article 2(1), point (35), of Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014[1]. Accordingly, functions that are critical functions pursuant to Directive (EU) 2014/59/EU should be critical or important functions within the meaning of this***	(52) To ensure that financial entities remain in full control of all **third-party** developments which may impair their ICT security, **contractual arrangements should provide for relevant** 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 **ICT services related to a** critical or important ~~functions, including the provision of assistance by the latter in case of an ICT-related incident~~**function. When an ICT-related incident occurs, contractual arrangements should require ICT third-party service providers to provide assistance,** at no additional cost**,** or at a cost that is determined ex-ante.

	Commission Proposal	EP Mandate	Council Mandate
		Regulation. _____ ***1. 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***	
Recital 53			
63	(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) ***In the case of contractual arrangements for critical or important functions,*** 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*~~***Joint Oversight Body and Lead Overseer*** 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. The financial entity and the ICT third-party service provider should be able to agree that the rights of access, inspection and audit can be delegated to an independent third party***.	(53) Rights of access, inspection and audit by the financial entity or an appointed ~~third party~~**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.
Recital 54			
64			

	Commission Proposal	EP Mandate	Council Mandate
	(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 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*~~***in-house*** solutions, consistent with the complexity of the provided service. ***Moreover, credit institutions should ensure that the relevant ICT contracts are robust and fully enforceable in the event of resolution of the credit institution. In line with the resolution authorities' expectations, credit institutions should ensure that the relevant contracts for ICT services are resolution-resilient. As long as critical or important ICT functions continue to be performed, those financial entities should ensure that the contracts contain, among other requirements, non-termination, non- suspension and non-modification clauses on the grounds of restructuring or resolution.***	(54) Contractual arrangements should provide for clear termination rights and related minimum notices**,** as well as **foresee** dedicated exit strategies ~~enabling~~**to enable**, in particular, mandatory transition periods during which~~ the~~ ICT third-party service providers should continue providing the relevant ~~functions~~**services** with a view to reduce the risk of disruptions at the level of the financial entity**, or to** ~~ or~~ allow the latter to effectively switch to **the use of** other ICT third-party service providers, or**,** alternatively resort to the use of on-premises solutions, consistent with the complexity of the provided **ICT** service.
Recital 55			
65	(55) Moreover, the voluntary use of standard contractual clauses developed by the Commission for cloud computing services may provide further comfort to the financial entities	(55) Moreover, the voluntary use of standard contractual clauses developed by the Commission for cloud computing services may provide further comfort to the financial entities	(55) ~~Moreover, the voluntary use of standard contractual clauses developed by the Commission for cloud computing services may provide further comfort to the financial entities~~

	Commission Proposal	EP Mandate	Council Mandate
	and their ICT third-party providers, by enhancing the level of legal certainty on the use of cloud computing services by the financial sector, in full alignment with requirements and expectations set out by the financial services regulation. This work builds on measures already envisaged in the 2018 Fintech Action Plan which announced Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders efforts, which the Commission has facilitated with the help of the financial sector's involvement.	and their ICT third-party providers, by enhancing the level of legal certainty on the use of cloud computing services by the financial sector, in full alignment with requirements and expectations set out by the financial services regulation. This work builds on measures already envisaged in the 2018 Fintech Action Plan ~~which~~***that*** announced Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders efforts, which the Commission has facilitated with the help of the financial sector's involvement.	~~and their ICT third-party providers, by enhancing the level of legal certainty on the use of cloud computing services by the financial sector, in full alignment with requirements and expectations set out by the financial services regulation. This work builds on measures already envisaged in the 2018 Fintech Action Plan which announced Commission's intention to encourage and facilitate the development of standard contractual clauses for the use of cloud computing services outsourcing by financial entities, drawing on cross-sectorial cloud computing services stakeholders efforts, which the Commission has facilitated with the help of the financial sector's involvement.~~
Recital 55a			
65a		***(55a) The ESAs should be mandated to draft implementing technical and regulatory standards specifying the expectations of the policies on managing ICT third-party risk and on contractual requirements. Until the entry into force of those standards, financial entities should follow relevant guidelines and other measures issued by the ESAs and competent authorities.***	
Recital 56			
66	(56) With a view to promote convergence and efficiency in relation to supervisory approaches to ICT third-party risk to the financial sector,	(56) With a view to promote convergence and efficiency in relation to supervisory approaches to ICT third-party risk to the financial sector,	(56) With a view to promote convergence and efficiency in relation to supervisory approaches to **address** ICT third-party risk ~~to~~**in** the

	Commission Proposal	EP Mandate	Council Mandate
	strengthen the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the performance of operational functions, and thus to contribute to preserving the Union's financial system stability, the integrity of the single market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework.	strengthen the digital operational resilience of financial entities ~~*which*~~***that*** rely on critical ICT third-party service providers for the performance of operational functions, and thus to contribute to preserving the Union's financial system stability, the integrity of the single market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework.	financial sector, strengthen the digital operational resilience of financial entities which rely on critical ICT third-party service providers for the performance of ~~operational~~ functions, and thus to contribute to preserving the Union's financial system stability, the integrity of the single market for financial services, critical ICT third-party service providers should be subject to a Union Oversight Framework. **While the set-up of the Oversight Framework, is justified by the added value of action at Union level and by virtue of the role and specificities of the use of ICT services in the provision of financial services, it should be kept in mind that this Regulation deals with a specific subject-matter, justifying this way of proceeding which should not be deemed as a new model for the areas of Union supervision of financial services and activities.**
Recital 57			
67	(57) Since only critical third-party service providers warrant a special treatment, a designation mechanism for the purposes of applying the Union Oversight Framework should be put in place to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers, which translates into a set of quantitative and qualitative criteria that would set the criticality parameters as a basis for inclusion into the Oversight. Critical ICT third-	(57) Since only critical third-party service providers warrant a special treatment, a designation mechanism for the purposes of applying the Union Oversight Framework should be put in place to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers, which translates into a set of quantitative and qualitative criteria that would set the criticality parameters as a basis for inclusion into the Oversight ***Framework***.	(57) Since only critical **ICT** third-party service providers warrant a special **Union monitoring** treatment, a designation mechanism for the purposes of applying the Union Oversight Framework should be put in place to take into account the dimension and nature of the financial sector's reliance on such ICT third-party service providers, which translates into a set of quantitative and qualitative criteria that would set the criticality parameters as a basis for inclusion into the Oversight.**– In order to**

	Commission Proposal	EP Mandate	Council Mandate
	party service providers which are not automatically designated by virtue of the application of the above-mentioned criteria should have the possibility to voluntary opt-in to the Oversight Framework, while those ICT third-party providers already subject to oversight mechanisms frameworks established at Eurosystem level with the aim to supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union should consequently be exempted.	Critical ICT third-party service providers ~~*which*~~***that*** are not automatically designated by virtue of the application of the above-mentioned criteria should have the possibility to voluntary opt-in to the Oversight Framework, while those ICT third-party providers already subject to oversight mechanisms frameworks ~~*established at Eurosystem level with the aim to supporting the tasks*~~ ***supporting the fulfilment of the tasks of the Eurosystem level as*** referred to in Article 127(2) of the Treaty on the Functioning of the European Union should consequently be exempted. ***Similarly, undertakings that are part of a financial group and that provide ICT services exclusively to financial entities within the same financial group should not be subject to the mechanism for being designated as critical.***	**ensure the accuracy of this assessment, regardless of the corporate structure of the ICT third-party service provider, such criteria should, in the case of a ICT third-party service provider that is part of a wider group, take into consideration the entire ICT third-party service provider's group structure.** Critical ICT third-party service providers which are not automatically designated by virtue of the application of the above-mentioned criteria should have the possibility to ~~voluntary opt-in~~**opt in** to the Oversight Framework **on a voluntary basis**, while those ICT third-party **service** providers **that are** already subject to oversight ~~mechanisms~~**mechanism** frameworks established at Eurosystem level with the aim to supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union should**, on the other hand,** ~~consequently~~ be exempted. **Similarly, financial entities which provide ICT services to other financial entities, while belonging to the category of ICT third-party service providers under this Regulation, should be exempted from the Oversight Framework since already subject to supervisory mechanisms established by the respective Union financial services legislation. Where applicable, competent authorities should take into account in their supervisory activities the ICT risks caused to financial entities by financial entities providing ICT services.**

	Commission Proposal	EP Mandate	Council Mandate
			Likewise, due to the existing risk monitoring mechanisms at group level, the same exemption should be introduced for ICT third-party service providers delivering services exclusively to entities of their group.
Recital 57a			
67a			**(57a) The digital transformation experienced in financial services has brought about an unprecedented usage of and reliance on ICT services. Since the provision of financial services has become unimaginable without cloud computing services, software solutions and data-related services, the Union financial ecosystem has become intrinsically co-dependent on certain ICT-related services provided by ICT service suppliers. Some of these companies, innovators in developing and applying ICT-based technologies, play a significant role in the delivery of financial services, or have become integrated in the financial services value chain. They have thus become critical to the stability and integrity of the Union financial system.** **This widespread reliance on the services supplied by critical ICT third-party service providers, combined with the interdependence between the information systems of different market operators, create a direct, and potentially severe, risk to the**

	Commission Proposal	EP Mandate	Council Mandate
			Union financial services system to the continuity of delivery of financial services if critical ICT third-party service providers were to be confronted with operational disruptions or major cyber incidents. Cyber incidents have a distinctive ability to multiply and propagate throughout the financial system at a considerably faster pace than other types of risk monitored in finance and can extend across sectors and beyond geographical borders. They may therefore evolve into a systemic crisis, where trust in the financial system has been eroded due to the disruption of functions supporting the real economy, or to substantial financial losses, reaching a level which the financial system either is unable to withstand, or which requires the deployment of heavy shock absorption measures. To prevent these scenarios from materialising and endangering the financial stability and integrity of the Union, the convergence of supervisory practices relating to ICT third-party risk in finance is essential, in particular through new rules enabling the Union-wide oversight of critical ICT third-party service providers. **The Oversight framework largely depends on the degree of collaboration between the Lead Overseer and critical ICT third-party service provider delivering to financial entities services affecting the supply of financial services.**

	Commission Proposal	EP Mandate	Council Mandate
			The successful conduct of the oversight is determined, among others, by the ability of the Lead Overseer to effectively conduct monitoring missions and inspections to assess the rules, controls and processes used by the critical ICT third-party service providers, as well as to assess the potential cumulative impact of their activities on financial stability and the integrity of the financial system. At the same time, it is crucial that critical ICT third-party service providers integrate the Lead Overseer's recommendations, concerns, perspectives and approaches. **Since a lack of cooperation by a critical ICT third-party service provider delivering services affecting the supply of financial services, such as the refusal to grant access to its premises or to submit information, ultimately deprives the Lead Overseer of its essential tools in appraising ICT third-party risk and could adversely impact the financial stability and the integrity of the financial system, it is necessary to provide for a commensurate sanctioning regime.**
Recital 57b			
67b			**(57b) Against this background, the need of the Lead Overseer to impose sanctions to compel critical ICT third-party service providers to comply with the set of transparency and access-related obligations should not be jeopardised by difficulties**

	Commission Proposal	EP Mandate	Council Mandate
			raised by the enforcement of those sanctions in relation to critical ICT third-party service providers established in third countries. In order to ensure the enforceability of such penalties, and as to allow a swift roll out of procedures upholding the critical ICT third-party service providers' rights of defence in the context of designation and issuance of recommendations, critical ICT third-party service providers, delivering to financial entities services affecting the supply of financial services, should maintain an adequate business presence in the Union. Due to the nature of the oversight, and the absence of comparable arrangements in other jurisdictions, there are no suitable alternative mechanisms ensuring this objective by way of effective cooperation with financial supervisors in third countries in relation to the monitoring of the impact of digital operational risks posed by systemic ICT third-party service providers. **Therefore, an ICT third-party service provider which has been designated as critical in accordance with this Regulation should undertake within 12 months of designation necessary arrangements to ensure the incorporation of a subsidiary in the Union in order to continue the provision of ICT services to financial entities in the Union.**
Recital 58			

	Commission Proposal	EP Mandate	Council Mandate
68	(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*~~*that* 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 an undertaking, such as a subsidiary constituted in the Union under the law of a Member State is intended to provide a contact point between the ICT third-party service provider, on the one hand, and the Lead Overseer and Joint Oversight Body, on the other, and to ensure that the Lead Overseer and Joint Oversight Body are able to carry out their duties and exercise their powers of oversight and enforcement as provided for in this Regulation. The contracted services of the ICT third-party service provider do not need to be performed by its entity in the Union.***	(58) ~~The~~**Such** requirement ~~of legal incorporation~~**to set up a subsidiary** in the Union**, does not prevent ICT services and related technical support to be provided from facilities and infrastructures located outside the Union. Neither does this Regulation impose** ~~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.
Recital 58a			
68a		***(58a) Due to the significant impact that designation as critical could have on ICT third-party service providers, prior hearing rights should be established as an obligation imposed on the ESAs and Joint Oversight Body to duly take into consideration any additional information provided by ICT third-party service providers in the course of the designation process.***	**(58a) Due to the significant impact of being designated as critical, such ICT third-party service providers should be granted the right to be heard prior to each designation decision.**

	Commission Proposal	EP Mandate	Council Mandate
Recital 59			
69	(59) This framework should be without prejudice to Member States' competence to conduct own oversight missions in respect to ICT third-party service providers which are not critical under this Regulation but could be deemed important at national level.	(59) ~~*This*~~***The Oversight*** framework should be without prejudice to Member States' competence to conduct own oversight missions in respect to ICT third-party service providers ~~*which*~~***that*** are not critical under this Regulation but could be deemed important at national level.	(59) ~~This~~**The Oversight** Framework should be without prejudice to Member States' competence to conduct own oversight **or monitoring** missions in respect to ICT third-party service providers which are not **designated as** critical under this Regulation but **which** could be deemed important at national level.
Recital 60			
70	(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 Subcommittee (the Oversight Forum) carrying out preparatory work for*~~***through the newly established Joint Oversight Body issuing*** 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 Subcommittee (~~the~~ Oversight Forum) carrying out preparatory work **both for the**~~for both~~ individual decisions addressed to critical ICT third-party service providers**, and for the issuance of** ~~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.
Recital 61			
71	(61) To ensure that ICT third-party service	(61) To ensure that ICT third-party service	(61) To ensure that **critical** ICT third-party

	Commission Proposal	EP Mandate	Council Mandate
	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.	providers fulfilling a critical role to the functioning of the financial sector are commensurately overseen on a Union scale, ***the Joint Oversight Body should be established to conduct direct oversight of ICT third-party service providers. Moreover,*** one of the ESAs should be designated as Lead Overseer for each critical ICT third-party service provider ***to conduct and coordinate day-to-day oversight and investigative work, to act as a single point of contact, and to ensure continuity. The Joint Oversight Body and Lead Overseer should work seamlessly to ensure efficient daily oversight as well as a holistic approach to decision-making and recommendations***.	service providers ~~fulfilling~~**are appropriately and effectively overseen on a Union scale, this Regulation provides that any of the three European Supervisory Authorities may be designated as a Union Lead Overseer. The individual assignment of** a critical ~~role to the functioning of~~ **ICT third-party service provider to one of the three ESAs should result from the preponderance of financial entities operating in** 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 providers~~**sectors for which an ESA has responsibilities. It would lead to a balanced allocation of tasks and responsibilities between the three ESAs, in the context of exercising the Oversight in order to make the best use of the human resources and technical expertise available in each of the three ESAs**.
Recital 62			
72	(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) 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) Lead Overseers should ~~enjoy~~**be granted** the necessary– powers to conduct investigations, **to carry out** onsite and offsite inspections at **the** critical ICT third-party service providers~~, access all relevant~~ premises and locations and **to** obtain complete and updated information**. This should** ~~to~~ enable ~~them~~**the Lead Overseer** to acquire real insight into the type, dimension and impact of the ICT third-party risk posed to ~~the~~ financial entities

	Commission Proposal	EP Mandate	Council Mandate
	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 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.*~~	and ultimately to the Union's financial system. Entrusting the ESAs with the lead oversight is a prerequisite for grasping and addressing the systemic dimension of ICT risk in finance. The Union footprint of critical ICT third-party service providers and the potential issues of **attached** ICT concentration risk ~~attached to it~~ call for taking a collective approach exercised at Union level. The ~~exercise~~**simultaneous conduct** of multiple audits and access rights, ~~conducted~~**performed separately** by numerous competent authorities ~~in separation~~**,** with little or no coordination would ~~not lead to~~**prevent** a complete **and comprehensive** overview on ICT third-party risk ~~while creating unnecessary~~**in the Union. It would also create** redundancy~~,~~ **and increase** burden and complexity ~~at the level of~~**for** critical ICT third-party **service** providers ~~facing such~~**if they were faced with** numerous **monitoring and inspection** requests.
Recital 62a			
72a		***(62a) Entrusting the Joint Oversight Body with direct 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.***	

	Commission Proposal	EP Mandate	Council Mandate
		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.	
Recital 63			
73	(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, Lead Overseers*~~***The Joint Oversight Body*** should be able to ~~*submit*~~***issue*** 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*~~***Joint Oversight Body*** should be duly taken into account by national competent authorities as part of their function relating to the prudential supervision of financial entities. ***Prior to the finalisation of such recommendations, critical ICT third-party service providers should be given the opportunity to provide information which they reasonably believe should be taken into account before the recommendation is finalised and issued.***	(63) In addition, **the Lead Overseer**~~Lead Overseers~~ should be able to submit recommendations on ICT risk matters and suitable remedies, ~~including opposing~~**which include the power to oppose** certain contractual arrangements ultimately affecting the stability of the financial entity or the financial system. **Critical ICT third-party service providers disagreeing with the a recommendation should be given the right to submit a reasoned explanation of their position.** **Where such explanations are deemed insufficient,** ~~Compliance with such substantive recommendations laid down by~~ the Lead ~~Overseers~~**Overseer** should ~~be duly taken into account by national~~ **issue a public notice describing summarily the matter of non-compliance.**

	Commission Proposal	EP Mandate	Council Mandate
			Competent authorities ~~as part of their function relating to the~~ **should duly integrate the task of verifying the substantive compliance with recommendations issued by the Lead Overseer in their functions of** prudential supervision of financial entities. **Competent authorities may require financial entities to take additional measures to duly tackle the risks identified in the Lead Overseer's recommendations, and should, in due course, issue notifications to that effect.** **Where recommendations are addressed to critical ICT third-party service providers that are supervised under the NIS Directive, competent authorities may, on a voluntary basis, before adopting additional measures, consult the NIS competent authorities to help foster a coordinated approach for the treatment of the respective critical ICT third-party service providers.**
Recital 63a			
73a		***(63a) In order to avoid duplication and contradictions with the technical and organisational measures that apply to critical ICT third-party service providers, Lead Overseers and the Joint Oversight Body should take due account of the framework established by Directive (EU) 2016/1148 in the exercise of their powers in accordance with the Oversight Framework in this Regulation. Before exercising such powers, the Joint Oversight***	

	Commission Proposal	EP Mandate	Council Mandate
		Body and the Lead Overseer should consult the relevant competent authorities that have jurisdiction under Directive (EU) 2016/1148.	
Recital 64			
74	(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 Any such measures should be previously coordinated and agreed in in the context of the Oversight Framework.	(64) The Oversight Framework ~~shall~~**should** not replace, or in any way ~~nor~~**or** for any part**,** substitute the ~~management by~~**requirement for** financial entities ~~of the risk~~**to manage the risks** entailed by the use of ICT third-party service providers, including the obligation of **maintaining an** ongoing monitoring of ~~their~~ contractual arrangements concluded with critical ICT third-party service providers, and ~~shall~~**should** not affect the full responsibility of ~~the~~ financial entities in complying with, and discharging of, all requirements ~~under~~**laid down by** this Regulation and **in the** relevant financial services legislation. To avoid duplications and overlaps, competent authorities should refrain from **taking** 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 exercise of tasks in** the Oversight Framework.
Recital 65			
75	(65) To promote convergence at international level on best practices to be used in the review of ICT third-party service providers' digital	(65) To promote convergence at international level on best practices to be used in the review of ICT third-party service providers' digital	(65) To promote convergence at international level on best practices to be used in the review **and monitoring** of ICT third-party service

	Commission Proposal	EP Mandate	Council Mandate
	risk-management, the ESAs should be encouraged to conclude cooperation arrangements with the relevant supervisory and regulatory third-country competent authorities to facilitate the development of best practices addressing ICT third-party risk.	risk-management, the ESAs should be encouraged to conclude cooperation arrangements with the relevant supervisory and regulatory third-country competent authorities to facilitate the development of best practices addressing ICT third-party risk.	providers' digital risk-management, the ESAs should be encouraged to conclude cooperation arrangements with ~~the~~ relevant supervisory and regulatory third-country ~~competent~~ authorities to facilitate the development of best practices addressing ICT third-party risk.
Recital 66			
76	(66) To leverage technical expertise of competent authorities' experts on operational and ICT risk management, Lead Overseers should draw on national supervisory experience and set up dedicated examination teams for each individual critical ICT third-party service provider, pooling together multidisciplinary teams to supporting both the preparation and the actual execution of oversight activities, including onsite inspections of critical ICT third-party service providers, as well as needed follow-up thereof.	(66) To leverage technical expertise of competent authorities' experts on operational and ICT risk management, Lead Overseers, ***when conducting general investigations or on-site inspections,*** should draw on national supervisory experience and set up dedicated examination teams for each individual critical ICT third-party service provider, pooling together multidisciplinary teams to supporting both the preparation and the actual execution of oversight activities, including onsite inspections of critical ICT third-party service providers, as well as needed follow-up thereof.	(66) To leverage **the specific competences and** technical **skills and** expertise of **staff specialising in operational and ICT risk, within the** competent authorities~~' experts on operational and ICT risk management, Lead Overseers~~**, the three ESAs and, on a voluntary basis, NIS authorities, the Lead Overseer** should draw on national supervisory ~~experience~~**capabilities and knowledge** and set up dedicated examination teams for each individual critical ICT third-party service provider, pooling together multidisciplinary teams ~~to supporting both~~**in support of** the preparation and ~~the actual~~ execution of oversight activities, including ~~onsite~~**for the on-site** inspections of critical ICT third-party service providers, as well as **for any** needed follow-up thereof.
Recital 67			
77	(67) Competent authorities should possess all necessary supervisory, investigative and sanctioning powers to ensure the application of	(67) Competent authorities should possess all necessary supervisory, investigative and sanctioning powers to ensure the application of	(67) Competent authorities should possess all ~~necessary~~**required** supervisory, investigative and sanctioning powers to ensure the

	Commission Proposal	EP Mandate	Council Mandate
	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[1], and consultation with the ESAs should be ensured by the mutual exchange of information and provision of assistance in the context of supervisory activities. _____ 1. 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).	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[1] , 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[2].*** _____ 1. 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). ***2. 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).***	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, **the application of this Regulation should be facilitated by** close cooperation**, on the one hand,** between the relevant competent authorities~~,~~ including **the** ECB with regard to specific tasks conferred on it by Council Regulation (EU) No 1024/2013[1] **and, on the other hand, by**~~, and~~ consultation with the ESAs ~~should be ensured by~~**through** the mutual exchange of information and **the** provision of assistance in the context of **relevant** supervisory activities. _____ 1. 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).
Recital 68			

	Commission Proposal	EP Mandate	Council Mandate
78	(68) In order to further quantify and qualify the designation criteria for critical ICT third-party service providers and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of: further specifying the systemic impact that a failure of an ICT third-party provider could have on the financial entities it serves, the numbers of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider, the number of ICT third-party service providers active on a specific market, the costs of migrating to another ICT third-party service provider, the number of Member States in which the relevant ICT third-party service provider provides services and in which financial entities using the relevant ICT third-party service provider are operating, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.[1] In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts	(68) In order to further quantify and qualify the designation criteria for critical ICT third-party service providers and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of: further specifying the systemic impact that a failure of an ICT third-party provider could have on the financial entities it serves, the numbers of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider, the number of ICT third-party service providers active on a specific market, the costs of migrating to another ICT third-party service provider, the number of Member States in which the relevant ICT third-party service provider provides services and in which financial entities using the relevant ICT third-party service provider are operating, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.[1] In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts	(68) In order to further quantify and qualify the ~~designation~~ criteria for ~~critical~~**the designation of** ICT third-party service providers **as critical** and to harmonise oversight fees, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of~~:~~ further specifying the systemic impact that a failure **or operational outage** of an ICT third-party **service** provider could have on the financial entities it ~~serves, the numbers~~**supplies, the number** of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider, the number of ICT third-party service providers active on a ~~specific~~**given** market, the costs of migrating **data and ICT workloads to other**~~to another~~ ICT third-party service provider, the number of Member States in which the relevant ICT third-party service provider ~~provides~~**delivers** services and in which financial entities using the relevant ICT third-party service provider are operating, as well as the amount of the oversight fees and the way in which they are to be paid. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April

	Commission Proposal	EP Mandate	Council Mandate
	systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. 1. OJ L 123, 12.5.2016, p. 1.	systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. 1. OJ L 123, 12.5.2016, p. 1.	2016 on Better Law-Making.[1] In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. 1. OJ L 123, 12.5.2016, p. 1.
Recital 69			
79	(69) Since this Regulation, together with Directive (EU) 20xx/xx of the European Parliament and of the Council,[1] entails a consolidation of the ICT risk management provisions spanning across multiple regulations and directives of the Union's financial services acquis, including Regulations (EC) No 1060/2009, (EU) No 648/2012 (EU) No 600/2014 and (EU) No 909/2014, in order to ensure full consistency, those Regulations should be amended to clarify that the relevant ICT risk-related provisions are laid down in this Regulation. Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. As bodies with highly specialised expertise, the ESAs should be mandated to develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the	(69) Since this Regulation, together with Directive (EU) 20xx/xx of the European Parliament and of the Council~~,~~[1], entails a consolidation of the ICT risk management provisions spanning across multiple regulations and directives of the Union's financial services acquis, including Regulations (EC) No 1060/2009, (EU) No 648/2012 (EU) No 600/2014 and (EU) No 909/2014, in order to ensure full consistency, those Regulations should be amended to clarify that the relevant ICT risk-related provisions are laid down in this Regulation. ***Relevant guidelines issued or currently being prepared by the ESAs on the application of those Regulations and Directives*** ~~*Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. As bodies with highly specialised expertise, the ESAs*~~ should be	(69) Since this Regulation, together with Directive (EU) 20xx/xx of the European Parliament and of the Council,[1] entails a consolidation of the ICT risk management provisions ~~spanning~~ across multiple regulations and directives of the Union's financial services acquis, including Regulations (EC) No 1060/2009, (EU) No 648/2012 (EU) No 600/2014 and (EU) No 909/2014, in order to ensure full consistency, those Regulations should be amended to clarify that the ~~relevant~~**applicable** ICT risk-related provisions are laid down in this Regulation. Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. ~~As~~**In their roles of** bodies **endowed** with highly specialised expertise, the ESAs should be mandated to develop draft regulatory technical standards

	Commission Proposal	EP Mandate	Council Mandate
	areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk. _____ 1. [Please insert full reference]	~~*mandated to develop draft regulatory technical standards which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk*~~***reviewed and revised as part of the consolidation process so that the legal basis for ICT risk requirements in Union law exclusively derive from this Regulation, its implementing acts and the decisions and recommendations taken in accordance therewith, concerning entities within its scope***. _____ 1. [Please insert full reference]	which do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, **major ICT-related** reporting, testing ~~and~~**as well as in relation to** key requirements for a sound monitoring of ICT third-party risk. _____ 1. [Please insert full reference]
Recital 69a			
79a		***(69a) Technical standards should ensure the consistent harmonisation of the requirements laid down in this Regulation. As bodies with highly specialised expertise, the ESAs should be mandated to develop draft regulatory technical standards that do not involve policy choices, for submission to the Commission. Regulatory technical standards should be developed in the areas of ICT risk management, reporting, testing and key requirements for a sound monitoring of ICT third-party risk. When developing draft regulatory technical standards, the ESAs should take due consideration of their mandate in relation to proportionality aspects,***	

	Commission Proposal	EP Mandate	Council Mandate
		and seek advice from their respective Advisory Committees on Proportionality, in particular in relation to the application of this Regulation to SMEs and mid-caps.	
Recital 70			
80	(70) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to the nature, scale and complexity of those entities and their activities.	(70) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to the nature, scale and complexity of those entities and their activities.	(70) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level. The Commission and the ESAs should ensure that those standards and requirements can be applied by all financial entities in a manner that is proportionate to the nature, scale and complexity of those entities and their activities.
Recital 71			
81	(71) To facilitate the comparability of major ICT-related incident reports and to ensure transparency on contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should be mandated to develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident, as well as standardized templates for the register of information. When developing those standards, the ESAs should take into account the size and complexity of financial entities, as well as the nature and level of risk of their	(71) To facilitate the comparability of major ICT-related incident reports and to ensure transparency on contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should be mandated to develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident, as well as standardized templates for the register of information. When developing those standards, the ESAs should take into account the ***nature, size, complexity and business profile***~~size and complexity~~ of financial entities,	(71) To facilitate the comparability of major ICT-related ~~incident~~**incidents, major operational or security payment-related incidents [and significant cyber threats]** reports ~~and~~**as well as** to ensure transparency on contractual arrangements for the use of ICT services provided by ICT third-party service providers, the ESAs should be mandated to develop draft implementing technical standards establishing standardised templates, forms and procedures for financial entities to report a major ICT-related incident**, a major operational or security payment-related incident or significant cyber threats**, as well

	Commission Proposal	EP Mandate	Council Mandate
	activities. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively. Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, respectively, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.	as well as the nature and level of risk of their activities. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively. Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, respectively, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.	as standardized templates for the register of information. When developing those standards, the ESAs should take into account the size and complexity of financial entities, as well as the nature and level of risk of their activities. The Commission should be empowered to adopt those implementing technical standards by means of implementing acts pursuant to Article 291 TFEU and in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively. Since further requirements have already been specified through delegated and implementing acts based on technical regulatory and implementing technical standards in Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, respectively, it is appropriate to mandate the ESAs, either individually or jointly through the Joint Committee, to submit regulatory and implementing technical standards to the Commission for adoption of delegated and implementing acts carrying over and updating existing ICT risk management rules.
Recital 72			
82	(72) This exercise will entail the subsequent amendment of existing delegated and implementing acts adopted in different areas of the financial services legislation. The scope of the operational risk articles upon which empowerments in those acts had mandated the	(72) This exercise will entail the subsequent amendment of existing delegated and implementing acts adopted in different areas of the financial services legislation. The scope of the operational risk articles upon which empowerments in those acts had mandated the	(72) This exercise will entail the subsequent ~~amendment~~**amendments** of existing delegated and implementing acts adopted in different areas of the financial services legislation. The scope of the **relevant articles related to** operational risk ~~articles~~ upon which

	Commission Proposal	EP Mandate	Council Mandate
	adoption of delegated and implementing acts should be modified with a view to carry over into this Regulation all provisions covering digital operational resilience which are today part of those Regulations.	adoption of delegated and implementing acts should be modified with a view to carry over into this Regulation all provisions covering digital operational resilience which are today part of those Regulations.	empowerments **laid down** in those acts had mandated the adoption of delegated and implementing acts should **consequently** be modified with a view to carry over into this Regulation all provisions covering **the** digital operational resilience ~~which are~~**aspects which** today **are** part of those Regulations.
Recital 72a			
82a			**(72a) The potential systemic cyber risk associated with the use of ICT infrastructures that enable the operation of payment systems and the provision of payment processing activities should be duly addressed at Union level through harmonised digital resilience rules. To that effect, the Commission should swiftly consider the need for enlarging the scope of this Regulation while aligning such review with the outcome of the comprehensive revision envisaged for the Payment Services Directive.** **Numerous large-scale attacks over the past decade demonstrate how payment systems have become an entry point for cyber threats. Placed at the core of the payment services chain and evidencing strong interconnections with the overall financial system, payment systems and payment processing activities acquired a critical significance for the functioning of the European financial markets. Cyber-attacks**

	Commission Proposal	EP Mandate	Council Mandate
			on such systems can cause severe operational business disruptions with direct repercussions on a key economic function, such the facilitation of payments, and indirect reactions on related economic processes. **Until a harmonised regime and supervision of operators of payment systems and processing entities are put in place at Union level, Member States may, with a view to apply similar market practices, draw inspiration from the digital operational resilience requirements laid down by this Regulation, when applying rules to operators of payment systems and processing entities supervised under their own jurisdictions.**
Recital 73			
83	(73) Since the objectives of this Regulation, namely to achieve a high level of digital operational resilience applicable to all financial entities, cannot be sufficiently achieved by the Member States because they require the harmonisation of a multitude of different rules, currently existing either in some Union acts, either in the legal systems of the various Member States, but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of	(73) Since the objectives of this Regulation, namely to achieve a high level of digital operational resilience applicable to all financial entities, cannot be sufficiently achieved by the Member States because they require the harmonisation of a multitude of different rules, currently existing either in some Union acts, either in the legal systems of the various Member States, but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of	(73) Since the objectives of this Regulation, namely to achieve a high level of digital operational resilience ~~applicable to all~~**for** financial entities, cannot be sufficiently achieved by the Member States because ~~they require the~~**it requires** harmonisation of ~~a multitude of different~~**different and various** rules~~, currently existing either in some~~ **in** Union acts~~, either~~ **or** in the ~~legal systems of the various~~**legislations of some** Member States, but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the

	Commission Proposal	EP Mandate	Council Mandate
	proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.
Formula			
84	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:
CHAPTER I			
85	CHAPTER I General provisions	CHAPTER I General provisions	CHAPTER I ~~General provisions~~**GENERAL PROVISIONS**
Article 1			
86	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter
Article 1(1), introductory part			
87	1. This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience, as follows:	1. This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience, as follows:	1. This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience, as follows:
Article 1(1), point (a), introductory part			

	Commission Proposal	EP Mandate	Council Mandate
88	(a) requirements applicable to financial entities in relation to:	(a) requirements applicable to financial entities in relation to:	(a) requirements applicable to financial entities in relation to:
Article 1(1), point (a), first indent			
89	- Information and Communication Technology (ICT) risk management;	- Information and Communication Technology (ICT) risk management;	- Information and Communication Technology (ICT) risk management;
Article 1(1), point (a), second indent			
90	- reporting of major ICT-related incidents to the competent authorities;	- reporting of major ICT-related incidents to the competent authorities;	- reporting of major ICT-related incidents **[and significant cyber threats]** to the competent authorities;
Article 1(1), point (a), third indent			
90a		***- reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (c);***	**- reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in points (a) to (c) of Article 2 (1);**
Article 1(1), point (a), third indent			
91	- digital operational resilience testing;	- digital operational resilience testing;	- digital operational resilience testing;
Article 1(1), point (a), fourth indent			
92	- information and intelligence sharing in relation to cyber threats and vulnerabilities;	- information and intelligence sharing in relation to cyber threats and vulnerabilities;	- information and intelligence sharing in relation to cyber threats and vulnerabilities;

	Commission Proposal	EP Mandate	Council Mandate
Article 1(1), point (a), fifth indent			
93	- measures for a sound management by financial entities of the ICT third-party risk;	- measures for ~~a~~***the*** sound management ~~***by financial entities of the***~~ ***of*** ICT third-party risk ***by financial entities***;	- measures for a sound management by financial entities of the ICT third-party risk;
Article 1(1), point (b)			
94	(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;	(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;	(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;
Article 1(1), point (c)			
95	(c) the oversight framework for critical ICT third-party service providers when providing services to financial entities;	(c) the oversight framework for critical ICT third-party service providers when providing services to financial entities;	(c) the oversight framework for critical ICT third-party service providers when providing services to financial entities;
Article 1(1), point (d)			
96	(d) rules on cooperation among competent authorities and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.	(d) rules on cooperation among competent authorities and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.	(d) rules on cooperation among competent authorities and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.
Article 1(2)			
97	2. In relation to financial entities identified as operators of essential services pursuant to national rules transposing Article 5 of Directive	2. In relation to financial entities identified as operators of essential services pursuant to national rules transposing Article 5 of Directive	2. In relation to financial entities identified as operators of essential services pursuant to national rules transposing Article 5 of Directive

	Commission Proposal	EP Mandate	Council Mandate
	(EU) 2016/1148, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 1(7) of that Directive.	(EU) 2016/1148, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 1(7) of that Directive.	(EU) 2016/1148, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 1(7) of that Directive.
Article 1(2a)			
97a		***2a. This Regulation is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security.***	**3. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.**
Article 2			
98	Article 2 Personal scope	Article 2 Personal scope	Article 2 Personal scope
Article 2(1), introductory part			
99	1. This Regulation applies to the following entities:	1. This Regulation applies to the following entities:	1. **Without prejudice to paragraphs 3 and 4,** this Regulation applies to the following entities:
Article 2(1), point (a)			
100	(a) credit institutions,	(a) credit institutions,	(a) credit institutions,
Article 2(1), point (b)			
101	(b) payment institutions,	(b) payment institutions,	(b) payment institutions, **including payment institutions exempted in accordance with**

	Commission Proposal	EP Mandate	Council Mandate
			Article 32 (1) of Directive (EU) 2015/2366,
Article 2(1), point (ba)			
101a			**(ba) account information service providers,**
Article 2(1), point (c)			
102	(c) electronic money institutions,	(c) electronic money institutions,	(c) electronic money institutions, **including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC,**
Article 2(1), point (d)			
103	(d) investment firms,	(d) investment firms,	(d) investment firms,
Article 2(1), point (e)			
104	(e) crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens,	(e) crypto-asset service providers, issuers ***and offerors*** of crypto-assets, issuers ***and offerors*** of asset-referenced tokens and issuers of significant asset-referenced tokens,	(e) crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens,
Article 2(1), point (f)			
105	(f) central securities depositories,	(f) central securities depositories ***and operators of securities settlement systems***,	(f) central securities depositories,
Article 2(1), point (g)			

	Commission Proposal	EP Mandate	Council Mandate
106	(g) central counterparties,	(g) central counterparties,	(g) central counterparties,
Article 2(1), point (h)			
107	(h) trading venues,	(h) trading venues,	(h) trading venues,
Article 2(1), point (i)			
108	(i) trade repositories,	(i) trade repositories,	(i) trade repositories,
Article 2(1), point (j)			
109	(j) managers of alternative investment funds,	(j) managers of alternative investment funds,	(j) managers of alternative investment funds,
Article 2(1), point (k)			
110	(k) management companies,	(k) management companies,	(k) management companies,
Article 2(1), point (l)			
111	(l) data reporting service providers,	(l) data reporting service providers,	(l) data reporting service providers,
Article 2(1), point (m)			
112	(m) insurance and reinsurance undertakings,	(m) insurance and reinsurance undertakings,	(m) insurance and reinsurance undertakings,
Article 2(1), point (n)			
113			

	Commission Proposal	EP Mandate	Council Mandate
	(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,	(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries ***that are not micro, small or medium-sized enterprises unless those micro, small or medium sized-enterprises rely exclusively on organised automated sales systems***,	(n) insurance intermediaries~~, reinsurance intermediaries and ancillary insurance~~ **and reinsurance** intermediaries,
Article 2(1), point (o)			
114	(o) institutions for occupational retirement pensions,	(o) institutions for occupational retirement ~~*pensions*~~***provisions (IORPs) that do not operate pension schemes having together fewer than 15 members***,	(o) institutions for occupational retirement ~~pensions~~**provision**,
Article 2(1), point (p)			
115	(p) credit rating agencies,	(p) credit rating agencies,	(p) credit rating agencies,
Article 2(1), point (q)			
116	(q) statutory auditors and audit firms,	(q) statutory auditors and audit firms ***that are not micro, small or medium-sized enterprises unless such micro, small or medium-sized enterprises provide auditing services to entities listed in this Article with the exception of micro, small or medium-sized enterprises that are non-profit-making auditing entities pursuant to Article 2(3) of Regulation (EU) No 537/2014 unless the competent authority decides that the exception is not valid***,	(q) ~~statutory auditors and audit firms,~~

	Commission Proposal	EP Mandate	Council Mandate
Article 2(1), point (r)			
117	(r) administrators of critical benchmarks,	(r) administrators of critical benchmarks,	(r) administrators of critical benchmarks,
Article 2(1), point (s)			
118	(s) crowdfunding service providers,	(s) crowdfunding service providers,	(s) crowdfunding service providers,
Article 2(1), point (t)			
119	(t) securitisation repositories,	(t) securitisation repositories,	(t) securitisation repositories,
Article 2(1), point (u)			
120	(u) ICT third-party service providers.	(u) ICT third-party service providers.	(u) ICT third-party service providers.
Article 2(1a)			
120a		***1a. This Regulation, with the exception of Section II of Chapter V, also applies to ICT intra-group service providers.***	
Article 2(2)			
121	2. For the purposes of this Regulation, entities referred to in paragraph (a) to (t) shall collectively be referred to as 'financial entities'.	2. For the purposes of this Regulation, entities referred to in paragraph (a) to (t) shall collectively be referred to as 'financial entities'.	2. For the purposes of this Regulation, entities referred to in paragraph (a) to (t) shall collectively be referred to as 'financial entities'.
Article 2(2a)			
121a			

	Commission Proposal	EP Mandate	Council Mandate
		2a. For the purposes of this Regulation, with the exception of Section II of Chapter V, ICT third-party service providers and ICT intra-group service providers shall be collectively referred to as 'ICT third-party service providers'.	
Article 2(3), introductory part			
121b			**3. This Regulation shall not apply to:**
Article 2(3), point (a)			
121c			**(a) managers of alternative investment funds referred to in Article 3 (2) of Directive 2011/61/EU;**
Article 2(3), point (b)			
121d			**(b) insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC;**
Article 2(3), point (c)			
121e			**(c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;**
Article 2(3), point (d)			

	Commission Proposal	EP Mandate	Council Mandate
121f			**(d) natural or legal persons exempted from the application of Directive 2014/65/EU pursuant to Articles 2 and 3 of that Directive;**
Article 2(3), point (e)			
121g			**(e) insurance intermediaries which are a microenterprise or a small enterprise, in accordance with points (50) and (54) of Article 3;**
Article 2(3), point (f)			
121h			**(f) reinsurance intermediaries which are a microenterprise or a small enterprise, in accordance with points (50) and (54) of Article 3;**
Article 2(4)			
121i			**4. Member States may exempt institutions referred to in points (3) to (23) of Article 2(5) of Directive 2013/36/EU that are located within their respective territory from the scope of this Regulation. In case such option is exercised, this Regulation shall not apply to the exempted institutions.** **Where a Member State makes use of such option, it shall inform the Commission**

	Commission Proposal	EP Mandate	Council Mandate
			thereof as well as of any subsequent changes. The Commission shall make the information public on a website or other easily accessible means.
Article 3			
122	Article 3 Definitions	Article 3 Definitions	Article 3 Definitions
Article 3, first paragraph, introductory part			
123	For the purposes of this Regulation, the following definitions shall apply:	For the purposes of this Regulation, the following definitions shall apply:	For the purposes of this Regulation, the following definitions shall apply:
Article 3, first paragraph, point (1)			
124	(1) 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality;	(1) 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity ~~*from a technological perspective*~~ by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, ~~*the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of*~~ ***the continued provision of financial services and their quality in the face of operational disruptions impacting the*** financial ~~*services and their quality*~~***entity's ICT capabilities***;	(1) 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity **and reliability** from a technological perspective by ensuring, either directly**,** or indirectly~~,~~ through the use of services of ICT third-party **service** providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality;

	Commission Proposal	EP Mandate	Council Mandate
Article 3, first paragraph, point (2)			
125	(2) 'network and information system' means network and information system as defined in point (1) of Article 4 of Directive (EU) No 2016/1148;	(2) 'network and information system' means network and information system as defined in point (1) of Article 4 of Directive (EU) No 2016/1148;	(2) 'network and information system' means network and information system as defined in point (1) of Article 4 of Directive (EU) No 2016/1148;
Article 3, first paragraph, point (2a)			
125a			**(2a) "legacy ICT system" means an ICT system that has reached the end of its lifecycle (end-of-life), that it is unsuitable for upgrades and fixes or no longer supported by its vendor or an ICT third-party service provider, but is still in use and supports the business functions of the financial entity;**
Article 3, first paragraph, point (3)			
126	(3) 'security of network and information systems' means security of network and information systems as defined in point (2) of Article 4 of Directive (EU) No 2016/1148;	(3) 'security of network and information systems' means security of network and information systems as defined in point (2) of Article 4 of Directive (EU) No 2016/1148;	(3) 'security of network and information systems' means security of network and information systems as defined in point (2) of Article 4 of Directive (EU) No 2016/1148;
Article 3, first paragraph, point (4)			
127	(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	(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~~	(4) 'ICT risk' means any reasonably identifiable circumstance ~~in relation to the use of~~**for event having a potential adverse effect on the** network and information systems, - including a malfunction, capacity overrun,

	Commission Proposal	EP Mandate	Council Mandate
	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;	~~*type of malicious or non-malicious event -*~~ which, if materialised, may compromise the security of the network and information systems, of any ~~*technology-dependant*~~***ICT-dependent*** tool or process, of the operation and process' running, or of the provision of services~~*, thereby compromising the integrity or availability of data, software or any other component of ICT services and infrastructures, or causing a breach of confidentiality, a damage to physical ICT infrastructure or other adverse effects*~~;	failure, disruption, impairment, misuse, loss or other type of malicious or non-malicious event - which, if materialised, may compromise the security **or functioning** 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;
Article 3, first paragraph, point (5)			
128	(5) 'information asset' means a collection of information, either tangible or intangible, that is worth protecting;	(5) 'information asset' means a collection of information, either tangible or intangible, that is worth protecting;	(5) 'information asset' means a collection of information, either tangible or intangible, that is worth protecting;
Article 3, first paragraph, point (5a)			
128a			**(5a) 'ICT asset' means a software or hardware asset in the network and information systems used by the financial entity;**
Article 3, first paragraph, point (6)			
129	(6) 'ICT-related incident' means an unforeseen identified occurrence in the network and information systems, whether resulting from	(6) 'ICT-related incident' means an unforeseen identified ~~*occurrence in the network and information systems, whether resulting from*~~	(6) 'ICT-related incident' means ~~an unforeseen identified occurrence in the network and information systems, whether resulting from~~

	Commission Proposal	EP Mandate	Council Mandate
	malicious activity or not, which compromises the security of network and information systems, of the information that such systems process, store or transmit, or has adverse effects on the availability, confidentiality, continuity or authenticity of financial services provided by the financial entity;	~~*malicious activity or not*~~***incident, or a series of linked incidents***, which compromises the security of network and information systems~~*, of the information that such systems process, store or transmit, or has*~~ ***or having*** adverse effects on the availability, confidentiality, continuity***,*** ***integrity*** or authenticity of financial services provided by the financial entity;	~~malicious activity or not, which compromises the security of~~**a singular event or a series of linked events unplanned by the financial entity in the** network and information systems, ~~of the information that such systems process, store or transmit, or has~~**which has an** adverse ~~effects~~**impact** on the **integrity,** availability, confidentiality, continuity ~~or~~**and/or** authenticity of financial services provided by the financial entity;
Article 3, first paragraph, point (6a)			
129a		***(6a) 'operational or security payment-related incident' means an event or a series of linked occurrences unforeseen by the financial entities referred to in Article 2(1), points (a) to (c) that has or is likely to have an adverse impact on the integrity, availability, confidentiality, authenticity or continuity of payment-related services;***	**(6a) 'operational or security payment-related incident', means a singular event or a series of linked events, ICT-related or not, unplanned by financial entities referred to in points (a) to (c) of Article 2(1) which has an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services;**
Article 3, first paragraph, point (7)			
130	(7) 'major ICT-related incident' means an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity;	(7) 'major ICT-related incident' means an ICT-related incident ~~*with a potentially*~~***that has or is likely to have a*** high adverse impact on the network and information systems that support critical functions of the financial entity;	(7) 'major ICT-related incident' means an ICT-related incident ~~with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity~~**which meets the criteria set out in accordance with Article 16(2)(a)**;
Article 3, first paragraph, point (7a)			

	Commission Proposal	EP Mandate	Council Mandate
130a		***(7a) 'major operational or security payment-related incident' means an operational or security payment-related incident that meets the criteria set out in Article 16;***	**(7a) 'major operational or security payment-related incident' means an operational or security payment-related incident which meets the criteria set out in accordance with Article 16(2)(a);**
Article 3, first paragraph, point (8)			
131	(8) 'cyber threat' means 'cyber threat' as defined in point (8) of Article 2 Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; _____ 1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p. 15).	(8) 'cyber threat' means 'cyber threat' as defined in point (8) of Article 2 Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; _____ 1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p. 15).	(8) 'cyber threat' means 'cyber threat' as defined in point (8) of Article 2 Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; _____ 1. **[1]** Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p. 15).
Article 3, first paragraph, point (8a)			
131a		***(8a) 'significant cyber threat' means a cyber threat the characteristics of which clearly indicate that it is likely to result in a major ICT-related incident;***	**(8a) ['significant cyber threat' means a cyber threat whose characteristics clearly indicate that it could likely result in a major ICT-related incident or a major operational or security payment-related incident.]**
Article 3, first paragraph, point (9)			
132	(9) 'cyber-attack' means a malicious ICT-related incident by means of an attempt to destroy, expose, alter, disable, steal or gain	(9) 'cyber-attack' means a malicious ICT-related incident by means of an attempt to destroy, expose, alter, disable, steal or gain	(9) 'cyber-attack' means a malicious ICT-related incident **caused** by means of an attempt to destroy, expose, alter, disable, steal or gain

	Commission Proposal	EP Mandate	Council Mandate
	unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor;	unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor;	unauthorized access to or make unauthorized use of an asset perpetrated by any threat actor;
Article 3, first paragraph, point (10)			
133	(10) 'threat intelligence' means information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and which brings relevant and sufficient understanding for mitigating the impact of an ICT-related incident or cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations;	(10) 'threat intelligence' means information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and ~~*which*~~***that*** brings relevant and sufficient understanding for mitigating the impact of an ICT-related incident or cyber threat, including the technical details of a cyber-attack, those responsible for the attack and their modus operandi and motivations;	(10) 'threat intelligence' means information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making and which brings relevant and sufficient understanding for mitigating the impact of an ICT-related incident or **a** cyber threat, including the technical details of a cyber-attack, those responsible for ~~the attack~~**it** and their modus operandi and motivations;
Article 3, first paragraph, point (11)			
134	(11) 'defence-in-depth' means an ICT-related strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the entity;	(11) 'defence-in-depth' means an ICT-related strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the entity;	(11) 'defence-in-depth' means an ICT-related strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the **financial** entity;
Article 3, first paragraph, point (12)			
135	(12) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a threat;	(12) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a ***cyber*** threat;	(12) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a **cyber** threat;
Article 3, first paragraph, point (13)			

	Commission Proposal	EP Mandate	Council Mandate
136	(13) 'threat led penetration testing' means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the entity's critical live production systems;	(13) 'threat led penetration testing' means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the entity's critical live production systems;	(13) 'threat led penetration testing' means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the **financial** entity's critical live production systems;
Article 3, first paragraph, point (14)			
137	(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 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 or by ~~further sub-contractors~~**subcontractors** of the latter**, including through outsourcing arrangements**;
Article 3, first paragraph, point (15)			
138	(15) 'ICT third-party service provider' means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council[1]; 1. Directive (EU) 2018/1972 of the European Parliament	(15) 'ICT third-party service provider' means an undertaking providing ~~*digital and data*~~***ICT services, including a financial entity providing ICT*** services~~*, including providers of cloud computing services, software, data analytics services, data centres,*~~ ***that forms part of an undertaking that provides a wider range of products or services*** but excluding providers of hardware components and undertakings authorised under Union law ~~*which*~~***that*** provide electronic communication services as defined referred to in point (4) of Article 2 of Directive	(15) 'ICT third-party service provider' means an undertaking providing ~~digital and data services, including providers of cloud computing~~**ICT** services, ~~software, data analytics services, data centres, but~~ excluding ~~providers of hardware components and~~ undertakings authorised under Union law which provide electronic communication services as defined ~~referred to~~ in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council[1]; ~~1. Directive (EU) 2018/1972 of the European Parliament~~

	Commission Proposal	EP Mandate	Council Mandate
	and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)(OJ L 321, 17.12.2018, p. 36).	(EU) 2018/1972 of the European Parliament and of the Council[1]; _____ 1. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)(OJ L 321, 17.12.2018, p. 36).	~~and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)(OJ L 321, 17.12.2018, p. 36).~~
Article 3, first paragraph, point (15a)			
138a		***(15a) 'ICT intra-group service provider' means an undertaking that is part of a financial group and that provides ICT services, exclusively to financial entities within the same group or to financial entities belonging to the same institutional protection scheme, including to their parent undertakings, subsidiaries, branches or other entities that are under common ownership or control;***	
Article 3, first paragraph, point (16)			
139	(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~~, *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*~~ ***on an ongoing basis, excluding telecommunication contracts***;	(16) 'ICT services' means digital and data services provided through the ICT systems to one or more internal or external users, **on an ongoing-basis,** including provision of **cloud computing services,** data, data entry, data storage, data processing and reporting services, data monitoring as well as data based business and decision support services**, hardware as a service and hardware services which include technical support via software or firmware updates by the hardware provider**;

	Commission Proposal	EP Mandate	Council Mandate
Article 3, first paragraph, point (17)			
140	(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 ***an activity or service that is essential to the operation of a financial entity and the disruption of which would materially impair the soundness or continuity of the financial entity's services and activities, or*** ~~*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*~~***including 'critical functions' as defined in Article 2, paragraph 1, point 35, of Directive 2014/59/EU***;	(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;
Article 3, first paragraph, point (18)			
141	(18) 'critical ICT third-party service provider' means an ICT third-party service provider designated in accordance with Article 29 and subject to the Oversight Framework referred to in Articles 30 to 37;	(18) 'critical ICT third-party service provider' means an ICT third-party service provider designated in accordance with Article ~~29~~***28*** and subject to the Oversight Framework referred to in Articles ~~30~~***29*** to 37;	(18) 'critical ICT third-party service provider' means an ICT third-party service provider designated in accordance with Article ~~29~~**28** and subject to the Oversight Framework referred to in Articles ~~30 to 37~~**29 to 36**;
Article 3, first paragraph, point (19)			
142	(19) 'ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal	(19) 'ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal	(19) 'ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal

	Commission Proposal	EP Mandate	Council Mandate
	person established in a third-country, has not set up business/presence in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services;	person established in a third-country~~, *has not set up business/presence in the Union,*~~ and has entered into a contractual arrangement with a financial entity for the provision of ICT services;	person established in a ~~third-country, has not set up business/presence in the Union, and~~**third country, that** has entered into a contractual arrangement with a financial entity for the provision of ICT services;
Article 3, first paragraph, point (19a)			
142a			**(19a) "subsidiary" means a subsidiary undertaking as defined in point (10) of Article 2 of Directive 2013/34/EU of the European Parliament and of the Council;**
Article 3, first paragraph, point (19b)			
142b			**(19b) "group" means a group as defined in point (11) of Article 2 of Directive 2013/34/EU of the European Parliament and of the Council;**
Article 3, first paragraph, point (19c)			
142c			**(19c) "parent undertaking" means a parent undertaking as defined in point (9) of Article 2 of Directive 2013/34/EU of the European Parliament and of the Council;**
Article 3, first paragraph, point (20)			
143	(20) 'ICT sub-contractor established in a third country' means an ICT sub-contractor that is a legal person established in a third-country, has	(20) 'ICT sub-contractor established in a third country' means an ICT sub-contractor that is a legal person established in a third-country, ~~*has*~~	(20) 'ICT ~~sub-contractor~~**subcontractor** established in a third country' means an ICT ~~sub-contractor~~**subcontractor** that is a legal

	Commission Proposal	EP Mandate	Council Mandate
	not set up business/presence in the Union and has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;	~~not set up business/presence in the Union~~ and has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;	person established in a third-country~~, has not set up business/presence in the Union and~~ **that** has entered into a contractual arrangement either with an ICT third-party service provider, or with an ICT third-party service provider established in a third country;
Article 3, first paragraph, point (21)			
144	(21) 'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of the latter may potentially endanger the ability of a financial entity, and ultimately of the Union's financial system as a whole, to deliver critical functions, or to suffer other type of adverse effects, including large losses;	(21) 'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of the latter may potentially endanger the ~~ability of a financial entity, and ultimately of the Union's financial system as a whole,~~ ***financial stability of the Union as a whole or the ability of a financial entity*** to deliver critical ***or important*** functions, or to suffer other type of adverse effects, including large losses;	(21) 'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of the latter may potentially endanger the ability of a financial entity, and ultimately of the Union's financial system as a whole, to deliver critical **or important** functions, or to suffer other type of adverse effects, including large losses;
Article 3, first paragraph, point (22)			
145	(22) 'management body' means a management body as defined in point (36) of Article 4(1) of Directive 2014/65/EU, point (7) of Article 3(1) of Directive 2013/36/EU, point (s) of Article 2(1) of Directive 2009/65/EC, point (45) of Article 2(1) of Regulation (EU) No 909/2014, point (20) of Article 3(1) of Regulation (EU) 2016/1011 of the European Parliament and of	(22) 'management body' means a management body as defined in point (36) of Article 4(1) of Directive 2014/65/EU, point (7) of Article 3(1) of Directive 2013/36/EU, point (s) of Article 2(1) of Directive 2009/65/EC, point (45) of Article 2(1) of Regulation (EU) No 909/2014, point (20) of Article 3(1) of Regulation (EU) 2016/1011 of the European Parliament and of	(22) 'management body' means a management body as defined in point (36) of Article 4(1) of Directive 2014/65/EU, point (7) of Article 3(1) of Directive 2013/36/EU, point (s) of Article 2(1) of Directive 2009/65/EC, point (45) of Article 2(1) of Regulation (EU) No 909/2014, point (20) of Article 3(1) of Regulation (EU) 2016/1011 of the European Parliament and of

	Commission Proposal	EP Mandate	Council Mandate
	the Council[1], point (u) of Article 3(1) of Regulation (EU) 20xx/xx of the European Parliament and of the Council[2] [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation; ___ 1. Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1). 2. [please insert full title and OJ details]	the Council[1], point ~~(u)~~***(18)*** of Article 3(1) of Regulation (EU) 20xx/xx of the European Parliament and of the Council[2] [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation; ___ 1. Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1). 2. [please insert full title and OJ details]	the Council[1], point (u) of Article 3(1) of Regulation (EU) 20xx/xx of the European Parliament and of the Council[2] [MICA] or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national legislation; ___ 1. Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1). 2. [please insert full title and OJ details]
Article 3, first paragraph, point (23)			
146	(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[1]; ___ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).	(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[1]; ___ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).	(23) ‘credit institution’ means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[1]; ___ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).
Article 3, first paragraph, point (23a)			
146a		***(23a) ‘credit institution exempted by Directive 2013/36/EU’ means an institution benefiting from an exemption pursuant to Article 2(5), points (4) to (23), of Directive 2013/36/EU;***	

	Commission Proposal	EP Mandate	Council Mandate
Article 3, first paragraph, point (23a)			
146b			**(23a) 'institution exempted under Directive 2013/36/EU' means a institution as referred to in points (3) to (23) of Article 2(5) of Directive 2013/36/EU;**
Article 3, first paragraph, point (24)			
147	(24) 'investment firm' means an investment firm as defined in point (1) of Article 4(1) of Directive 2014/65/EU;	(24) 'investment firm' means an investment firm as defined in point (1) of Article 4(1) of Directive 2014/65/EU;	(24) 'investment firm' means an investment firm as defined in point (1) of Article 4(1) of Directive 2014/65/EU;
Article 3, first paragraph, point (24a)			
147a		***(24a) 'small and non-interconnected investment firm' means an investment firm that meets the conditions laid out in Article 12 (1) of Regulation (EU) 2019/2033;***	**(24a) 'small and non-interconnected investment firm' means an investment firm that meets the conditions laid out in Article 12 (1) of Regulation (EU) 2019/2033;**
Article 3, first paragraph, point (25)			
148	(25) 'payment institution' means a payment institution as defined in point (d) of Article 1(1) of Directive (EU) 2015/2366;	(25) 'payment institution' means a payment institution as defined in point (d) of Article 1(1) of Directive (EU) 2015/2366;	(25) 'payment institution' means a payment institution as defined in point ~~(d)~~**(4)** of Article ~~1(1)~~**4** of Directive (EU) 2015/2366;
Article 3, first paragraph, point (25a)			
148a		***(25a) 'payment institution exempted by Directive (EU) 2015/2366' means a payment institution benefitting from an exemption***	**(25a) 'payment institution exempted under Directive (EU) 2015/2366' means a payment institution benefiting from an exemption**

	Commission Proposal	EP Mandate	Council Mandate
		pursuant to Article 32 (1) of Directive (EU) 2015/2366;	**pursuant to Article 32 (1) of Directive (EU) 2015/2366;**
Article 3, first paragraph, point (25b)			
148b			**(25b) ‘account information service providers’ means an account information service provider as referred to in Article 33(1) of Directive (EU) 2015/2366;**
Article 3, first paragraph, point (26)			
149	(26) ‘electronic money institution’ means an electronic money institution as defined in point (1) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[1]; __________ 1. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).	(26) ‘electronic money institution’ means an electronic money institution as defined in point (1) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[1]; __________ 1. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).	(26) ‘electronic money institution’ means an electronic money institution as defined in point (1) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[1]; __________ 1. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).
Article 3, first paragraph, point (26a)			
149a		***(26a) ‘electronic money institution exempted by Directive 2009/110/EC’ means an electronic money institution benefitting from a waiver under Article 9 of Directive 2009/110/EC;***	**(26a) ‘electronic money institution exempted under Directive 2009/110/EC’ means an electronic money institution benefiting from an exemption pursuant to Article 9 of Directive 2009/110/EC;**
Article 3, first paragraph, point (27)			

	Commission Proposal	EP Mandate	Council Mandate
150	(27) 'central counterparty' means a central counterparty as defined in point (1) of Article 2 of Regulation (EU) No 648/2012;	(27) 'central counterparty' means a central counterparty as defined in point (1) of Article 2 of Regulation (EU) No 648/2012;	(27) 'central counterparty' means a central counterparty as defined in point (1) of Article 2 of Regulation (EU) No 648/2012;
Article 3, first paragraph, point (28)			
151	(28) 'trade repository' means a trade repository' as defined in point (2) of Article 2 of Regulation (EU) No 648/2012;	(28) 'trade repository' means a trade repository' as defined in point (2) of Article 2 of Regulation (EU) No 648/2012;	(28) 'trade repository' means a trade repository' as defined in point (2) of Article 2 of Regulation (EU) No 648/2012;
Article 3, first paragraph, point (29)			
152	(29) 'central securities depository' means a central securities as defined in point (1) of Article 2(1) of Regulation 909/2014;	(29) 'central securities depository' means a central securities as defined in point (1) of Article 2(1) of Regulation 909/2014;	(29) 'central securities depository' means a central securities **depository** as defined in point (1) of Article 2(1) of Regulation 909/2014;
Article 3, first paragraph, point (30)			
153	(30) 'trading venue' means a trading venue as defined in point (24) of Article 4(1) of Directive 2014/65/EU;	(30) 'trading venue' means a trading venue as defined in point (24) of Article 4(1) of Directive 2014/65/EU;	(30) 'trading venue' means a trading venue as defined in point (24) of Article 4(1) of Directive 2014/65/EU;
Article 3, first paragraph, point (31)			
154	(31) 'manager of alternative investment funds' means a manager of alternative investment funds as defined in point (b) of Article 4(1) of Directive 2011/61/EU;	(31) 'manager of alternative investment funds' means a manager of alternative investment funds as defined in point (b) of Article 4(1) of Directive 2011/61/EU;	(31) 'manager of alternative investment funds' means a manager of alternative investment funds as defined in point (b) of Article 4(1) of Directive 2011/61/EU;
Article 3, first paragraph, point (32)			

	Commission Proposal	EP Mandate	Council Mandate
155	(32) 'management company' means a management company as defined in point (b) of Article 2(1) of Directive 2009/65/EC;	(32) 'management company' means a management company as defined in point (b) of Article 2(1) of Directive 2009/65/EC;	(32) 'management company' means a management company as defined in point (b) of Article 2(1) of Directive 2009/65/EC;
Article 3, first paragraph, point (33)			
156	(33) 'data reporting service provider' means a data reporting service provider as defined in point (63) of Article (4)(1) of Directive 2014/65/EU;	(33) 'data reporting service provider' means a data reporting service provider as defined in point (63) of Article (4)(1) of Directive 2014/65/EU;	(33) 'data reporting service provider' means a data reporting service provider as defined in point (63) of Article (4)(1) of Directive 2014/65/EU;
Article 3, first paragraph, point (34)			
157	(34) 'insurance undertaking' means an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC;	(34) 'insurance undertaking' means an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC;	(34) 'insurance undertaking' means an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC;
Article 3, first paragraph, point (35)			
158	(35) 'reinsurance undertaking' means a reinsurance undertaking as defined in point (4) of Article 13 of Directive 2009/138/EC;	(35) 'reinsurance undertaking' means a reinsurance undertaking as defined in point (4) of Article 13 of Directive 2009/138/EC;	(35) 'reinsurance undertaking' means a reinsurance undertaking as defined in point (4) of Article 13 of Directive 2009/138/EC;
Article 3, first paragraph, point (36)			
159	(36) 'insurance intermediary' means insurance intermediary as defined in point (3) of Article 2 of Directive (EU) 2016/97;	(36) 'insurance intermediary' means insurance intermediary as defined in point (3) of Article 2 ***(1)*** of Directive (EU) 2016/97;	(36) 'insurance intermediary' means **an** insurance intermediary as defined in point (3) **of paragraph 1** of Article 2 of Directive (EU) 2016/97;

	Commission Proposal	EP Mandate	Council Mandate
Article 3, first paragraph, point (37)			
160	(37) 'ancillary insurance intermediary' means ancillary insurance intermediary as defined in point (4) of Article 2 of Directive (EU) 2016/97;	(37) 'ancillary insurance intermediary' means ***an*** ancillary insurance intermediary as defined in point (4) of Article 2 ***(1)*** of Directive (EU) 2016/97;	(37) ~~'ancillary insurance intermediary' means ancillary insurance intermediary as defined in point (4) of Article 2 of Directive (EU) 2016/97;~~
Article 3, first paragraph, point (38)			
161	(38) 'reinsurance intermediary' means reinsurance intermediary as defined in point (5) of Article 2 of Directive (EU) 2016/97;	(38) 'reinsurance intermediary' means reinsurance intermediary as defined in point (5) of Article 2 ***(1)*** of Directive (EU) 2016/97;	(38) 'reinsurance intermediary' means **a** reinsurance intermediary as defined in point (5) **of paragraph 1** of Article 2 of Directive (EU) 2016/97;
Article 3, first paragraph, point (39)			
162	(39) 'institution for occupational retirement pensions' means institution for occupational retirement pensions as defined in point (6) of Article 1 of Directive 2016/2341;	(39) 'institution for occupational retirement pensions' means institution for occupational retirement pensions as defined in point (6) of Article 1 of Directive 2016/2341;	(39) '~~institution~~**institutions** for occupational retirement ~~pensions~~**provision**' means **an** institution for occupational retirement ~~pensions~~**provision** as defined in point ~~(6)~~**(1)** of Article ~~1~~**6** of Directive 2016/2341;
Article 3, first paragraph, point (39a)			
162a			**(39a) 'small institution for occupational retirement provision' means an institution for occupational retirement provision as defined in point (39), which operates pension schemes which together have less than 100 members in total;**
Article 3, first paragraph, point (40)			

	Commission Proposal	EP Mandate	Council Mandate
163	(40) 'credit rating agency' means a credit rating agency as defined in point (a) of Article 3(1) of Regulation (EC) No 1060/2009;	(40) 'credit rating agency' means a credit rating agency as defined in point (a) of Article 3(1) of Regulation (EC) No 1060/2009;	(40) 'credit rating agency' means a credit rating agency as defined in point (a) of Article 3(1) of Regulation (EC) No 1060/2009;
Article 3, first paragraph, point (41)			
164	(41) 'statutory auditor' means statutory auditor as defined in point (2) of Article 2 of Directive 2006/43/EC;	(41) 'statutory auditor' means statutory auditor as defined in point (2) of Article 2 of Directive 2006/43/EC;	(41) ~~'statutory auditor' means statutory auditor as defined in point (2) of Article 2 of Directive 2006/43/EC;~~
Article 3, first paragraph, point (42)			
165	(42) 'audit firm' means an audit firm as defined in point (3) of Article 2 of Directive 2006/43/EC;	(42) 'audit firm' means an audit firm as defined in point (3) of Article 2 of Directive 2006/43/EC;	(42) ~~'audit firm' means an audit firm as defined in point (3) of Article 2 of Directive 2006/43/EC;~~
Article 3, first paragraph, point (43)			
166	(43) 'crypto-asset service provider' means crypto-asset service provider as defined in point (n) of Article 3(1) of Regulation (EU) 202x/xx [PO: insert reference to MICA Regulation];	(43) 'crypto-asset service provider' means crypto-asset service provider as defined in point ~~(n)~~ ***(8)*** of Article 3(1) of Regulation (EU) 202x/xx [PO: insert reference to MICA Regulation];	(43) 'crypto-asset service provider' means crypto-asset service provider as defined in point (n) of Article 3(1) of Regulation (EU) 202x/xx [PO: insert reference to ~~MICA~~**MiCA** Regulation];
Article 3, first paragraph, point (44)			
167	(44) 'issuer of crypto-assets' means issuer of crypto-assets as defined in point (h) of Article 3 (1) of [OJ: insert reference to MICA Regulation];	(44) 'issuer of crypto-assets' means issuer of crypto-assets as defined in point ~~(h)~~ ***(6)*** of Article 3 (1) of [OJ: insert reference to MICA Regulation];	(44) 'issuer of crypto-assets' means issuer of crypto-assets as defined in point (h) of Article 3 (1) of [OJ: insert reference to ~~MICA~~**MiCA** Regulation];

	Commission Proposal	EP Mandate	Council Mandate
Article 3, first paragraph, point (44a)			
167a		***(44a) 'offeror' means an offeror as defined in point [(XX)] of Article 3(1) of [OJ: insert reference to MICA Regulation];***	
Article 3, first paragraph, point (44b)			
167b		***(44b) 'offeror of crypto-assets' means an offeror of 'crypto-assets' as defined in point [(XX) of Article 3 (1)] of [OJ: insert reference to MICA Regulation];***	
Article 3, first paragraph, point (45)			
168	(45) 'issuer of asset-referenced tokens' means 'issuer of asset-referenced payment tokens' as defined in point (i) of Article 3 (1) of [OJ: insert reference to MICA Regulation];	(45) 'issuer of asset-referenced tokens' means 'issuer of asset-referenced payment tokens' as defined in point (i) of Article 3 (1) of [OJ: insert reference to MICA Regulation];	(45) 'issuer of asset-referenced tokens' means 'issuer of asset-referenced payment tokens' as defined in point (i) of Article 3 (1) of [OJ: insert reference to ~~MICA~~**MiCA** Regulation];
Article 3, first paragraph, point (45a)			
168a		***(45a) 'offeror of asset-referenced tokens' means an offeror of asset-referenced payment tokens as defined in point [(XX)] of Article 3 (1) of [OJ: insert reference to MICA Regulation];***	
Article 3, first paragraph, point (46)			
169	(46) 'issuer of significant asset-referenced	(46) 'issuer of significant asset-referenced	(46) 'issuer of significant asset-referenced

	Commission Proposal	EP Mandate	Council Mandate
	tokens' means issuer of significant asset-referenced payment tokens ad defined in point (j) of Article 3 (1) of [OJ: insert reference to MICA Regulation];	tokens' means issuer of significant asset-referenced payment tokens ~~ad~~**as** defined in point ~~(j)~~**(XX)** of Article 3 (1) of [OJ: insert reference to MICA Regulation];	tokens' means issuer of significant asset-referenced payment tokens ad defined in point (j) of Article 3 (1) of [OJ: insert reference to ~~MICA~~**MiCA** Regulation];
Article 3, first paragraph, point (47)			
170	(47) 'administrator of critical benchmarks' means an administrator of critical benchmarks as defined in point (x) of Article x of Regulation xx/202x [OJ: insert reference to Benchmark Regulation];	(47) 'administrator of critical benchmarks' means an administrator of **"**critical benchmarks**"** as defined in point ~~(x)~~**(25)** of Article ~~x of Regulation xx/202x~~**3 of Regulation 2016/1011** [OJ: insert reference to Benchmark Regulation];	(47) 'administrator of critical benchmarks' means an administrator of critical benchmarks as defined in point ~~(x)~~**(25)** of Article ~~x of Regulation xx/202x [OJ: insert reference to Benchmark Regulation]~~**3 of Regulation 2016/1011**;
Article 3, first paragraph, point (48)			
171	(48) 'crowdfunding service provider' means a crowdfunding service provider as defined in point (x) Article x of Regulation (EU) 202x/xx [PO: insert reference to Crowdfunding Regulation];	(48) 'crowdfunding service provider' means a crowdfunding service provider as defined in point ~~(x)~~**(e)** Article ~~x~~**2(1)** of Regulation (EU) ~~202x/xx~~**2020/1503** [PO: insert reference to Crowdfunding Regulation];	(48) 'crowdfunding service provider' means a crowdfunding service provider as defined in point ~~(x)~~**(e)** Article ~~x~~**2(1)** of Regulation (EU) ~~202x/xx [PO: insert reference to Crowdfunding Regulation]~~**2020/1503**;
Article 3, first paragraph, point (49)			
172	(49) 'securitisation repository' means securitisation repository as defined in point (23) of Article 2 of Regulation (EU) 2017/2402;	(49) 'securitisation repository' means securitisation repository as defined in point (23) of Article 2 of Regulation (EU) 2017/2402;	(49) 'securitisation repository' means securitisation repository as defined in point (23) of Article 2 of Regulation (EU) 2017/2402;
Article 3, first paragraph, point (50)			
173	(50) 'microenterprise' means a financial entity as defined in Article 2(3) of the Annex to	(50) '~~microenterprise~~**micro, small and medium-sized enterprise**' means a financial	(50) 'microenterprise' means a financial entity ~~as defined in Article 2(3) of the Annex to~~

	Commission Proposal	EP Mandate	Council Mandate
	Recommendation 2003/361/EC.	entity as defined in Article ~~2(3)~~2 of the Annex to Recommendation 2003/361/EC~~.~~;	~~Recommendation 2003/361/EC.~~**other than a trading venue, a central counterparty, a trade repository or a central securities depository which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million;**
Article 3, first paragraph, point (50a)			
173a		***(50a) 'resolution authority' means the authority designated by a Member State in accordance with Article 3 of Directive 2014/59/EU or the Single Resolution Board established pursuant to Article 42 of Regulation (EU) No 806/2014.***	
Article 3, first paragraph, point (51)			
173b			**(51) Lead Overseer means the authority appointed in accordance with Article 28;**
Article 3, first paragraph, point (52)			
173c			**(52) Joint Committee means the committee referred to in Article 54 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010;**
Article 3, first paragraph, point (53)			
173d			**(53) European Supervisory Authorities or**

	Commission Proposal	EP Mandate	Council Mandate
			ESAs shall be understood as a joint reference to the European Banking Authority, the European Securities and Markets Authorities and the European Insurance and Occupational Pensions Authority;
Article 3, first paragraph, point (54)			
173e			**(54) 'small enterprise' means a financial entity which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million;**
Article 3, first paragraph, point (55)			
173f			**(55) 'public authority' means any government or other public administration entity, including national central bank.**
Article 3a			
173g		***Article 3a*** ***Proportionality principle***	
Article 3a(1)			
173h		***1. Financial entities shall implement the rules introduced by Chapters II, III and IV in accordance with the principle of proportionality, taking into account their size, the nature, scale and complexity of their***	

	Commission Proposal	EP Mandate	Council Mandate
		services, activities and operations, and their overall risk profile.	
Article 3a(2), introductory part			
173i		***2. Pursuant to the principle of proportionality, Articles 4 to 14 of this Regulation shall not apply to:***	
Article 3a(2), point (a)			
173j		***(a) small and non-interconnected investment firms or payment institutions exempted by Directive (EU) 2015/2366;***	
Article 3a(2), point (b)			
173k		***(b) credit institutions exempted by Directive 2013/36/EU;***	
Article 3a(2), point (c)			
173l		***(c) electronic money institutions exempted by Directive 2009/110/EC; or***	
Article 3a(2), point (d)			
173m		***(d) small institutions for occupational retirement pensions.***	

	Commission Proposal	EP Mandate	Council Mandate
Article 3a(3)			
173n		***3. On the basis of the annual report on the review of the ICT risk management framework, referred to in Article 5(6) and Article 14a(2), the relevant competent authorities shall review and evaluate the application of the proportionality by a financial entity and determine whether the financial entity's ICT risk management framework ensures sound management and digital operational resilience and coverage of ICT risk. In doing so, the competent authorities shall take into account the size of the financial entity, the nature, scale and complexity of its services, activities and operations, and its overall risk profile.***	
Article 3a(4)			
173o		***4. In the event that the relevant competent authority deems the financial entity's ICT risk management framework to be insufficient and disproportionate, it shall enter into a dialogue with the financial entity to rectify the shortcomings and ensure full compliance with Chapter II.***	
Article 3a(5), introductory part			
173p		***5. The ESAs shall develop draft regulatory technical standards in respect of the following:***	

	Commission Proposal	EP Mandate	Council Mandate
Article 3a(5), point (a)			
173q		***(a) determining the extent to which ICT risk management obligations are applicable to each of the financial entities mentioned in paragraph 1;***	
Article 3a(5), point (b)			
173r		***(b) specifying further the content and format of the annual report on the review of the ICT risk management framework referred to in paragraph 3;***	
Article 3a(5), point (c)			
173s		***(c) specifying further the rules and procedures to be followed by the competent authorities and financial entities in the dialogue referred to in paragraph 4.***	
Article 3a(6)			
173t		***6. The ESAs shall submit the draft regulatory technical standards referred to in paragraph 5 to the Commission by [OJ: insert date 1 year after the date of entry into force].***	
Article 3a(7)			
173u		***Power is delegated to the Commission to***	

	Commission Proposal	EP Mandate	Council Mandate
		adopt the regulatory technical standards referred to in paragraph 5 of this Article in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	
CHAPTER II			
174	CHAPTER II ICT RISK MANAGEMENT	CHAPTER II ICT RISK MANAGEMENT	CHAPTER II ICT RISK MANAGEMENT
SECTION I			
175	SECTION I	SECTION I	SECTION I
Article 3a			
175a			**Article 3a** **Proportionality Principle**
Article 3a(1)			
175b			**Financial entities shall implement the rules on ICT risk management laid out in this Chapter in accordance with the principle of proportionality, by taking into account the size, the nature, scale and complexity of their services, activities and operations, as well as their overall risk profile.**

	Commission Proposal	EP Mandate	Council Mandate
Article 4			
176	Article 4 Governance and organisation	Article 4 Governance and organisation	Article 4 Governance and organisation
Article 4(1)			
177	1. Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks.	1. Financial entities shall have in place ***an*** internal governance and ***a*** control ~~*frameworks that ensure*~~***framework that ensures*** an effective and prudent management of all ICT risks***, with a view to achieving a high level of digital operational resilience***.	1. Financial entities shall have in place internal governance and control frameworks that ensure an effective and prudent management of all ICT risks. **Within their internal governance and control frameworks, financial entities shall assign the responsibility for managing and overseeing ICT-related operations and shall establish a control function in relation to ICT risks, independent and segregated from ICT operations processes.**
Article 4(2), first subparagraph			
178	2. The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework referred to in Article 5(1):	2. The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework referred to in Article 5(1):	2. The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework referred to in Article 5(1)~~:~~**.**
Article 4(2), second subparagraph, introductory part			
179	For the purposes of the first subparagraph, the management body shall:	For the purposes of the first subparagraph, the management body shall:	For the purposes of the first subparagraph, the management body shall:

	Commission Proposal	EP Mandate	Council Mandate
Article 4(2), second subparagraph, point (a)			
180	(a) bear the final responsibility for managing the financial entity's ICT risks;	(a) bear the ~~*final*~~***ultimate*** responsibility for managing the financial entity's ICT risks;	(a) bear the ~~final~~**ultimate** responsibility for managing the financial entity's ICT risks;
Article 4(2), second subparagraph, point (aa)			
180a		***(aa) put in place procedures and policies that aim to ensure the maintenance of high standards of security, confidentiality and integrity of data;***	
Article 4(2), second subparagraph, point (b)			
181	(b) set clear roles and responsibilities for all ICT-related functions;	(b) set clear roles and responsibilities for all ICT-related functions;	(b) set clear roles and responsibilities for all ICT-related functions **and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among them**;
Article 4(2), second subparagraph, point (c)			
182	(c) determine the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9);	(c) determine the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in point (b) of Article 5(9);	(c) ~~determine~~**bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 5(9) including the determination of** the appropriate risk tolerance ~~level~~**limit** of ICT risk of the financial entity, as referred to in point (b) of Article 5(9);
Article 4(2), second subparagraph, point (d)			

	Commission Proposal	EP Mandate	Council Mandate
183	(d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan referred to in, respectively, paragraphs 1 and 3 of Article 10;	(d) approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan***, which may be adopted as a dedicated distinct policy and as an integral part of the financial entity's broader business-wide continuity policy and disaster recovery plan,*** referred to in, respectively, paragraphs 1 and 3 of Article 10;	(d) approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT ~~Disaster~~**response and** recovery ~~Plan~~**plans** referred to in, respectively, paragraphs 1 and 3 of Article 10;
Article 4(2), second subparagraph, point (e)			
184	(e) approve and periodically review the ICT audit plans, ICT audits and material modifications thereto;	(e) approve and periodically review the ICT audit plans, ICT audits and material modifications thereto;	(e) approve and periodically review the **financial entities' ICT internal**~~ICT~~ audit plans, ICT audits and material modifications thereto;
Article 4(2), second subparagraph, point (f)			
185	(f) allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including training on ICT risks and skills for all relevant staff;	(f) allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including ***relevant*** training on ICT risks and skills for all ~~*relevant*~~ staff;	(f) allocate and periodically review appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including training on ICT ~~risks and~~**security awareness and digital operational resilience referred to in Article 12(6) and ICT** skills for all relevant staff;
Article 4(2), second subparagraph, point (g)			
186	(g) approve and periodically review the financial entity's policy on arrangements	(g) approve and periodically review the financial entity's policy on arrangements	(g) approve and periodically review the financial entity's policy on arrangements

	Commission Proposal	EP Mandate	Council Mandate
	regarding the use of ICT services provided by ICT third-party service providers;	regarding the use of ICT services provided by ICT third-party service providers;	regarding the use of ICT services provided by ICT third-party service providers;
Article 4(2), second subparagraph, point (h)			
187	(h) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;	(h) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;	(h) be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes;
Article 4(2), second subparagraph, point (i)			
188	(i) be duly informed about ICT-related incidents and their impact and about response, recovery and corrective measures.	(i) be ~~duly~~***regularly*** informed about ***at least major*** ICT-related incidents and their impact and about response, recovery and corrective measures~~.~~	(i) be duly informed about **at least major** ICT-related incidents and their impact and about response, recovery and corrective measures.
Article 4(3)			
189	3. Financial entities other than microenterprises shall establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.	3. Financial entities other than microenterprises shall establish a role to monitor the arrangements ~~concluded with ICT third-party service providers on~~***within the financial entity for*** the use of ICT services***, especially those concluded with ICT third-party service providers***, or shall designate a member of senior	3. Financial entities other than microenterprises shall establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.

	Commission Proposal	EP Mandate	Council Mandate
		management as responsible for overseeing the related risk exposure and relevant documentation.	
Article 4(4)			
190	4. Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.	4. Members of the management body ~~*shall, on a regular basis, follow specific training to gain and*~~***of the financial entity shall actively*** keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity***, including by following specific training on a regular basis, commensurate to the ICT risks being managed***.	4. Members of the management body **of financial entities other than microenterprises** shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity.
SECTION II			
191	SECTION II	SECTION II	SECTION II
Article 5			
192	Article 5 ICT risk management framework	Article 5 ICT risk management framework	Article 5 ICT risk management framework
Article 5(1)			
193	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	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	1. Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework **as part of their overall risk management system**, which enables them to address ICT risk quickly,

	Commission Proposal	EP Mandate	Council Mandate
	digital operational resilience that matches their business needs, size and complexity.	digital operational resilience ~~*that matches their business needs, size and complexity*~~.	efficiently and comprehensively and to ensure a high level of digital operational resilience ~~that matches their business needs, size and complexity~~.
Article 5(2)			
194	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*~~***that*** 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 **at least** strategies, policies, procedures, ICT protocols and tools which are necessary to duly and ~~effectively~~**adequately** protect all ~~relevant physical components and infrastructures~~**information assets and ICT assets**, including computer hardware**, software**, servers, as well as all relevant premises, data centres and sensitive designated areas, to ensure that all those ~~physical elements~~**information assets and ICT assets** are adequately protected from risks including damage and unauthorized access or usage.
Article 5(3)			
195	3. Financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, protocols and tools as determined in the ICT risk management framework. They shall provide complete and updated information on ICT risks as required by the competent authorities.	3. Financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, protocols and tools as determined in the ICT risk management framework. They shall provide complete and updated information on ICT risks ***and on their ICT risk management framework as requested*** ~~*as required*~~ by the competent authorities.	3. Financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, protocols and tools as determined in ~~the~~**their** ICT risk management framework. They shall provide complete and updated information on ICT risks as required by the competent authorities.

	Commission Proposal	EP Mandate	Council Mandate
Article 5(4)			
196	4. As part of the ICT risk management framework referred to in paragraph 1, financial entities other than microenterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance and shall regularly review it.	4. As part of the ICT risk management framework referred to in paragraph 1, financial entities other than microenterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance***, where already available and appropriate, including guidance laid out in relevant guidelines established by the ESAs*** and shall regularly review it.	4. ~~As part of the ICT risk management framework referred to in paragraph 1, financial entities other than microenterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance and shall regularly review it.~~
Article 5(5)			
197	5. Financial entities other than microenterprises shall ensure appropriate segregation of ICT management functions, control functions, and internal audit functions, according to the three lines of defense model, or an internal risk management and control model.	5. Financial entities other than microenterprises shall ***assign the responsibility for managing and overseeing ICT risks to a control function and ensure the independence of such control function in order to avoid conflicts of interest. Financial entities shall*** ensure appropriate ~~*segregation*~~***independence*** of ICT management functions, control functions, and internal audit functions, according to the three lines of defense model, or an internal risk management and control model.	5. Financial entities other than microenterprises shall ensure appropriate segregation of ICT **risk** management functions, control functions, and internal audit functions, according to the three lines of ~~defense~~**defence** model, or an internal risk management and control model.
Article 5(6)			
198	6. The ICT risk management framework referred to in paragraph 1 shall be documented	6. The ICT risk management framework referred to in paragraph 1 shall be documented	6. The ICT risk management framework referred to in paragraph 1 shall be **internally**

	Commission Proposal	EP Mandate	Council Mandate
	and reviewed at least once a year, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring.	and reviewed at least once a year, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. ***A report on the review of the ICT risk management framework shall be submitted to the competent authority on an annual basis.***	documented and reviewed at least once a year **or periodically, in the case of microenterprises**, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring.
Article 5(7)			
199	7. The ICT risk management framework referred to in paragraph 1 shall be audited on a regular basis by ICT auditors possessing sufficient knowledge, skills and expertise in ICT risk. The frequency and focus of ICT audits shall be commensurate to the ICT risks of the financial entity.	7. ***As regards financial entities other than microenterprises,*** the ICT risk management framework referred to in paragraph 1 shall be audited on a regular basis by ICT auditors possessing sufficient knowledge, skills and expertise in ICT risk. The frequency and focus of ICT audits shall be commensurate to the ICT risks of the financial entity.	7. **Except for microenterprises,** the ICT risk management framework referred to in paragraph 1 shall be ~~audited~~**subject to internal audit** on a regular basis **in line with the financial entities' audit plan** by ~~ICT~~ auditors possessing sufficient knowledge, skills and expertise in ICT risk**, as well as appropriate independence**. The frequency and focus of ICT audits shall be commensurate to the ICT risks of the financial entity.
Article 5(8)			
200	8. A formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings, shall be established, taking into consideration the conclusions from the audit review while having due regard to the nature, scale and complexity of the financial	8. A formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings, shall be established, taking into consideration the conclusions from the audit review ~~*while having due regard to the nature, scale and complexity of the financial*~~	8. A formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings, shall be established, taking into consideration the conclusions from the audit review ~~while having due regard to the nature, scale and complexity of the financial~~

	Commission Proposal	EP Mandate	Council Mandate
	entities' services and activities.	~~*entities' services and activities.*~~.	~~entities' services and activities~~.
Article 5(9), introductory part			
201	9. The ICT risk management framework referred to in paragraph 1 shall include a digital resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by:	9. The ICT risk management framework referred to in paragraph 1 shall include a digital ***operational*** resilience strategy setting out how the framework is implemented. To that effect it shall include the methods to address ICT risk and attain specific ICT objectives, by:	9. The ICT risk management framework referred to in paragraph 1 shall include a digital **operational** resilience strategy setting out how the framework is implemented. To that effect ~~it~~**the digital operational resilience strategy** shall include the methods to address ICT risk and attain specific ICT objectives, by:
Article 5(9), point (a)			
202	(a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;	(a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;	(a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;
Article 5(9), point (b)			
203	(b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance of ICT disruptions;	(b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance ~~*of*~~***for*** ICT disruptions;	(b) establishing the risk tolerance ~~level~~**limit** for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance of ICT disruptions;
Article 5(9), point (c)			
204	(c) setting out clear information security objectives;	(c) setting out clear information security objectives;	(c) setting out clear information security objectives **and establishing performance and risk metrics and indicators, such as key performance indicators and key risk indicators**;

	Commission Proposal	EP Mandate	Council Mandate
Article 5(9), point (d)			
205	(d) explaining the ICT reference architecture and any changes needed to reach specific business objectives;	(d) explaining the ICT ~~*reference*~~ architecture and any changes needed to reach specific business objectives;	(d) explaining the ICT reference architecture and any changes needed to reach specific business objectives;
Article 5(9), point (e)			
206	(e) outlining the different mechanisms put in place to detect, protect and prevent impacts of ICT-related incidents;	(e) outlining the different mechanisms put in place to detect, protect and prevent impacts of ICT-related incidents;	(e) outlining the different mechanisms put in place to detect, protect and prevent impacts of ICT-related incidents;
Article 5(9), point (f)			
207	(f) evidencing the number of reported major ICT-related incidents and the effectiveness of preventive measures	(f) evidencing the number of reported major ICT-related incidents and the effectiveness of preventive measures	(f) evidencing the **current digital operational resilience situation on the basis of the** number of reported major ICT-related incidents and the effectiveness of preventive measures**;**
Article 5(9), point (g)			
208	(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	(g) ~~*defining a holistic ICT multi-vendor strategy at entity level showing*~~***identifying*** key dependencies on ICT third-party service providers and ~~*explaining the rationale behind the procurement mix of third-party service providers*~~***detailing exit strategies in relation to such key dependencies ;***	(g) **for financial entities other than microenterprises, assess the need for a multi-vendor strategy, and if applicable,** 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 **ICT** third-party service providers**;**

	Commission Proposal	EP Mandate	Council Mandate
Article 5(9), point (h)			
209	(h) implementing digital operational resilience testing;	(h) implementing digital operational resilience testing***, in accordance with Chapter IV of this Regulation***;	(h) implementing digital operational resilience testing;
Article 5(9), point (i)			
210	(i) outlining a communication strategy in case of ICT-related incidents.	(i) outlining a communication strategy in case of ICT-related incidents ***required to be disclosed in accordance with Article 13***.	(i) outlining a communication strategy in case of ICT-related incidents.
Article 5(10)			
211	10. Upon approval of competent authorities, financial entities may delegate the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings.	10. Upon approval of competent authorities, financial entities may ~~*delegate*~~***outsource*** the tasks of verifying compliance with the ICT risk management requirements to ~~*intra-group or external*~~***external undertakings.*** ***Upon notification to the competent authorities, financial entities may delegate the task of verifying compliance with the ICT risk management requirements to intra-group*** undertakings. ***Where the delegation referred to in the second subparagraph is put in place, the financial entity shall remain fully accountable for the verification of compliance with ICT risk management requirements.***	10. ~~Upon~~**After notification to or** approval of competent authorities, **in accordance with national and European sectoral legislation,** financial entities may ~~delegate~~**outsource** the tasks of verifying compliance with the ICT risk management requirements to intra-group or external undertakings. **In case of such outsourcing, the financial entity remains fully accountable for the verification of compliance with the ICT risk management requirements.**
Article 6			

	Commission Proposal	EP Mandate	Council Mandate
212	Article 6 ICT systems, protocols and tools	Article 6 ICT systems, protocols and tools	Article 6 ICT systems, protocols and tools
Article 6(1), introductory part			
213	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*~~ ***in order to address and manage ICT risk, that*** fulfil the following conditions:	1. Financial entities shall use and maintain updated ICT systems, protocols and tools, which fulfil the following conditions:
Article 6(1), point (a)			
214	(a) the systems and tools are appropriate to the nature, variety, complexity and magnitude of operations supporting the conduct of their activities;	(a) the systems and tools are appropriate to the ~~*nature, variety, complexity and*~~ magnitude of operations supporting the conduct of their activities;	(a) the systems**, protocols** and tools are appropriate to the **size,** nature, ~~variety~~**scale**, complexity and ~~magnitude~~**overall risk profile** of operations supporting the conduct of their activities;
Article 6(1), point (b)			
215	(b) they are reliable;	(b) they are reliable;	(b) ~~they are reliable;~~
Article 6(1), point (c)			
216	(c) they have sufficient capacity to accurately process the data necessary for the performance of activities and the provision of services in time, and to deal with peak orders, message or transaction volumes, as needed, including in the case of introduction of new technology;	(c) they have sufficient capacity to accurately process the data necessary for the performance of activities and the provision of services in time, and to deal with peak orders, message or transaction volumes, as needed, including in the case of introduction of new technology;	(c) they have sufficient capacity to accurately process the data necessary for the performance of activities and the provision of services in time, and to deal with peak orders, message or transaction volumes, as needed, including in the case of introduction of new technology;

	Commission Proposal	EP Mandate	Council Mandate
Article 6(1), point (d)			
217	(d) they are technologically resilient to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.	(d) they are technologically resilient to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.	(d) they are technologically resilient to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.
Article 6(2)			
218	2. Where financial entities use internationally recognized technical standards and industry leading practices on information security and ICT internal controls, they shall use those standards and practices in line with any relevant supervisory recommendation on their incorporation.	2. Where financial entities use internationally recognized technical standards and industry leading practices on information security and ICT internal controls, they shall use those standards and practices in line with any relevant supervisory recommendation on their incorporation.	2. ~~Where financial entities use internationally recognized technical standards and industry leading practices on information security and ICT internal controls, they shall use those standards and practices in line with any relevant supervisory recommendation on their incorporation.~~
Article 7			
219	Article 7 Identification	Article 7 Identification	Article 7 Identification
Article 7(1)			
220	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	1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ***critical or important*** ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial	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~~**ICT supported** business functions, **roles and responsibilities,** the information assets **and ICT assets** supporting these functions, and ~~the ICT system configurations and interconnections with~~

	Commission Proposal	EP Mandate	Council Mandate
	needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.	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.	~~internal and external ICT systems~~**their roles and dependencies with ICT risk**. Financial entities shall review as needed, and at least yearly, the adequacy of ~~the~~**this** classification ~~of the information assets~~ and of any relevant documentation.
Article 7(2)			
221	2. Financial entities shall on a continuous basis identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT-related business functions and information assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.	2. Financial entities shall on a continuous basis identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ***critical or important*** ICT-related business functions and information assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.	2. Financial entities shall on a continuous basis identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess**, inter alia,** cyber threats and ~~ICT~~ vulnerabilities relevant to their ~~ICT-related~~**ICT supported** business functions**, information assets and ICT** ~~and information~~ assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.
Article 7(3)			
222	3. Financial entities other than microenterprises shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their functions, supporting processes or information assets.	3. Financial entities other than microenterprises shall perform***, where appropriate,*** a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their functions, supporting processes or information assets.	3. Financial entities other than microenterprises shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their functions, supporting processes or information assets.
Article 7(4)			
223			

	Commission Proposal	EP Mandate	Council Mandate
	4. Financial entities shall identify all ICT systems accounts, including those on remote sites, the network resources and hardware equipment, and shall map physical equipment considered critical. They shall map the configuration of the ICT assets and the links and interdependencies between the different ICT assets.	4. Financial entities shall identify all ICT systems accounts, including those on remote sites, the network resources and hardware equipment, and shall map physical equipment considered critical. They shall map the configuration of the ***critical or important*** ICT assets ***having regard to their purpose*** and the links and interdependencies between ~~*the*~~***those*** different ICT assets.	4. Financial entities shall identify all ~~ICT systems accounts~~**information assets and ICT assets**, including those on remote sites, ~~the~~ network resources and hardware equipment, and shall map ~~physical equipment~~**those** considered critical. They shall map the configuration of the **information asset and** ICT assets and the links and interdependencies between the different **information assets and** ICT assets.
Article 7(5)			
224	5. Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers.	5. Financial entities shall identify and document all ***critical or important*** processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers ***that support critical or important functions***.	5. Financial entities shall identify and document all ~~processes that are dependent on ICT third-party service providers, and shall identify~~**critical processes and** interconnections with ICT third-party service providers.
Article 7(6)			
225	6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain and regularly update relevant inventories.	6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain and regularly update relevant inventories.	6. For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain **relevant inventories which must be updated periodically and every time any major change as referred to in Article 7(3) occurs**~~and regularly update relevant inventories~~.
Article 7(7)			
226	7. Financial entities other than microenterprises	7. Financial entities other than microenterprises	7. Financial entities other than microenterprises

	Commission Proposal	EP Mandate	Council Mandate
	shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems, especially before and after connecting old and new technologies, applications or systems.	shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems, ~~*especially before and after connecting old and new technologies, applications or systems.*~~***including systems that are still in use and perform their function but that are:***	shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems, especially before and after connecting old and new technologies, applications or systems.
Article 7(7), point (a)			
226a		***(a) old or at the end of their life, in the case of hardware;***	
Article 7(7), point (b)			
226b		***(b) no longer able to receive support or maintenance from their supplier; or***	
Article 7(7), point (c)			
226c		***(c) impossible or uneconomical to update. Annual ICT risk assessments shall be conducted on legacy ICT systems especially before and after connecting technologies, applications or systems.***	
Article 8			
227	Article 8 Protection and Prevention	Article 8 Protection and Prevention	Article 8 Protection and Prevention

	Commission Proposal	EP Mandate	Council Mandate
Article 8(1)			
228	1. For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the functioning of the ICT systems and tools and shall minimise the impact of such risks through the deployment of appropriate ICT security tools, policies and procedures.	1. For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the functioning of the ICT systems and tools and shall minimise the impact of such risks through the deployment of appropriate ICT security tools, policies and procedures.	1. For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the **security and** functioning of the ICT systems and tools and shall minimise the impact of such **ICT** risks through the deployment of appropriate ICT security tools, policies and procedures.
Article 8(2)			
229	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.	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~~**confidentiality, integrity and availability** of data, whether at rest, in use or in transit.
Article 8(3), introductory part			
230	3. To achieve the objectives referred to in paragraph 2, financial entities shall use state-of-the-art ICT technology and processes which:	3. To achieve the objectives referred to in paragraph 2, financial entities shall use ~~*state-of-the-art*~~ ICT technology and processes ~~*which*~~***that***:	3. To achieve the objectives referred to in paragraph 2, financial entities shall use ~~state-of-the-art~~ ICT technology and processes **that are appropriate to the financial entities' risk profile** which:
Article 8(3), point (a)			

	Commission Proposal	EP Mandate	Council Mandate
231	(a) guarantee the security of the means of transfer of information;	(a) ~~guarantee~~***maximise*** the security of the means of transfer of information;	(a) ~~guarantee~~**ensure** the security of the means of transfer of ~~information~~**data**;
Article 8(3), point (b)			
232	(b) minimise the risk of corruption or loss of data, unauthorized access and of the technical flaws that may hinder business activity;	(b) minimise the risk of corruption or loss of data, unauthorized access and of the technical flaws that may hinder business activity;	(b) minimise the risk of corruption or loss of data, unauthorized access and of the technical flaws that may hinder business activity;
Article 8(3), point (c)			
233	(c) prevent information leakage;	(c) prevent information leakage;	(c) prevent ~~information leakage~~**breaches of confidentiality, impairment of integrity, lack of availability and loss of data**;
Article 8(3), point (d)			
234	(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 ~~*or*~~***,*** processing-related risks~~*, including inadequate record keeping*~~ ***and human error***.	(d) ensure that data is protected from poor administration or processing-related risks, including inadequate record-keeping.
Article 8(4), first subparagraph, introductory part			
235	4. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:	4. As part of the ICT risk management framework referred to in Article 5(1), ***in accordance with their risk profile,*** financial entities shall:	4. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:
Article 8(4), first subparagraph, point (a)			

	Commission Proposal	EP Mandate	Council Mandate
236	(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of theirs, and their customers' ICT resources, data and information assets;	(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of ~~*theirs, and*~~ ***their ICT resources, data and information assets while ensuring full protection of*** their customers' ICT resources, data and information assets ***where they comprise part of financial entities' ICT systems***;	(a) develop and document an information security policy defining rules to protect the confidentiality, integrity and availability of theirs, and their customers' ICT resources, data and information assets;
Article 8(4), first subparagraph, point (b)			
237	(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;	(b) following a risk-based approach, establish a sound network and infrastructure management using appropriate techniques, methods and protocols ~~*including implementing automated*~~***that may include implementing*** mechanisms to isolate affected information assets in case of cyber-attacks;	(b) following a risk-based approach, establish a sound network and infrastructure management using appropriate techniques, methods and protocols ~~including~~**that may include in particular** implementing automated mechanisms to isolate affected information assets in case of cyber-attacks;
Article 8(4), first subparagraph, point (c)			
238	(c) implement policies that limit the physical and virtual access to ICT system resources and data to what is required only for legitimate and approved functions and activities, and establish to that effect a set of policies, procedures and controls that address access privileges and a sound administration thereof;	(c) implement policies***, procedures and controls*** that limit the physical and virtual access to ICT system resources and data to what is required only for legitimate and approved functions and activities~~, and establish to that effect a set of policies, procedures and controls that address access privileges and a sound administration thereof~~;	(c) implement policies that limit the physical ~~and virtual~~**or logical** access to ICT ~~system resources and data~~**systems and information assets** to what is required only for legitimate and approved functions and activities, and establish to that effect a set of policies, procedures and controls that address access privileges and a sound administration thereof;
Article 8(4), first subparagraph, point (d)			

	Commission Proposal	EP Mandate	Council Mandate
239	(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and risk assessment processes;	(d) implement policies and protocols for strong authentication mechanisms, ~~*based on relevant standards and dedicated controls systems to prevent access to*~~***and protection of*** cryptographic keys ~~*whereby data is encrypted*~~, based on ~~*results of approved data classification and risk assessment processes*~~***relevant standards and dedicated controls systems***;	(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and **ICT** risk assessment processes;
Article 8(4), first subparagraph, point (e)			
240	(e) implement policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, system or security changes, that are based on a risk-assessment approach and as an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;	(e) implement policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, system or security changes, that are based on a risk-assessment approach and as an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;	(e) implement ~~policies,~~**documented** procedures and controls for ICT change management, including changes to software, hardware, firmware components, system or security changes, that are based on a risk-assessment approach and as an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;
Article 8(4), first subparagraph, point (f)			
241	(f) have appropriate and comprehensive policies for patches and updates.	(f) have appropriate and comprehensive policies for patches and updates.	(f) have appropriate and comprehensive ~~policies~~**documented processes** for patches and updates.
Article 8(4), second subparagraph			
242			

	Commission Proposal	EP Mandate	Council Mandate
	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 ~~*instantaneously severed*~~***severed as quickly as possible*** 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 instantaneously severed and shall~~**to** ensure its compartmentalisation and segmentation, in order to minimise and prevent contagion, especially for interconnected financial processes.
Article 8(4), third subparagraph			
243	For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.	For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.	For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.
Article 9			
244	Article 9 Detection	Article 9 Detection	Article 9 Detection
Article 9(1), first subparagraph			
245	1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure.	1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and***, where technologically possible,*** to identify ***and monitor*** all potential material single points of	1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify all potential ~~material~~ single points of failure.

	Commission Proposal	EP Mandate	Council Mandate
		failure.	
Article 9(1), second subparagraph			
246	All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.	All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.	All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.
Article 9(2)			
247	2. The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger ICT-related incident detection and ICT-related incident response processes, and shall put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	2. The detection mechanisms referred to in paragraph 1 shall ~~*enable multiple layers of control, define alert thresholds and criteria to*~~ trigger ICT-related incident detection and ICT-related incident response processes, ~~*and shall put in place*~~***including*** automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	2. The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger ~~ICT-related incident detection~~ and **initiate** ICT-related incident response processes, and shall put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response.
Article 9(3)			
248	3. Financial entities shall devote sufficient resources and capabilities, with due consideration to their size, business and risk profiles, to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	3. Financial entities shall devote sufficient resources and capabilities, ~~*with due consideration to their size, business and risk profiles,*~~ to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	3. Financial entities shall devote sufficient resources and capabilities, ~~with due consideration to their size, business and risk profiles,~~ to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.
Article 9(3a)			
248a		***3a. Financial entities shall record all ICT-related incidents that have an impact on the***	

	Commission Proposal	EP Mandate	Council Mandate
		stability, continuity or quality of financial services, including where the incident has or is likely to have an impact on such services.	
Article 9(4)			
249	4. Financial entitles referred to in point (l) of Article 2(1) shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors and request re-transmission of any such erroneous reports.	4. Financial entitles referred to in point (l) of Article 2(1) shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors and request re-transmission of any such erroneous reports.	4. Financial ~~entitles~~**entities** referred to in ~~point (l)~~**points (34) and (36)** of Article ~~2(1)~~**2 (1) of Regulation 600/2014** shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors and request re-transmission of any such erroneous reports.
Article 10			
250	Article 10 Response and recovery	Article 10 Response and recovery	Article 10 Response and recovery
Article 10(1)			
251	1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy of the financial entity.	1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place ~~a dedicated and~~ comprehensive ICT Business Continuity Policy***, which may be adopted as a dedicated distinct policy and*** as an integral part of the ***broader business-wide*** operational business continuity policy of the financial entity.	1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial entities shall put in place a dedicated and comprehensive ICT business continuity policy as an integral part of the ~~operational~~**overall** business continuity ~~policy~~**management** of the financial entity.

	Commission Proposal	EP Mandate	Council Mandate
Article 10(1a)			
251a		***The ICT Business Continuity Policy shall aim to manage and mitigate risks that could have a harmful effect on financial entities' ICT systems and ICT services and to facilitate their swift recovery if necessary. In drawing up the ICT Business Continuity Policy, financial entities shall specifically consider risks that could have a harmful impact on ICT services and ICT systems.***	
Article 10(2), introductory part			
252	2. Financial entities shall implement the ICT Business Continuity Policy referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:	2. Financial entities shall implement the ICT Business Continuity Policy referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:	2. Financial entities shall implement the ICT business continuity policy referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:
Article 10(2), point (a)			
253	(a) recording all ICT-related incidents;	(a) ~~*recording all ICT-related incidents;*~~	(a) ~~recording all ICT-related incidents;~~
Article 10(2), point (b)			
254	(b) ensuring the continuity of the financial entity's critical functions;	(b) ensuring the continuity of the financial entity's critical functions;	(b) ensuring the continuity of the financial entity's critical functions;
Article 10(2), point (c)			
255			

	Commission Proposal	EP Mandate	Council Mandate
	(c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritises resumption of activities and recovery actions;	(c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way ~~*which*~~***that*** limits damage and prioritises resumption of activities and recovery actions;	(c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in ~~particular but not limited to cyber-attacks, in~~ a way which limits damage and prioritises resumption of activities and recovery actions;
Article 10(2), point (d)			
256	(d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;	(d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;	(d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;
Article 10(2), point (e)			
257	(e) estimating preliminary impacts, damages and losses;	(e) estimating preliminary impacts, damages and losses;	(e) estimating preliminary impacts, damages and losses;
Article 10(2), point (f)			
258	(f) setting out communication and crisis management actions which ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 13, and reported to competent authorities in accordance with Article 17.	(f) setting out communication and crisis management actions ~~*which*~~***that*** ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 13, and reported to competent authorities in accordance with Article 17.	(f) setting out communication and crisis management actions which ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 13, and reported to competent authorities in accordance with Article 17.

	Commission Proposal	EP Mandate	Council Mandate
Article 10(3)			
259	3. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement an associated ICT Disaster Recovery Plan, which, in the case of financial entities other than microenterprises, shall be subject to independent audit reviews.	3. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement an associated ICT Disaster Recovery Plan, which, in the case of financial entities other than microenterprises, shall be subject to independent audit reviews.	3. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement ~~an~~ associated ICT ~~Disaster~~**response and** recovery ~~Plan~~**plans**, which, in the case of financial entities other than microenterprises, shall be subject to independent **internal** audit reviews.
Article 10(4)			
260	4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans **as part of their overall business continuity management, including those**~~, notably~~ with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.
Article 10(4a)			
260a			**4a. As part of the overall business continuity management, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions.** **Financial entities shall assess under the BIA the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and/or external data and scenario analysis. The BIA**

	Commission Proposal	EP Mandate	Council Mandate
			shall consider the criticality of identified and mapped business functions, supporting processes, third-party dependencies and information assets, and their interdependencies. **Financial entities shall foresee a design and usage of ICT systems and ICT services in full alignment with the BIA notably with regard to adequately ensuring the redundancy of all critical components.**
Article 10(5), first subparagraph, introductory part			
261	5. As part of their comprehensive ICT risk management, financial entities shall:	5. As part of their comprehensive ICT risk management, financial entities shall:	5. As part of their comprehensive ICT risk management, financial entities shall:
Article 10(5), first subparagraph, point (a)			
262	(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to the ICT systems;	(a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to ~~the~~***critical or important*** ICT systems;	(a) test the ICT business continuity ~~Policy and the ICT Disaster~~**plans and ICT response and** recovery ~~Plan~~**plans regularly, and for financial entities other than microenterprises,** at least **on a** yearly **basis,** and after ~~substantive~~**significant** changes to the ICT systems;
Article 10(5), first subparagraph, point (b)			
263	(b) test the crisis communication plans established in accordance with Article 13.	(b) test the crisis communication plans established in accordance with Article 13.	(b) test the crisis communication plans established in accordance with Article 13.

	Commission Proposal	EP Mandate	Council Mandate
Article 10(5), second subparagraph			
264	For the purposes of point (a), financial entities other than microenterprises shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 11.	For the purposes of point (a), financial entities other than microenterprises shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 11.	For the purposes of point (a), financial entities other than microenterprises shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 11.
Article 10(5), third subparagraph			
265	Financial entities shall regularly review their ICT Business Continuity Policy and ICT Disaster Recovery Plan taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.	Financial entities shall regularly review their ICT Business Continuity Policy and ICT Disaster Recovery Plan taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.	Financial entities shall regularly review their ICT business continuity policy and ICT ~~Disaster~~**response and** recovery ~~Plan~~**plans** taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.
Article 10(6)			
266	6. Financial entities other than microenterprises shall have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13.	6. Financial entities other than microenterprises shall have a crisis management function, ~~*which*~~***either as a dedicated function or comprising part of the functions with responsibilities for incident handling response and management. The crisis management function shall***, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan,~~ *shall*~~ set out clear procedures to manage internal and external crisis communications in accordance with Article 13.	6. Financial entities other than microenterprises shall have a crisis management function, which, in case of activation of their ICT business continuity ~~Policy or ICT Disaster~~**plans and ICT response and** recovery ~~Plan~~**plans**, shall **inter alia** set out clear procedures to manage internal and external crisis communications in accordance with Article 13.

	Commission Proposal	EP Mandate	Council Mandate
Article 10(7)			
267	7. Financial entities shall keep records of activities before and during disruption events when their ICT Business Continuity Policy or ICT Disaster Recovery Plan is activated. Such records shall be readily available.	7. Financial entities shall keep records of ***relevant*** activities before and during disruption events when their ICT Business Continuity Policy or ICT Disaster Recovery Plan is activated. Such records shall be readily available.	7. Financial entities shall keep records of activities before and during disruption events when their ICT business continuity ~~Policy or ICT Disaster~~**plans and ICT response and** recovery ~~Plan is~~**plans are** activated. ~~Such records shall be readily available.~~
Article 10(8)			
268	8. Financial entities referred to in point (f) of Article 2(1) shall provide to the competent authorities copies of the results of the ICT business continuity tests or similar exercises performed during the period under review.	8. Financial entities referred to in point (f) of Article 2(1) shall provide to the competent authorities copies of the results of the ICT business continuity tests or similar exercises performed during the period under review.	8. ~~Financial entities referred to in point (f) of Article 2(1)~~**Central securities depositories** shall provide to the competent authorities copies of the results of the ICT business continuity tests or similar exercises performed during the period under review.
Article 10(9)			
269	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 ***estimated financial*** costs and losses caused by ***significant*** ICT disruptions and ***major*** ICT-related incidents.	9. ~~Financial entities other than microenterprises shall report to competent authorities all costs and losses caused by ICT disruptions and ICT-related incidents.~~
Article 10(9a)			
269a		***9a. The ESAs shall, through the Joint Committee, develop common guidelines on the methodology for calculating the costs, and***	

	Commission Proposal	EP Mandate	Council Mandate
		quantifying the losses, referred to in paragraph 9.	
Article 11			
270	Article 11 Backup policies and recovery methods	Article 11 Backup policies and recovery methods	Article 11 Backup policies**, restoration** and recovery methods
Article 11(1), introductory part			
271	1. For the purpose of ensuring the restoration of ICT systems with minimum downtime and limited disruption, as part of their ICT risk management framework, financial entities shall develop:	1. For the purpose of ensuring the restoration of ICT systems with minimum downtime and limited disruption, as part of their ICT risk management framework, financial entities shall develop:	1. For the purpose of ensuring the restoration of ICT systems **and data** with minimum downtime ~~and~~**,** limited disruption **and loss**, as part of their ICT risk management framework, financial entities shall develop:
Article 11(1), point (a)			
272	(a) a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitiveness of the data;	(a) a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitiveness of the data;	(a) ~~a~~**documented** backup ~~policy~~**policies and procedures** specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the ~~sensitiveness~~**confidentiality level** of the data;
Article 11(1), point (b)			
273	(b) recovery methods.	(b) recovery methods.	(b) recovery methods.
Article 11(2)			

	Commission Proposal	EP Mandate	Council Mandate
274	2. Backup systems shall begin processing without undue delay, unless such start would jeopardize the security of the network and information systems or the integrity or confidentiality of data.	2. ***In accordance with the backup policy specified in point (a) of paragraph 1,*** backup systems shall begin processing without undue delay, unless such start would jeopardize the security of the network and information systems or the integrity or confidentiality of data.	2. ~~Backup systems~~**Financial entities** shall ~~begin~~**set up backup-systems that can be activated for** processing ~~without undue delay, unless such start would~~**in accordance with the backup policies, procedures and recovery methods referred to in paragraph 1.** **The activation of backup systems shall not** jeopardize the security of the network and information systems or the integrity**, availability** or confidentiality of data. **Testing of the backup and restoration procedures should be undertaken on a periodic basis.**
Article 11(3), first subparagraph			
275	3. When restoring backup data using own systems, financial entities shall use ICT systems that have an operating environment different from the main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption.	3. When restoring backup data using own systems, financial entities shall use ICT systems that ~~*have an operating environment different from the main one, that is not directly connected with the latter*~~***are segregated, either physically or logically, from their main ICT system*** and that is securely protected from any unauthorized access or ICT corruption.	3. When restoring ~~backup data using own systems~~**services**, financial entities shall use **restore backup data on** ICT systems ~~that have an operating environment different~~**which are segregated (physically and logically)** from the ~~main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption~~**source system and that allow for the timely restoration of services making use of data and system backups as necessary**.
Article 11(3), second subparagraph			
276			

	Commission Proposal	EP Mandate	Council Mandate
	For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.	For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.	For ~~financial entities referred to in point (g) of Article 2(1)~~**central counterparties**, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.
Article 11(3), second subparagraph a			
276a			**Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.**
Article 11(4)			
277	4. Financial entities shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.	4. Financial entities shall ***assess the need to*** maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs ***and meet digital operational resilience requirements as set out in this Regulation***.	4. Financial entities **other than microenterprises** shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.
Article 11(5), first subparagraph			
278	5. Financial entities referred to in point (f) of Article 2(1) shall maintain or ensure that their ICT third-party providers maintain at least one secondary processing site endowed with	5. Financial entities referred to in point (f) of Article 2(1) shall maintain or ensure that their ICT third-party providers maintain at least one secondary processing site endowed with	5. ~~Financial entities referred to in point (f) of Article 2(1)~~**Central securities depositories** shall maintain ~~or ensure that their ICT third-party providers maintain~~ at least one secondary

	Commission Proposal	EP Mandate	Council Mandate
	resources, capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.	resources, capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.	processing site endowed with resources, capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.
Article 11(5), second subparagraph, introductory part			
279	The secondary processing site shall be:	The secondary processing site shall be:	The secondary processing site shall be:
Article 11(5), second subparagraph, point (a)			
280	(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;	(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;	(a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;
Article 11(5), second subparagraph, point (b)			
281	(b) capable of ensuring the continuity of critical services identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;	(b) capable of ensuring the continuity of critical services identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;	(b) capable of ensuring the continuity of critical services identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;
Article 11(5), second subparagraph, point (c)			
282	(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) ~~*immediately*~~ accessible to the financial entity's staff to ensure continuity of critical ~~*services*~~***or important functions*** in case the primary processing site has become unavailable.	(c) immediately accessible to the financial entity's staff to ensure continuity of critical services in case the primary processing site has become unavailable.

	Commission Proposal	EP Mandate	Council Mandate
Article 11(6)			
283	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.	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.
Article 11(7)			
284	7. When recovering from an ICT-related incident, financial entities shall perform multiple checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.	7. When recovering from an ICT-related incident, financial entities shall ~~*perform multiple checks, including reconciliations, in order to*~~ ensure that the level of data integrity is of the highest level***, for instance through performing multiple checks, including reconciliations. Such***~~*. These*~~ checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.	7. When recovering from an ICT-related incident, financial entities shall perform multiple checks, including reconciliations, in order to ensure that the level of data integrity is of the highest level. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.
Article 12			
285	Article 12 Learning and evolving	Article 12 Learning and evolving	Article 12 Learning and evolving
Article 12(1)			
286	1. Financial entities shall have in place	1. Financial entities shall have in place	1. Financial entities shall have in place

	Commission Proposal	EP Mandate	Council Mandate
	capabilities and staff, suited to their size, business and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.	capabilities and staff, suited to their size, business and risk profiles, to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.	capabilities and staff, ~~suited to their size, business and risk profiles,~~ to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse their likely impacts on their digital operational resilience.
Article 12(2), first subparagraph			
287	2. Financial entities shall put in place post ICT-related incident reviews after significant ICT disruptions of their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT Business Continuity Policy referred to in Article 10.	2. Financial entities shall put in place post ***major*** ICT-related incident reviews after significant ICT disruptions of their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT Business Continuity Policy referred to in Article 10.	2. Financial entities shall put in place post ICT-related incident reviews after significant ICT disruptions of their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy referred to in Article 10.
Article 12(2), second subparagraph			
288	When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authorities.	When implementing changes ***related to addressing ICT risk identified as the result of major ICT-related incident reviews***, financial entities other than microenterprises shall communicate ~~those~~ ***all significant*** changes to the competent authorities***, detailing the improvements required and how they aim to prevent or mitigate disruption in the future. Communication of changes to the competent authorities may be prior to or post the implementation of the changes***.	~~When implementing changes, financial entities other than microenterprises shall communicate those changes to the competent authorities.~~
Article 12(2), third subparagraph, introductory part			

	Commission Proposal	EP Mandate	Council Mandate
289	The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to:	The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to:	The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to:
Article 12(2), third subparagraph, point (a)			
290	(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;	(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;	(a) the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;
Article 12(2), third subparagraph, point (b)			
291	(b) the quality and speed in performing forensic analysis;	(b) the quality and speed in performing forensic analysis;	(b) the quality and speed in performing **ICT-related incident analysis and** forensic analysis **where deemed appropriate**;
Article 12(2), third subparagraph, point (c)			
292	(c) the effectiveness of incident escalation within the financial entity;	(c) the effectiveness of incident escalation within the financial entity;	(c) the effectiveness of incident escalation within the financial entity;
Article 12(2), third subparagraph, point (d)			
293	(d) the effectiveness of internal and external communication.	(d) the effectiveness of internal and external communication.	(d) the effectiveness of internal and external communication.
Article 12(3)			
294			

	Commission Proposal	EP Mandate	Council Mandate
	3. Lessons derived from the digital operation resilience testing carried out in accordance with Articles 23 and 24 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of business continuity or recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework referred to in Article 5(1).	3. Lessons derived from the digital operation resilience testing carried out in accordance with Articles 23 and 24 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of business continuity or recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework referred to in Article 5(1).	3. Lessons derived from the digital operation resilience testing carried out in accordance with Articles 23 and 24 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of business continuity ~~or~~**plans and ICT response and** recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework referred to in Article 5(1).
Article 12(4)			
295	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.	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.
Article 12(5)			
296			

	Commission Proposal	EP Mandate	Council Mandate
	5. Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.	5. Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.	5. Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.
Article 12(6), first subparagraph			
297	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*~~***The ICT security awareness programmes*** shall ~~*be applicable to*~~***apply to all staff. The digital operational resilience trainings shall apply to, at least,*** all employees ***with rights of direct access to the ICT systems*** and to senior management staff. ***The complexity of the training modules shall be commensurate to the level of direct access to the ICT systems of the staff member and, in particular, shall take account of their access to critical or important functions.***	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~~**include** senior management staff~~.~~ **and, if relevant, ICT third-party service providers.**
Article 12(6), second subparagraph			
298	Financial entities shall monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience. They shall keep abreast of the latest ICT risk management processes, effectively countering	Financial entities***, other than microenterprises,*** shall monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience. They shall keep abreast of the latest ICT risk management processes,	**7.** Financial entities **other than microenterprises** shall monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience. They shall keep abreast of the latest ICT risk

	Commission Proposal	EP Mandate	Council Mandate
	current or new forms of cyber-attacks.	effectively countering current or new forms of cyber-attacks.	management processes, effectively countering current or new forms of cyber-attacks.
Article 13			
299	Article 13 Communication	Article 13 Communication	Article 13 Communication
Article 13(1)			
300	1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.	1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of***, at least, major*** ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.	1. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate.
Article 13(1a)			
300a		***The communication plans referred to in the first subparagraph shall also ensure the disclosure to clients and counterparts, on an annual basis, of a summary of all ICT-related incidents. Such a disclosure shall fully respect the business confidentiality of the financial entity and of its clients and counterparts, and shall not jeopardise the ICT risk management framework referred to in Article 5(1).***	
Article 13(2)			
301			

	Commission Proposal	EP Mandate	Council Mandate
	2. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.	2. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.	2. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement communication policies for staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.
Article 13(3)			
302	3. At least one person in the entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the role of public and media spokesperson for that purpose.	3. At least one person in the entity shall be tasked with implementing the communication strategy for ***at least major*** ICT-related incidents and fulfil the role of public and media spokesperson for that purpose.	3. At least one person in the entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the role of public and media ~~spokesperson~~**function** for that purpose.
Article 14			
303	Article 14 Further harmonisation of ICT risk management tools, methods, processes and policies	Article 14 Further harmonisation of ICT risk management tools, methods, processes and policies	Article 14 Further harmonisation of ICT risk management tools, methods, processes and policies
Article 14, first paragraph, introductory part			
304	The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) shall, in consultation with the European Union Agency on Cybersecurity (ENISA), develop	The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) shall, in consultation with the European Union Agency on Cybersecurity (ENISA), develop	The ~~European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) shall~~**ESAs shall, through the Joint Committee**, in consultation with the European

	Commission Proposal	EP Mandate	Council Mandate
	draft regulatory technical standards for the following purposes:	draft regulatory technical standards for the following purposes:	Union Agency on Cybersecurity (ENISA), develop **common** draft regulatory technical standards for the following purposes:
Article 14, first paragraph, point (a)			
305	(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the authenticity and integrity of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions;	(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the authenticity and integrity of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions ***and undue delays***;	(a) specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 8(2), with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the ~~authenticity and integrity~~**confidentiality, integrity and availability** of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions;
Article 14, first paragraph, point (b)			
306	(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;	(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;*~~	(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;~~
Article 14, first paragraph, point (c)			
307	(c) specify further the appropriate techniques, methods and protocols referred to in point (b) of	(c) ~~*specify further the appropriate techniques, methods and protocols referred to in point (b)*~~	(c) ~~specify further the appropriate techniques, methods and protocols referred to in point (b) of~~

	Commission Proposal	EP Mandate	Council Mandate
	Article 8(4);	~~*of Article 8(4);*~~	~~Article 8(4);~~
Article 14, first paragraph, point (d)			
308	(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;	(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;	(d) develop further components of the controls of access management rights referred to in point (c) of Article 8(4) and associated human resources policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risks through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;
Article 14, first paragraph, point (e)			
309	(e) develop further the elements specified in Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;	(e) develop further the elements specified in Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;	(e) develop further the elements specified in Article 9(1) enabling a prompt detection of anomalous activities and the criteria referred to in Article 9(2) triggering ICT-related incident detection and response processes;
Article 14, first paragraph, point (f)			
310	(f) specify further the components of the ICT Business Continuity Policy referred to in Article 10(1);	(f) specify further the components of the ICT Business Continuity Policy referred to in Article 10(1);	(f) specify further the components of the ICT business continuity ~~Policy~~**p** referred to in Article 10(1);
Article 14, first paragraph, point (g)			
311	(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to	(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to	(g) specify further the testing of ICT business continuity plans referred to in Article 10(5) to

	Commission Proposal	EP Mandate	Council Mandate
	ensure that it duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency or other failures of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;	ensure that it duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency or other failures of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;	ensure that it duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency or other failures of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;
Article 14, first paragraph, point (h)			
312	(h) specify further the components of the ICT Disaster Recovery Plan referred to in Article 10(3).	(h) specify further the components of the ICT Disaster Recovery Plan referred to in Article 10(3).	(h) specify further the components of the ICT ~~Disaster~~**response and** recovery ~~Plan~~**plans** referred to in Article 10(3).
Article 14, first paragraph a			
312a			**When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors.**
Article 14, second paragraph			
313	EBA, ESMA and EIOPA shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force].	EBA, ESMA and EIOPA shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force].	~~EBA, ESMA and EIOPA~~**The ESAs** shall submit those draft regulatory technical standards to the Commission by [OJ: insert date ~~1 year~~**18 months** after the date of entry into

	Commission Proposal	EP Mandate	Council Mandate
			force].
Article 14, third paragraph			
314	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.
Article 14a			
314a		***Article 14a*** ***ICT risk management framework for small, non-interconnected and exempt entities***	
Article 14a, first paragraph, introductory part			
314b		***1. Pursuant to Article 3a, small and non-interconnected investment firms, payment institutions exempted by Directive (EU) 2015/2366, credit institutions exempted by Directive 2013/36/EU, electronic money institutions exempted by Directive 2009/110/EC and small institutions for occupational retirement pensions, shall put in place and maintain a sound and documented ICT risk management framework that shall:***	
Article 14a, first paragraph, point (a)			
314c			

	Commission Proposal	EP Mandate	Council Mandate
		(a) detail the mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, including for the protection of relevant physical components and infrastructures;	
Article 14a, first paragraph, point (b)			
314d		***(b) continuously monitor the security and functioning of all ICT systems;***	
Article 14a, first paragraph, point (c)			
314e		***(c) minimise the impact of ICT risks through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate for supporting the performance of their activities and the provision of services;***	
Article 14a, first paragraph, point (d)			
314f		***(d) adequately protect confidentiality, integrity and availability of data network and information systems;***	
Article 14a, first paragraph, point (e)			
314g		***(e) allow sources of risk and anomalies in the network and information systems to be promptly identified and detected and ICT incidents to be swiftly handled.***	

	Commission Proposal	EP Mandate	Council Mandate
Article 14a, second paragraph			
314h		***2. The ICT risk management framework referred to in paragraph 1 shall be documented and reviewed at least once a year, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring.***	
Article 14a, third paragraph			
314i		***A report on the review of the ICT risk management framework shall be submitted to the competent authority on an annual basis.***	
Article 14a			
314j			**Article 14a** **Proportionate ICT Risk Management framework**
Article 14a(1), introductory part			
314k			**1. Articles 4 to 14 shall not apply to institutions exempted under Directive 2013/36/EU, in respect of which Member States have decided not to apply the option referred to in Article 2(4), small and non-**

	Commission Proposal	EP Mandate	Council Mandate
			interconnected investment firms, payment institutions exempted under Directive (EU) 2015/2366, electronic money institutions exempted under Directive 2009/110/EC and small institutions for occupational retirement provision. **Financial entities referred to in the previous subparagraph shall implement an ICT Risk Management framework in accordance with the principle of proportionality, by taking into account the size, nature, scale and complexity of their services, activities and operations as well as their overall risk profile and shall:**
Article 14a(1), point (a)			
314l			**(a) put in place and maintain a sound and documented ICT risk management framework which details the mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, including for the protection of relevant physical components and infrastructures;**
Article 14a(1), point (b)			
314m			**(b) continuously monitor the security and functioning of all ICT systems;**
Article 14a(1), point (c)			

	Commission Proposal	EP Mandate	Council Mandate
314n			**(c) minimize the impact of ICT risks through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect confidentiality, integrity and availability of data network and information systems;**
Article 14a(1), point (d)			
314o			**(d) allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled;**
Article 14a(1), point (e)			
314p			**(e) identify key dependencies on ICT third-party service providers;**
Article 14a(1), point (f)			
314q			**(f) ensure the continuity of critical and important functions, through business continuity plans response and recovery measures, which include, at least, back-up and restore measures;**
Article 14a(1), point (g)			
314r			

	Commission Proposal	EP Mandate	Council Mandate
			(g) test, on a regular basis, the plans and measures referred to in point (f) as well as the effectiveness of the controls implemented according to points (a) and (c) above;
Article 14a(1), point (h)			
314s			**(h) implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process and develop, according to needs and ICT risk profile, ICT security training and awareness programs for staff and management.**
Article 14a(2), introductory part			
314t			**2. The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards for the following purposes:**
Article 14a(2), point (a)			
314u			**(a) specify further the elements to be included in the ICT risk management framework referred to in point (a) of paragraph 1;**

	Commission Proposal	EP Mandate	Council Mandate
Article 14a(2), point (b)			
314v			**(b) specify further the elements in relation to measures, protocols and tools to minimize the impact of ICT risks referred to in point (c) of paragraph 1, with a view to ensure the security of networks, enable adequate safeguards against intrusions and data misuse and preserve the confidentiality, integrity and availability of data;**
Article 14a(2), point (c)			
314w			**(c) specify further the components of the ICT business continuity plans referred to in point (f) of paragraph 1;**
Article 14a(2), point (d)			
314x			**(d) specify further the rules on the testing of ICT business continuity plans and of the effectiveness of the ICT controls implemented referred to in point (g) of paragraph 1 to ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails.**
Article 14a(2), second subparagraph			
314y			**When developing those draft regulatory**

	Commission Proposal	EP Mandate	Council Mandate
			technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities.
Article 14a(2), third subparagraph			
314z			**The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 18 months year after the date of entry into force].**
Article 14a(2), fourth subparagraph			
314aa			**Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.**
CHAPTER III			
315	CHAPTER III ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING	CHAPTER III ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING	CHAPTER III ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING
Article 15			
316			

	Commission Proposal	EP Mandate	Council Mandate
	Article 15 ICT-related incident management process	Article 15 ICT-related incident management process	Article 15 ICT-related incident management process
Article 15(1)			
317	1. Financial entities shall establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents and shall put in place early warning indicators as alerts.	1. Financial entities shall establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents and shall put in place early warning indicators as alerts.	1. Financial entities shall **define,** establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents ~~and shall put in place early warning indicators as alerts~~.
Article 15(2)			
318	2. Financial entities shall establish appropriate processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents.	2. Financial entities shall establish appropriate ***procedures and*** processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to make sure that root causes are identified and ~~*eradicated*~~***addressed in order*** to prevent the occurrence of such incidents.	2. Financial entities shall establish appropriate processes to ensure a consistent and integrated ~~monitoring, handling and~~ follow-up of ICT-related incidents, to make sure that root causes are identified**, documented** and eradicated to prevent the occurrence of such incidents.
Article 15(3), introductory part			
319	3. The ICT-related incident management process referred to in paragraph 1 shall:	3. The ICT-related incident management process referred to in paragraph 1 shall:	3. The ICT-related incident management process referred to in paragraph 1 shall:
Article 15(3), point (a)			
320	(a) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and to the severity and criticality of the services impacted, in	(a) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and to the severity and criticality of the services impacted, in	(a) establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority ~~and to the severity and criticality of the services impacted,~~ in

	Commission Proposal	EP Mandate	Council Mandate
	accordance with the criteria referred to in Article 16(1);	accordance with the criteria referred to in Article 16(1);	accordance with the criteria referred to in Article 16(1);
Article 15(3), point (b)			
321	(b) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;	(b) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;	(b) assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;
Article 15(3), point (c)			
322	(c) set out plans for communication to staff, external stakeholders and media in accordance with Article 13, and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;	(c) set out plans for communication to staff, external stakeholders and media in accordance with Article 13, and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;	(c) set out plans for communication to staff~~,~~ **and** external stakeholders ~~and media~~ in accordance with Article 13, and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;
Article 15(3), point (d)			
323	(d) ensure that major ICT-related incidents are reported to relevant senior management and inform the management body on major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of ICT-related incidents;	(d) ensure that ***at least*** major ICT-related incidents are reported to relevant senior management and inform the management body on major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of ***major*** ICT-related incidents;	(d) ensure that **at least** major ICT-related incidents are reported to relevant senior management and inform the management body on major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of ICT-related incidents;
Article 15(3), point (e)			
324			

	Commission Proposal	EP Mandate	Council Mandate
	(e) establish ICT-related incident response procedures to mitigate impacts and ensure that services becomes operational and secure in a timely manner.	(e) establish ICT-related incident response procedures to mitigate impacts and ensure that services becomes operational and secure in a timely manner.	(e) establish ICT-related incident response procedures to mitigate impacts and ensure that services ~~becomes~~**become** operational and secure in a timely manner.
Article 16			
325	Article 16 Classification of ICT-related incidents	Article 16 Classification of ICT-related incidents	Article 16 Classification of ICT-related incidents**[and cyber threats]**
Article 16(1), introductory part			
326	1. Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:	1. Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:	1. Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:
Article 16(1), point (a)			
327	(a) the number of users or financial counterparts affected by the disruption caused by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;	(a) the number of users or financial counterparts affected by the disruption caused by the ICT-related incident~~, *and whether the ICT-related incident has caused reputational impact*~~;	(a) the number **and/or relevance of clients**~~of users~~ or financial counterparts affected ~~by the disruption caused~~**and, where applicable, the amount or number of transactions affected** by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;
Article 16(1), point (b)			
328	(b) the duration of the ICT-related incident, including service downtime;	(b) the duration of the ICT-related incident, including service downtime;	(b) the duration of the ICT-related incident, including **the** service downtime;

	Commission Proposal	EP Mandate	Council Mandate
Article 16(1), point (c)			
329	(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;	(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;	(c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;
Article 16(1), point (d)			
330	(d) the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss;	(d) the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss;	(d) the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss**,** or availability loss;
Article 16(1), point (e)			
331	(e) the severity of the impact of the ICT-related incident on the financial entity's ICT systems;	(e) the severity of the impact of the ICT-related incident on the financial entity's ICT systems;	(e) ~~the severity of the impact of the ICT-related incident on the financial entity's ICT systems;~~
Article 16(1), point (f)			
332	(f) the criticality of the services affected, including the financial entity's transactions and operations;	(f) the criticality of the services affected, including the financial entity's transactions and operations;	(f) the criticality of the services affected, including the financial entity's transactions and operations;
Article 16(1), point (g)			
333	(g) the economic impact of the ICT-related incident in both absolute and relative terms.	(g) the economic impact of the ICT-related incident in both absolute and relative terms.	(g) the economic impact**, in particular on indirect and direct cost and losses,** of the ICT-related incident in both absolute and relative terms.

	Commission Proposal	EP Mandate	Council Mandate
Article 16(1a)			
333a			**1a. [Financial entities shall classify significant cyber threats based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.]**
Article 16(2), introductory part			
334	2. The ESAs shall, through the Joint Committee of the ESAs (the 'Joint Committee') and after consultation with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards further specifying the following:	2. The ESAs shall, through the Joint Committee of the ESAs (the 'Joint Committee') and ~~*after consultation*~~ ***in coordination*** with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards further specifying the following:	2. The ESAs shall, through the Joint Committee ~~of the ESAs (the 'Joint Committee') and after~~**and in** consultation with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards further specifying the following:
Article 16(2), point (a)			
335	(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents which are subject to the reporting obligation laid down in Article 17(1);	(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents ~~*which*~~***that*** are subject to the reporting obligation laid down in Article 17(1);	(a) the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents **or, as applicable, major operational or security payment-related incidents** which are subject to the reporting obligation laid down in Article 17(1);
Article 16(2), point (b)			
336	(b) the criteria to be applied by competent authorities for the purpose of assessing the	(b) the criteria to be applied by competent authorities for the purpose of assessing the	(b) the criteria to be applied by competent authorities for the purpose of assessing the

	Commission Proposal	EP Mandate	Council Mandate
	relevance of major ICT-related incidents to other Member States' jurisdictions, and the details of ICT-related incidents reports to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.	relevance of major ICT-related incidents to other Member States' jurisdictions, and the details of ***major*** ICT-related incidents reports to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.	relevance of major ICT-related incidents **or, as applicable, major operational or security payment-related incidents to relevant competent authorities in** ~~to~~ other Member States~~' jurisdictions~~, and the details of **reports for major** ICT-related incidents ~~reports~~**or, as applicable, major operational or security payment-related incidents** to be shared with other competent authorities pursuant to points (5) and (6) of Article 17.
Article 16(2), point (c)			
336a			**(c) [the criteria set out in paragraph 1a, including high materiality thresholds for determining significant cyber threats which are subject to the reporting obligation laid down in Article 17(1a).]**
Article 16(3), first subparagraph			
337	3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account international standards, as well as specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors.	3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account international standards, as well as specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. ***The ESAs shall further take into account that the timely and efficient management of an incident by small and microenterprises is not constricted by the need to respect the classification requirements set out in this Article. The ESAs shall also take***	3. When developing the common draft regulatory technical standards referred to in paragraph 2, the ESAs shall take into account ~~international standards~~**the size, nature, scale, complexity and overall risk profile of the financial entities**, as well as **international standards and** specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors.

	Commission Proposal	EP Mandate	Council Mandate
		into consideration the size of financial entities, the nature, scale and complexity of their services, activities and operations, and their overall risk profile.	
Article 16(3), second subparagraph			
338	The ESAs shall submit those common draft regulatory technical standards to the Commission by [PO: insert date 1 year after the date of entry into force].	The ESAs shall submit those common draft regulatory technical standards to the Commission by [PO: insert date ~~*1 year*~~***2 years*** after the date of entry into force].	The ESAs shall submit those common draft regulatory technical standards to the Commission by [PO: insert date ~~1 year~~**18 months** after the date of entry into force].
Article 16(3), third subparagraph			
339	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 2 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.
Article 17			
340	Article 17 Reporting of major ICT-related incidents	Article 17 Reporting of major ICT-related incidents	Article 17 Reporting of major ICT-related incidents **[and significant cyber threats]**
Article 17(1), first subparagraph			
341	1. Financial entities shall report major ICT-related incidents to the relevant competent	1. Financial entities shall report major ICT-related incidents to the relevant competent	1. Financial entities shall report major ICT-related incidents to the relevant competent

	Commission Proposal	EP Mandate	Council Mandate
	authority as referred to in Article 41, within the time-limits laid down in paragraph 3.	authority as referred to in Article 41, within the time-limits laid down in paragraph 3.	authority as referred to in Article 41, within the time-limits ~~laid down in paragraph 3.~~ **set out in accordance with Article 18(1a).**
Article 17(1), first subparagraph a			
341a			**Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 41, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this Article.**
Article 17(1), first subparagraph b			
341b			**Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013 shall report major ICT-related incidents to relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU that shall systematically and immediately, transmit the report to the ECB.**
Article 17(1), second subparagraph			
342	For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, an incident report using the template referred to in	For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, an incident report using the template referred to in	For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, ~~an incident report~~**the initial notification and**

	Commission Proposal	EP Mandate	Council Mandate
	Article 18 and submit it to the competent authority.	Article 18 and submit it to the competent authority.	**reports referred to in paragraph 3** using the template referred to in Article 18 and submit it to the competent authority. **In case of technical impossibility of submitting the template, financial entities shall submit the initial notification to the competent authority via alternative communication channels.**
Article 17(1), third subparagraph			
343	The report shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.	The report shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.	The ~~report~~**initial notification and reports referred to in paragraph 3** shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts.
Article 17(1), third subparagraph a, introductory part			
343a			**Without prejudice to the reporting by the financial entity to the relevant competent authority, pursuant to the first subparagraph, Member States may additionally determine that:**
Article 17(1), third subparagraph a, point (a)			
343b			**(a) the competent authority shall in a timely manner provide the initial notification [, the notification referred in paragraph 1a] and each report referred to in paragraph 3 to the national single point of contact, the national**

	Commission Proposal	EP Mandate	Council Mandate
			competent authorities or the national Computer Security Incident Response Teams designated, respectively, in accordance with Articles 8 and 9 of Directive (EU) 2016/1148;
Article 17(1), third subparagraph a, point (b)			
343c			**(b) some or all financial entities shall also provide the initial notification [, the notification referred in paragraph 1a] and each report referred to in paragraph 3 using the template referred to in Article 18 to the national competent authorities or the national Computer Security Incident Response Teams designated in accordance with Articles 8 and 9 of Directive (EU) 2016/1148.**
Article 17(1a), first subparagraph			
343d		***1a. Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities in accordance with paragraph 5.***	**1a [Financial entities shall classify a significant cyber threat and notify a significant cyber threat without undue delay to the relevant competent authority as referred to in Article 41.]** **[Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013 shall report significant cyber threats to relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU that shall systemically and immediately, transmit the**

	Commission Proposal	EP Mandate	Council Mandate
			report to the ECB.]
Article 17(2)			
344	2. Where a major ICT-related incident has or may have an impact on the financial interests of service users and clients, financial entities shall, without undue delay, inform their service users and clients about the major ICT-related incident and shall as soon as possible inform them of all measures which have been taken to mitigate the adverse effects of such incident.	2. Where a major ICT-related incident ~~*has or may have an*~~***occurs and has a material*** impact on the financial interests of service users and clients, financial entities shall, without undue delay ***after having become aware of it***, inform their service users and clients about the major ICT-related incident and shall ~~*as soon as possible*~~ inform them of ~~*all measures which*~~ ***the pertinent measures that*** have been taken to mitigate the adverse effects of such incident. ***Where no harm to service users and clients materialises due to the countermeasures taken by the financial entity, the requirement to inform service users and clients shall not apply.***	2. Where a major ICT-related incident has ~~or may have~~ an impact on the financial interests of ~~service users and~~ clients, financial entities shall, without undue delay, inform their ~~service users and~~ clients about the major ICT-related incident and shall as soon as possible inform them of all measures which have been taken to mitigate the adverse effects of such incident. **[Financial entities shall inform, without undue delay, their clients that are potentially affected by a significant cyber threat, communicating where appropriate the type of measures which the recipients may take accordingly.]**
Article 17(3), introductory part			
345	3. Financial entities shall submit to the competent authority as referred to in Article 41:	3. Financial entities shall submit to the competent authority as referred to in Article 41:	3. Financial entities shall submit to the competent authority as referred to in Article 41 **within the time-limits set out in accordance with Article 18(1a)**:
Article 17(3), point (a)			
346	(a) an initial notification, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place	(a) an initial notification~~*, without delay, but no later than the end*~~ of the ~~*business day, or, in case of a*~~ major ICT-related incident that ~~*took*~~	(a) an initial notification~~, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place~~

	Commission Proposal	EP Mandate	Council Mandate
	later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available;	~~*place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available,*~~ ***shall contain information available to the notifying entity on a best efforts basis as follows:***	~~later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available~~;
Article 17(3), point (a)(i)			
346a		***(i) with regard to incidents that significantly disrupt the availability of the services provided by the financial entity, the competent authority shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***	
Article 17(3), point (a)(ii)			
346b		***(ii) with regard to incidents that have a significant impact on the financial entity other than on the availability of the services provided by that financial entity, the competent authority shall be notified without undue delay and in any event within 72 hours of becoming aware of the incident;***	
Article 17(3), point (a)(iii)			
346c		***(iii) with regard to incidents that have an impact on the integrity, confidentiality or security of personal data maintained by that***	

	Commission Proposal	EP Mandate	Council Mandate
		financial entity, the competent authority shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;	
Article 17(3), point (b)			
347	(b) an intermediate report, no later than 1 week after the initial notification referred to in point (a), followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;	(b) an intermediate report, ~~*no later than 1 week*~~***as soon as the status of the original incident has changed significantly or new information has come to light that could have a major impact on how the ICT-related incident is addressed by the competent authority,*** after the initial notification referred to in point (a), followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;	(b) an intermediate report, ~~no later than 1 week~~ after the initial notification referred to in point (a), followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;
Article 17(3), point (c)			
348	(c) a final report, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates, but not later than one month from the moment of sending the initial report	(c) a final report, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates, but not later than one month from the ~~*moment*~~***date*** of sending the initial report.	(c) a final report, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates~~, but not later than one month from the moment of sending the initial report~~**.**
Article 17(3), point (ca)			
348a		***(ca) in the case of an ongoing incident at the***	

	Commission Proposal	EP Mandate	Council Mandate
		time of submission of the final report referred to in point (c), a final report shall be provided one month after the incident has been resolved.	
Article 17(3a)			
348b		***The relevant competent authority referred to in Article 41 shall provide that, in duly justified cases, a financial entity is permitted to deviate from the deadlines set out in points (a), (b), (c) and (ca) of this paragraph, giving due consideration to the ability of financial entities to provide accurate and meaningful information in relation to major ICT-related incidents.***	
Article 17(4)			
349	4. Financial entities may only delegate the reporting obligations under this Article to a third-party service provider upon approval of the delegation by the relevant competent authority referred to in Article 41.	4. Financial entities may only delegate the reporting obligations under this Article to a third-party service provider upon approval of the delegation by the relevant competent authority referred to in Article 41. ***In cases of such delegation, the financial entity shall remain fully accountable for the fulfilment of the incident reporting requirements.***	4. ~~Financial entities may only delegate the reporting obligations~~**The outsourcing of the reporting of major ICT-related incidents [or of the notification of significant cyber threats]** under this Article to ~~a~~ third-party service ~~provider upon approval of the delegation by~~**providers shall be subject to the conditions established in Section I of Chapter V and to the notification to** the relevant competent authority referred to in Article 41. **In case of such outsourcing, the financial entity remains fully accountable for the fulfilment of the incident reporting requirements.**

	Commission Proposal	EP Mandate	Council Mandate
Article 17(5), introductory part			
350	5. Upon receipt of the report referred to in paragraph 1, the competent authority shall, without undue delay, provide details of the incident to:	5. Upon receipt of the report referred to in paragraph 1, the competent authority shall, without undue delay, provide details of the ***major ICT-related*** incident to:	5. Upon receipt of the **initial notification and each** report referred to in paragraph ~~1~~**3[, as well as the notification of significant cyber threats referred to in paragraph 1.1]**, the competent authority shall, ~~without undue delay~~**in a timely manner and while respecting national legislation on national security**, provide details of the **major ICT-related** incident **[or the significant cyber threat]** to:
Article 17(5), point (a)			
351	(a) EBA, ESMA or EIOPA, as appropriate;	(a) EBA, ESMA or EIOPA, as appropriate;	(a) EBA, ESMA or EIOPA, as appropriate;
Article 17(5), point (b)			
352	(b) the ECB, as appropriate, in the case of financial entities referred to in points (a), (b) and (c) of Article 2(1); and	(b) the ECB, as appropriate, in the case of financial entities referred to in points (a), (b) and (c) of Article 2(1); and	(b) the ECB, as appropriate, in the case of financial entities referred to in points (a), (b) and (c) of Article 2(1); and
Article 17(5), point (c)			
353	(c) the single point of contact designated under Article 8 of Directive (EU) 2016/1148.	(c) the single point of contact designated under Article 8 of Directive (EU) 2016/1148~~.~~ ***or CSIRTs designated under Article 9 of Directive (EU) 2016/1149;***	(c) the single point of contact designated under Article 8 of Directive (EU) 2016/1148~~.~~**;**
Article 17(5), point (ca)			
353a			

	Commission Proposal	EP Mandate	Council Mandate
		(ca) the resolution authority responsible for the relevant financial entity. The Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014, and for the entities and groups referred to in Article 7(4)(b) and (5) of Regulation (EU) No 806/2014 where the conditions for the application of those paragraphs are met;	
Article 17(5), point (d)			
353b			**(d) other relevant public authorities under national law.**
Article 17(5), point (cb)			
353c		***(cb) national resolution authorities, in relation to entities and groups referred to in Article 7(3) of Regulation (EU) No 806/2014. National resolution authorities shall provide to the SRB, on a quarterly basis, a summary of the reports they have received under this point in relation to entities and groups referred to in Article 7(3) of Regulation (EU) No 806/2014;***	
Article 17(5), point (cc)			
353d		***(cc) other relevant public authorities, including ones in other Member States.***	
Article 17(6)			

	Commission Proposal	EP Mandate	Council Mandate
354	6. EBA, ESMA or EIOPA and the ECB shall assess the relevance of the major ICT-related incident to other relevant public authorities and notify them accordingly as soon as possible. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.	6. EBA, ESMA or EIOPA and the ECB***, in cooperation with ENISA,*** shall assess the relevance of the major ICT-related incident to other relevant public authorities and notify them accordingly as soon as possible. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.	6. **Following receipt of information in accordance with paragraph 5,** EBA, ESMA or EIOPA and the ECB **in cooperation with the competent authority** shall assess the relevance of the major ICT-related incident to other relevant ~~public~~**competent** authorities ~~and~~**in other Member States. Following this assessment EBA, ESMA or EIOPA shall** notify ~~them~~**relevant competent authorities in other Member States** accordingly as soon as possible. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.
Article 18			
355	Article 18 Harmonisation of reporting content and templates	Article 18 Harmonisation of reporting content and templates	Article 18 Harmonisation of reporting content and templates
Article 18(1), first subparagraph, introductory part			
356	1. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop:	1. The ESAs, through the Joint Committee and after consultation with ENISA and the ECB, shall develop:	1. The ESAs, through the Joint Committee and ~~after~~**in** consultation with ENISA and the ECB, shall develop:
Article 18(1), first subparagraph, point (a), introductory part			

	Commission Proposal	EP Mandate	Council Mandate
357	(a) common draft regulatory technical standards in order to:	(a) common draft regulatory technical standards in order to:	(a) common draft regulatory technical standards in order to:
Article 18(1), first subparagraph, point (a)(1)			
358	(1) establish the content of the reporting for major ICT-related incidents;	(1) establish the content of the reporting for major ICT-related incidents;	(1) establish the content of the reporting for major ICT-related incidents **taking into account the criteria laid out in the first paragraph of Article 16 for financial entities to classify ICT-related incidents, which shall include their relevance to other Member States, as well as reference to whether it constitutes a major operational or security payment-related incidents or not**;
Article 18(1), first subparagraph, point (a)(2)			
359	(2) specify further the conditions under which financial entities may delegate to a third-party service provider, upon prior approval by the competent authority, the reporting obligations set out in this Chapter;	(2) specify further the conditions under which financial entities may delegate to a third-party service provider, upon prior approval by the competent authority, the reporting obligations set out in this Chapter;	(2) ~~specify further the conditions under which financial entities may delegate to a third-party service provider, upon prior approval by the competent authority, the reporting obligations set out in this Chapter;~~**determine the time-limits for the initial notification and each report referred to in Article 17(3).**
Article 18(1), first subparagraph, point (a)(2a)			
359a		***(2a) specify further the criteria for determining the impact of a major ICT-related incident on a financial entity for the purposes of Article 17(3), point (a).***	

	Commission Proposal	EP Mandate	Council Mandate
Article 18(1), first subparagraph, point (a)(3)			
359b			**(3) [establish the content of the notification for significant cyber threats.]**
Article 18(1), first subparagraph, point (b)			
360	(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident.	(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident.	(b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident **[and notify a significant cyber threat]**.
Article 18(1), first subparagraph a			
360a			**When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities.**
Article 18(1), second subparagraph			
361	The ESAs shall submit the common draft regulatory technical standards referred to in point (a) of paragraph 1 and the common draft implementing technical standards referred to in point (b) of the paragraph 1 to the Commission by xx 202x [PO: insert date 1 year after the date of entry into force].	The ESAs shall submit the common draft regulatory technical standards referred to in point (a) of ~~*paragraph 1*~~***the first subparagraph*** and the common draft implementing technical standards referred to in point (b) of the ~~*paragraph 1*~~***first subparagraph*** to the Commission by xx 202x [PO: insert date ~~*1 year*~~***2 years*** after the date of entry into force].	The ESAs shall submit the common draft regulatory technical standards referred to in point (a) of paragraph 1 and the common draft implementing technical standards referred to in point (b) of the paragraph 1 to the Commission by xx 202x [PO: insert date ~~1 year~~**18 months** after the date of entry into force].

	Commission Proposal	EP Mandate	Council Mandate
Article 18(1), third subparagraph			
362	Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in point (a) of paragraph 1 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in point (a) of ~~paragraph 1~~***the first subparagraph*** in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the common regulatory technical standards referred to in point (a) of paragraph 1 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
Article 18(1), fourth subparagraph			
363	Power is conferred on the Commission to adopt the common implementing technical standards referred to in point (b) of paragraph 1 in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is conferred on the Commission to adopt the common implementing technical standards referred to in point (b) of ~~paragraph 1~~***the first subparagraph*** in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is conferred on the Commission to adopt the common implementing technical standards referred to in point (b) of paragraph 1 in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
Article 18(1a), first subparagraph			
363a		***1a. Pending the outcome of the feasibility report referred to in Article 19 on the further centralisation of incident reporting, the ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB, the SRB and ENISA, shall develop guidelines for the exchange of information on major ICT-related incident reports in***	

	Commission Proposal	EP Mandate	Council Mandate
		accordance with Article 17(5).	
Article 18(1a), second subparagraph, introductory part			
363b		***The guidelines referred to in the first subparagraph shall consider at least the following:***	
Article 18(1a), second subparagraph, point (a)			
363c		***(a) the most efficient lines of communication***	
Article 18(1a), second subparagraph, point (b)			
363d		***(b) maintaining the security, confidentiality and integrity of the data being exchanged;***	
Article 18(1a), second subparagraph, point (c)			
363e		***(c) the possible involvement of financial entities to complement the exchange of information referred to in Article 40.***	
Article 19			
364	Article 19 Centralisation of reporting of major ICT-related incidents	Article 19 Centralisation of reporting of major ICT-related incidents	Article 19 Centralisation of reporting of major ICT-related incidents
Article 19(1)			

	Commission Proposal	EP Mandate	Council Mandate
365	1. The ESAs, through the Joint Committee and in consultation with ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.	1. The ESAs, through the Joint Committee and in consultation with ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.	1. The ESAs, through the Joint Committee and in consultation with **the** ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.
Article 19(2), introductory part			
366	2. The report referred to in the paragraph 1 shall comprise at least the following elements:	2. The report referred to in the paragraph 1 shall comprise at least the following elements:	2. The report referred to in ~~the~~ paragraph 1 shall comprise at least the following elements:
Article 19(2), point (a)			
367	(a) prerequisites for the establishment of such an EU Hub;	(a) prerequisites for the establishment of ~~*such an*~~ ***a single*** EU Hub;	(a) prerequisites for the establishment of ~~such~~ an EU Hub;
Article 19(2), point (b)			
368	(b) benefits, limitations and possible risks;	(b) benefits, limitations and possible risks;	(b) benefits, limitations and ~~possible~~**risks including** risks **associated with the high concentration of sensitive information**;
Article 19(2), point (ba)			
368a		***(ba) capability to establish the interoperability***	

	Commission Proposal	EP Mandate	Council Mandate
		and assess its added value with regard to other relevant reporting schemes, including Directive (EU) 2016/1148.	
Article 19(2), point (c)			
369	(c) elements of operational management;	(c) elements of operational management;	(c) elements of operational management;
Article 19(2), point (d)			
370	(d) conditions of membership;	(d) conditions of membership;	(d) conditions of membership;
Article 19(2), point (e)			
371	(e) modalities for financial entities and national competent authorities to access the EU Hub;	(e) modalities for financial entities and national competent authorities to access the ***single*** EU Hub;	(e) modalities for financial entities and national competent authorities to access the EU Hub;
Article 19(2), point (f)			
372	(f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the EU Hub, including the required expertise	(f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the ***single*** EU Hub, including the required expertise	(f) a preliminary assessment of financial costs entailed by the setting-up the operational platform supporting the EU Hub, including the required expertise**.**
Article 19(3)			
373	3. The ESAs shall submit the report referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [OJ: insert date 3 years after the date of	3. The ESAs shall submit the report referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [OJ: insert date 3 years after the date of	3. The ESAs shall submit the report referred to in the paragraph 1 to the Commission, the European Parliament and to the Council by xx 202x [OJ: insert date 3 years after the date of

	Commission Proposal	EP Mandate	Council Mandate
	entry into force].	entry into force].	entry into force].
Article 20			
374	Article 20 Supervisory feedback	Article 20 Supervisory feedback	Article 20 Supervisory feedback
Article 20(1)			
375	1. Upon receipt of a report as referred to in Article 17(1), the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity, in particular to discuss remedies at the level of the entity or ways to minimise adverse impact across sectors.	1. Upon receipt of a report as referred to in Article 17(1), the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity, in particular to discuss remedies at the level of the entity or ways to minimise adverse impact across sectors ***and also provide appropriately anonymised feedback, insight and intelligence to all relevant financial entities where it could be beneficial, based on any major ICT- related incident reports that it receives***.	1. ~~Upon receipt of a report as referred to~~**Without prejudice to the technical input, advice or remedies and subsequent follow-up which may be provided, where applicable, in accordance with national law, by the national Computer Security Incident Response Teams pursuant to the tasks foreseen** in Article ~~17(1)~~**9 of Directive (EU) 2016/1148**, the competent authority shall**, upon** ~~acknowledge~~ receipt of **each initial** notification and ~~shall as quickly as possible~~**report as referred to in Article 17(3), acknowledge receipt of notification and may, where feasible,** provide ~~all necessary~~**in a timely manner relevant and proportionate** feedback or **high-level** guidance to the financial entity, in particular to **make available any relevant information on similar threats,** discuss remedies **applied** at the level of the entity ~~or~~**and** ways to minimise **and mitigate** adverse impact across **financial** sectors. **Without prejudice to the supervisory feedback received, financial entities shall remain fully accountable for the handling**

	Commission Proposal	EP Mandate	Council Mandate
			and consequences of the [threats and] incidents reported pursuant to Article 17[1.1 and] (3).
Article 20(2), first subparagraph			
376	2. The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the ICT-related incident notifications received from competent authorities, setting out at least the number of ICT-related major incidents, their nature, impact on the operations of financial entities or customers, costs and remedial actions taken.	2. The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the ***major*** ICT-related incident ***report*** notifications received from competent authorities, setting out at least the number of ICT-related major incidents, their nature, impact on the operations of financial entities or customers, ***estimated*** costs and remedial actions taken.	2. The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the **major** ICT-related incident **[and significant cyber threat]** notifications received from competent authorities **in accordance with Article 17(1) [and 17(1a)]**, setting out at least the number of ICT-related major incidents **[and significant cyber threats]**, their nature, impact on the operations of financial entities or customers, costs and remedial actions taken.
Article 20(2), second subparagraph			
377	The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.	The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.	The ESAs shall issue warnings and produce high-level statistics to support ICT threat and vulnerability assessments.
Article 20a			
377a		***Article 20a*** ***Operational or security payment-related incidents concerning certain financial entities***	**Article 14b** **Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions**

	Commission Proposal	EP Mandate	Council Mandate
Article 20a(1)			
377b		***The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents where they concern financial entities referred to in Article 2(1), points (a), (b) and (c).***	**The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, in case they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.**
CHAPTER IV			
378	CHAPTER IV DIGITAL OPERATIONAL RESILIENCE TESTING	CHAPTER IV DIGITAL OPERATIONAL RESILIENCE TESTING	CHAPTER IV DIGITAL OPERATIONAL RESILIENCE TESTING
Article 21			
379	Article 21 General requirements for the performance of digital operational resilience testing	Article 21 General requirements for the performance of digital operational resilience testing	Article 21 General requirements for the performance of digital operational resilience testing
Article 21(1)			
380	1. For the purpose of assessing preparedness for ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities shall establish, maintain and review,	1. For the purpose of assessing preparedness for ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities ***other than microenterprises*** shall	1. For the purpose of assessing preparedness for **handling** ICT-related incidents, of identifying weaknesses, deficiencies or gaps in the digital operational resilience and of promptly implementing corrective measures, financial entities **other than financial entities**

	Commission Proposal	EP Mandate	Council Mandate
	with due consideration to their size, business and risk profiles, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.	establish, maintain and review~~, with due consideration to their size, business and risk profiles,~~ a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.	**referred to in Article 14a and other than microenterprises** shall establish, maintain and review, with due consideration to their size, ~~business and risk profiles~~**nature, scale, complexity, and overall risk profile**, a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework referred to in Article 5.
Article 21(2)			
381	2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.	2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.	2. The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.
Article 21(3)			
382	3. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme referred to in paragraph 1, taking into account the evolving landscape of ICT risks, any specific risks to which the financial entity is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.	3. Financial entities shall follow a risk-based approach when conducting the digital operational resilience testing programme referred to in paragraph 1, taking into account the evolving landscape of ICT risks, any specific risks to which the financial entity is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.	3. Financial entities **referred to in paragraph 1** shall follow a risk-based approach when conducting the digital operational resilience testing programme referred to in paragraph 1**, with due consideration to their size, nature, scale, complexity, and overall risk profile**, taking into account the evolving landscape of ICT risks, any specific risks to which the financial entity is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.

	Commission Proposal	EP Mandate	Council Mandate
Article 21(4)			
383	4. Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external.	4. Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external. ***Where tests are undertaken by an internal tester, financial entities shall dedicate sufficient resources and ensure that conflicts of interest are avoided throughout the design and execution phases of the test.***	4. Financial entities **referred to in paragraph 1** shall ensure that tests are undertaken by independent parties, whether internal or external.
Article 21(5)			
384	5. Financial entities shall establish procedures and policies to prioritise, classify and remedy all issues acknowledged throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.	5. Financial entities shall establish procedures and policies to prioritise, classify and ~~*remedy*~~***address*** all issues acknowledged throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.	5. Financial entities **referred to in paragraph 1** shall establish procedures and policies to prioritise, classify and remedy all issues acknowledged throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.
Article 21(6)			
385	6. Financial entities shall test all critical ICT systems and applications at least yearly.	6. Financial entities shall ~~*test*~~***ensure that appropriate tests are conducted on*** all critical ICT systems and applications at least yearly.	6. Financial entities **referred to in paragraph 1** shall test all critical ICT systems and applications at least yearly.
Article 22			
386	Article 22 Testing of ICT tools and systems	Article 22 Testing of ICT tools and systems	Article 22 Testing of ICT tools and systems

	Commission Proposal	EP Mandate	Council Mandate
Article 22(1)			
387	1. The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, including vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.	1. The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests~~, *including*~~**.** ***Those tests may include*** vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.	1. The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, ~~including~~**with due consideration to the entity's size, nature, scale, complexity, and overall risk profile such as** vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing. **Financial entities shall either use internal or external testers for the deployment of the testing programme.**
Article 22(2)			
388	2. Financial entities referred to in points (f) and (g) of Article 2(1) shall perform vulnerability assessments before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.	2. Financial entities referred to in points (f) and (g) of Article 2(1) shall perform vulnerability assessments before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.	2. ~~Financial entities referred to in points (f) and (g) of Article 2(1)~~**Central securities depositories and central counterparties** shall perform vulnerability assessments before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.
Article 22(3)			
388a			**3. Financial entities referred to in Article**

	Commission Proposal	EP Mandate	Council Mandate
			14a and microenterprises shall perform the tests referred to in Paragraph 1 combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and time to be allocated to the ICT testing foreseen in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.
Article 23			
389	Article 23 Advanced testing of ICT tools, systems and processes based on threat led penetration testing	Article 23 Advanced testing of ICT tools, systems and processes based on threat led penetration testing	Article 23 Advanced testing of ICT tools, systems and processes based on threat led penetration testing
Article 23(1)			
390	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 ***the second subparagraph of*** paragraph ~~4~~***3*** shall carry out at least every 3 years advanced testing by means of threat led penetration testing.	1. Financial entities **other than financial entities referred to in Article 14a and other than microenterprises** identified in accordance with paragraph ~~4 shall~~**3shall** carry out ~~at least every 3 years~~**according to the frequency established by the competent authorities** advanced testing by means of threat led penetration testing **frameworks undertaken by external testers**.
Article 23(2), first subparagraph			

	Commission Proposal	EP Mandate	Council Mandate
391	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 ***or important*** functions and services of a financial entity, and shall be performed on live production systems supporting such functions ***where possible, or on pre-production systems with the same security configuration***. The precise scope of threat led penetration testing, based on the assessment of critical ***or important*** functions and services, shall be determined by financial entities and shall be validated by the competent authorities. ***It shall not be a requirement for a single threat led penetration test to cover all critical or important functions.***	2. **The** 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.
Article 23(2), second subparagraph			
392	For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or contracted to ICT third-party service providers.	For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical ***or important*** functions and services, including ***critical or important*** functions and services outsourced or contracted to ICT third-party service providers.	For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and **ICT** services outsourced or contracted to ICT third-party service providers **referred to in Article 27 (2)(l)**.
Article 23(2), third subparagraph			
393	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	Where ***critical ICT third-party service providers and, where necessary, non-critical*** ICT third-party service providers are included in the remit of the threat led penetration testing,	Where ICT third-party service providers are included in the remit of the threat led penetration testing, the financial entity shall take the necessary measures **and safeguards** to

	Commission Proposal	EP Mandate	Council Mandate
	participation of these providers.	the financial entity shall take the necessary measures to ensure the participation of these providers. ***Those ICT third-party service providers shall not be required to communicate information or provide any details in relation to items that are not relevant to the risk management controls of the relevant critical or important functions of the relevant financial entities. Such testing shall not adversely impact other customers of the ICT third-party service providers.***	ensure the participation of ~~these~~**such ICT third-party service** providers **and shall retain at all times the full responsibility for ensuring compliance with this Regulation**.
Article 23(2), third subparagraph a			
393a		***In cases where the involvement of an ICT third-party service provider in the threat led penetration testing could potentially 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, or on the overall integrity of the ICT third-party service provider's operations, the financial entity and the ICT third-party service provider may contractually agree that the ICT third-party service provider is permitted to enter directly into contractual arrangements with an external tester. ICT third-party service providers may enter into such arrangements on behalf of all their financial entity service users in order to conduct pooled testing.***	**Without prejudice to the obligation laid down in the first subparagraph, where, in the case referred to in the third subparagraph, an involvement of an ICT third-party service provider in the threat led penetration testing is reasonably expected to have an adverse impact on the quality, confidentiality or security of services delivered by the respective ICT third-party service provider to customers that do not fall within the scope of this Regulation, the financial entity and the ICT third-party service provider may agree that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled threat led penetration testing involving several financial entities to which the ICT third-party provides ICT services.**

	Commission Proposal	EP Mandate	Council Mandate
Article 23(2), third subparagraph b			
393b			**The pooled testing referred to in subparagraph 4 shall cover the relevant scope of services supporting the critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing referred to in subparagraph 4 shall be considered as threat led penetration testing carried out by respective pooled financial entities referred to in paragraph 1.**
Article 23(2), third subparagraph c			
393c			**The number of financial entities participating in the pooled threat led penetration testing shall be duly calibrated taking into account the complexity and types of services involved.**
Article 23(2), fourth subparagraph			
394	Financial entities shall apply effective risk management controls to reduce the risks of any potential impact to data, damage to assets and disruption to critical services or operations at the financial entity itself, its counterparties or to the financial sector.	Financial entities shall apply effective risk management controls to ~~*reduce*~~***mitigate*** the risks of any potential impact to data, damage to assets and disruption to critical ~~*services*~~***or important functions*** or operations at the financial entity itself, its counterparties or to the financial sector.	Financial entities shall**, with the cooperation of ICT third-party service providers and other involved parties, including the testers but excluding the competent authorities,** apply effective risk management controls to ~~reduce~~**mitigate** the risks of any potential impact ~~to~~**on** data, damage to assets and disruption to critical **or important functions,** services or

	Commission Proposal	EP Mandate	Council Mandate
			operations at the financial entity itself, its counterparties or to the financial sector.
Article 23(2), fifth subparagraph			
395	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~~***single public*** authority***, designated in accordance with paragraph 3a, or, in the case of ICT third-party service providers entering directly into contractual arrangements with external testers, to ENISA, a confidential summary of the test results and*** the documentation confirming that the threat led penetration testing has been conducted in accordance with the requirements. ***The single public authority or ENISA, as applicable, shall issue an attestation confirming that the test was performed in accordance with the requirements set out in the documentation in order to allow for mutual recognition of threat led penetration tests between*** competent authorities***. The attestation*** shall ~~*validate the documentation and issue an attestation*~~***be shared with the competent authority of the financial entity and, where relevant, with the Lead Overseer of the critical ICT third-party service provider***.	At the end of the test~~, after reports and remediation plans have been agreed, the financial entity and the external testers~~ **the financial entity, external testers and where applicable the designated authority in accordance with paragraph 3.1** shall provide to the competent authority the documentation ~~confirming~~**demonstrating** that the threat led penetration testing has been conducted in accordance with the requirements.~~ Competent authorities shall validate the documentation and issue an attestation.~~
Article 23(2), fifth subparagraph a			
395a			**Competent authorities or the authority**

	Commission Proposal	EP Mandate	Council Mandate
			designated in accordance with paragraph (3.1), when such task has been delegated to it, shall issue an attestation confirming, that the test was performed in accordance with the requirements in order to allow for mutual recognition of threat led penetration tests between competent authorities.
Article 23(2), fifth subparagraph b			
395b			**Without prejudice of such attestation, financial entities shall remain at all times fully responsible for the impacts of the tests referred to in the fourth subparagraph of Article 23 (2).**
Article 23(3), first subparagraph			
396	3. Financial entities shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.	3. Financial entities***, or ICT third-party service providers permitted to enter directly into contractual arrangements with an external tester in accordance with paragraph 2 of this Article,*** shall contract testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.	3. Financial entities shall contract **external** testers in accordance with Article 24 for the purposes of undertaking threat led penetration testing.
Article 23(3), second subparagraph, introductory part			
397	Competent authorities shall identify financial entities to perform threat led penetration testing in a manner that is proportionate to the size, scale, activity and overall risk profile of the	~~*Competent authorities shall identify financial entities to perform*~~***Without prejudice to their ability to delegate tasks and competences under this Article to other competent***	Competent authorities shall identify financial entities **required** to perform threat led penetration testing in a manner that is proportionate to the size, **nature,** scale,

	Commission Proposal	EP Mandate	Council Mandate
	financial entity, based on the assessment of the following:	***authorities in charge of*** threat led penetration testing***, competent authorities shall identify financial entities to perform threat led penetration testing in a proportionate manner*** ~~*in a manner that is proportionate to the size, scale, activity and overall risk profile of the financial entity,*~~ based on the assessment of the following:	~~activity~~**complexity** and overall risk profile of the financial entity, based on the assessment of the following:
Article 23(3), second subparagraph, point (a)			
398	(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;	(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;	(a) impact-related factors, in particular the criticality of services provided and activities undertaken by the financial entity;
Article 23(3), second subparagraph, point (b)			
399	(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;	(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;	(b) possible financial stability concerns, including the systemic character of the financial entity at national or Union level, as appropriate;
Article 23(3), second subparagraph, point (c)			
400	(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved.	(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved.	(c) specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved.
Article 23(3a), first subparagraph			
400a		***3a Member States shall designate a single public authority to be responsible for threat led penetration testing in the financial sector at***	**3a Member States may designate a single public authority in the financial sector responsible for threat led penetration testing**

	Commission Proposal	EP Mandate	Council Mandate
		national level, except for the identification of financial entities in accordance with paragraph 3, including threat led penetration testing undertaken by financial entities and by ICT third-party service providers entering directly into contractual arrangements with external testers. The designated single public authority shall be entrusted with all competences and tasks to that effect.	**related matters at national level in relation to threat led penetration testing in the financial sector and shall entrust it with all competences and tasks to that effect.**
Article 23(4), first subparagraph, introductory part -a			
400b			**3b. In the absence of a designation in accordance with paragraph 3a, a competent authority may delegate the exercise of some or all of the tasks referred to in Articles 23 and 24 to other national authority in the financial sector.**
Article 23(4), first subparagraph, introductory part			
401	4. EBA, ESMA and EIOPA shall, after consulting the ECB and taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests, develop draft regulatory technical standards to specify further:	4. ~~*EBA, ESMA and EIOPA shall*~~***The ESAs shall, in coordination with ENISA***, after consulting the ECB and taking into account relevant frameworks in the Union ~~*which*~~***that*** apply to intelligence-based ***threat led*** penetration tests, ***including the TIBER-EU framework,*** develop ***one set of*** draft regulatory technical standards to specify further:	4. EBA, ESMA and EIOPA shall~~, after consulting~~ **in agreement with** the ECB and ~~taking into account relevant frameworks in the Union which apply to intelligence-based penetration tests~~**in accordance with the TIBER-EU framework**, develop **joint** draft regulatory technical standards to specify further:
Article 23(4), first subparagraph, point (a)			
402			

	Commission Proposal	EP Mandate	Council Mandate
	(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 ~~6~~***3*** of this Article;	(a) the criteria used for the purpose of the application of paragraph ~~6~~**1** of this Article;
Article 23(4), first subparagraph, point (b), introductory part			
403	(b) the requirements in relation to:	(b) the requirements in relation to:	(b) the requirements in relation to:
Article 23(4), first subparagraph, point (b)(i)			
404	(i) the scope of threat led penetration testing referred to in paragraph 2 of this Article;	(i) the scope of threat led penetration testing referred to in paragraph 2 of this Article;	(i) the scope of threat led penetration testing referred to in paragraph 2 of this Article;
Article 23(4), first subparagraph, point (b)(ii)			
405	(ii) the testing methodology and approach to be followed for each specific phase of the testing process;	(ii) the testing methodology and approach to be followed for each specific phase of the testing process;	(ii) the testing methodology and approach to be followed for each specific phase of the testing process;
Article 23(4), first subparagraph, point (b)(iii)			
406	(iii) the results, closure and remediation stages of the testing;	(iii) the results, closure and remediation stages of the testing;	(iii) the results, closure and remediation stages of the testing;
Article 23(4), first subparagraph, point (c)			
407	(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	(c) the type of supervisory cooperation needed for the implementation ***and to facilitate full mutual recognition*** of threat led penetration testing in the context of financial entities	(c) the type of supervisory **and other relevant** cooperation needed for the implementation of threat led penetration testing in the context of financial entities which operate in more than

	Commission Proposal	EP Mandate	Council Mandate
	allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets..	~~which~~***that*** operate in more than one Member State ***and testing undertaken by external testers that have entered directly into contractual arrangements with ICT third-party service providers in accordance with paragraph 2 of this Article***, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.~~.~~	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.~~.~~
Article 23(4), first subparagraph a			
407a			**When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors.**
Article 23(4), second subparagraph			
408	The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date 2 months before the date of entry into force].	The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date ~~2~~***6*** months before the date of entry into force].	The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date ~~2~~**18** months ~~before~~**after** the date of entry into force].
Article 23(4), third subparagraph			
409	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with

	Commission Proposal	EP Mandate	Council Mandate
	Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
Article 24			
410	Article 24 Requirements for testers	Article 24 Requirements for testers	Article 24 Requirements for **external** testers
Article 24(1), introductory part			
411	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 permitted to enter directly into contractual arrangements with an external tester in accordance with Article 23(2)*** shall only use testers for the deployment of threat led penetration testing, which:	1. Financial entities **other than financial entities referred to in Article 14a and other than microenterprises** shall only use **external** testers for the deployment of threat led penetration testing, which:
Article 24(1), point (a)			
412	(a) are of the highest suitability and reputability;	(a) are of the highest suitability and reputability;	(a) are of the highest suitability and reputability;
Article 24(1), point (b)			
413	(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing;	(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing;	(b) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing;
Article 24(1), point (c)			

	Commission Proposal	EP Mandate	Council Mandate
414	(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;	(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks***, whether the testers are from within the Union, or from a third country***;	(c) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;
Article 24(1), point (d)			
415	(d) in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;	(d) ~~*in case of external testers,*~~ provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;	(d) ~~in case of external testers,~~**are independent and** provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing, including the proper protection of the financial entity's confidential information and redress for the business risks of the financial entity;
Article 24(1), point (e)			
416	(e) in case of external testers, are dully and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.	(e) ~~*in case of external testers,*~~ are dully and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.	(e) ~~in case of external testers, are dully~~**are duly** and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.
Article 24(1), point (ea)			
416a		***(ea) in the case of internal testers, their use has been approved by the relevant competent authority and by the single public authority designated in accordance with Article 23(3a), and those authorities have verified that the***	

	Commission Proposal	EP Mandate	Council Mandate
		financial entity has dedicated sufficient resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test.	
Article 24(2)			
417	2. Financial entities shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.	2. Financial entities ***and ICT third-party service providers permitted to enter directly into contractual arrangements with an external tester in accordance with Article 23(2)*** shall ensure that ~~*agreements*~~***arrangements*** concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.	2. Financial entities **other than financial entities referred to in Article 14a and other than microenterprises** shall ensure that agreements concluded with external testers require a sound management of the threat led penetration testing results and that any processing thereof, including any generation, draft, store, aggregation, report, communication or destruction, do not create risks to the financial entity.
CHAPTER V			
418	CHAPTER V MANAGING OF ICT THIRD-PARTY RISK	CHAPTER V MANAGING OF ICT THIRD-PARTY RISK	CHAPTER V MANAGING OF ICT THIRD-PARTY RISK
SECTION I			
419	SECTION I Key principles for a sound management of ICT third party risk	SECTION I Key principles for a sound management of ICT third party risk	SECTION I ~~Key principles for a sound management of ICT third party risk~~ **KEY PRINCIPLES FOR A SOUND MANAGEMENT OF ICT THIRD PARTY RISK**

	Commission Proposal	EP Mandate	Council Mandate
Article 25			
420	Article 25 General principles	Article 25 General principles	Article 25 General principles
Article 25, first paragraph, first subparagraph, introductory part			
421	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:
Article 25, first paragraph, first subparagraph, point (1)			
422	1. Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.	1. Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.	1. Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.
Article 25, first paragraph, first subparagraph, point (2), introductory part			
423	2. Financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account:	2. Financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account:	2. Financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account:

	Commission Proposal	EP Mandate	Council Mandate
Article 25, first paragraph, first subparagraph, point (2)(a)			
424	(a) the scale, complexity and importance of ICT-related dependencies,	(a) the ***nature,*** scale, complexity and importance of ICT-related dependencies,	(a) the scale, complexity and importance of ICT-related dependencies,
Article 25, first paragraph, first subparagraph, point (2)(b)			
425	(b) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level..	(b) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level..	(b) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and ~~quality~~**availability** of financial services and activities, at individual and at group level.~~.~~
Article 25, first paragraph, first subparagraph, point (2)(ba)			
425a		***(ba) whether a provider of ICT services is an ICT intra-group service provider.***	
Article 25, first paragraph, first subparagraph, point (3)			
426	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	3. As part of their ICT risk management framework, financial entities ***other than microenterprises*** shall adopt and regularly review a strategy on ICT third-party risk~~, taking into account the multi-vendor strategy referred to in point (g) of Article 5(9)~~. That strategy shall	3. As part of their ICT risk management framework **as referred to in Article 5 paragraph 1**, financial entities **other than financial entities referred to in Article 14a and other microenterprises** shall adopt and regularly review a strategy on ICT third-party

	Commission Proposal	EP Mandate	Council Mandate
	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.	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.	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 **concerning critical or important functions** provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall **in accordance with the size, nature, scale, complexity and overall risk profile of the financial entity** regularly review the risks identified in respect ~~of outsourcing of~~**to contractual arrangements on the use of ICT services concerning** critical or important functions.
Article 25, first paragraph, first subparagraph, point (4)			
427	4. As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover critical or important functions and those that do not.	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 ***supporting critical or important functions*** provided by ICT third-party service providers. The contractual arrangements referred to in the first subparagraph shall be appropriately documented.	4. As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. The contractual arrangements referred to in the first subparagraph shall be appropriately documented~~,~~ distinguishing between those that cover critical or important functions and those that do not.

	Commission Proposal	EP Mandate	Council Mandate
	Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided. Financial entities shall make available to the competent authority, upon request, the full Register of Information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity. Financial entities shall inform the competent authority in a timely manner about planned contracting of critical or important functions and when a function has become critical or important.	***Where available, financial entities shall follow the guidelines and other measures issued by the ESAs and competent authorities until the entry into force of the implementing technical standards referred to in paragraph 10.*** ~~*, distinguishing between those that cover critical or important functions and those that do not.*~~ Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services ***supporting critical or important functions***, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided. Financial entities shall make available to the competent authority, upon request, the full Register of Information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity. Financial entities shall inform the competent	Financial entities shall ~~report~~**transmit** 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.~~ ~~**the register of information.**~~ Financial entities shall make available to the competent authority, upon request, the full register of information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity. Financial entities shall inform the competent authority in a timely manner about **any** planned ~~contracting of~~ **contractual arrangements on the use of ICT services concerning** critical or important functions and when ~~a function~~**an ICT service** has become critical or important.

	Commission Proposal	EP Mandate	Council Mandate
		authority in a timely manner about planned contracting of critical or important functions and when a function has become critical or important.	
Article 25, first paragraph, first subparagraph, point (5), introductory part			
428	5. Before entering into a contractual arrangement on the use of ICT services, financial entities shall:	5. Before entering into a contractual arrangement on the use of ICT services, financial entities shall:	5. Before entering into a contractual arrangement on the use of ICT services, financial entities shall:
Article 25, first paragraph, first subparagraph, point (5)(a)			
429	(a) assess whether the contractual arrangement covers a critical or important function;	(a) assess whether the contractual arrangement covers a critical or important function;	(a) assess whether the contractual arrangement covers **the use of ICT services concerning** a critical or important function;
Article 25, first paragraph, first subparagraph, point (5)(b)			
430	(b) assess if supervisory conditions for contracting are met;	(b) assess if supervisory conditions for contracting are met;	(b) assess if supervisory conditions for contracting are met;
Article 25, first paragraph, first subparagraph, point (5)(c)			
431	(c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT concentration risk;	(c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT concentration risk;	(c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT **related** concentration risk **as referred to in**

	Commission Proposal	EP Mandate	Council Mandate
			Article 26;
Article 25, first paragraph, first subparagraph, point (5)(d)			
432	(d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;	(d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;	(d) undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;
Article 25, first paragraph, first subparagraph, point (5)(e)			
433	(e) identify and assess conflicts of interest that the contractual arrangement may cause.	(e) identify and assess conflicts of interest that the contractual arrangement may cause.	(e) identify and assess conflicts of interest that the contractual arrangement may cause.
Article 25, first paragraph, first subparagraph, point (6)			
434	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 ***up-to-date security standards.*** The latest ~~*information*~~***standards shall also be considered when determining whether the*** security standards ***in place are appropriate***.	6. Financial entities may only enter into contractual arrangements **on the use of ICT services concerning critical or important functions** with ICT third-party service providers that comply with high~~, appropriate and the latest~~ **and appropriate** information security standards.
Article 25, first paragraph, first subparagraph, point (7)			
435	7. In exercising access, inspection and audit rights over the ICT third-party service provider,	7. In exercising access, inspection and audit rights over the ICT third-party service provider	7. In exercising access, inspection and audit rights over the ICT third-party service provider,

	Commission Proposal	EP Mandate	Council Mandate
	financial entities shall on a risk-based approach pre-determine the frequency of audits and inspections and the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. For contractual arrangements that entail a high level of technological complexity, the financial entity shall verify that auditors, whether internal, pools of auditors or external auditors possess appropriate skills and knowledge to effectively perform relevant audits and assessments.	***in relation to critical or important functions***, financial entities shall on a risk-based approach pre-determine the frequency of audits and inspections and the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. For contractual arrangements that entail a ~~*high level of*~~***detailed*** technological complexity, the financial entity shall verify that auditors, whether internal, pools of auditors or external auditors possess appropriate skills and knowledge to effectively perform relevant audits and assessments.	financial entities shall on a risk-based approach pre-determine the frequency of audits and inspections and the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. For contractual arrangements that entail a high level of technological complexity, the financial entity shall verify that auditors, whether internal, pools of auditors or external auditors possess appropriate skills and knowledge to effectively perform relevant audits and assessments.
Article 25, first paragraph, first subparagraph, point (8), introductory part			
436	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 terminated*~~ ***allow the financial entities to take appropriate corrective or remedial measures, which could include wholly terminating the arrangements, if no rectification is possible, or partially terminating the arrangements, if rectification is possible, under applicable law*** at least under the following circumstances:	8. Financial entities shall ensure that contractual arrangements on the use of ICT services ~~are~~ **concerning critical or important functions may be** terminated at least under the following circumstances:
Article 25, first paragraph, first subparagraph, point (8)(a)			

	Commission Proposal	EP Mandate	Council Mandate
437	(a) breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;	(a) ***significant*** breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;	(a) ~~breach~~**substantial breaches** by the ICT third-party service provider of applicable laws, regulations or contractual terms;
Article 25, first paragraph, first subparagraph, point (8)(aa)			
437a		***(aa) a recommendation issued by the Joint Oversight Body pursuant to Article 37 to a critical ICT third-party service provider;***	
Article 25, first paragraph, first subparagraph, point (8)(b)			
438	(b) circumstances identified throughout the monitoring of ICT third-party risk which are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;	(b) circumstances identified throughout the monitoring of ICT third-party risk ~~*which*~~ ***that*** are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;	(b) circumstances identified throughout the monitoring of ICT third-party risk which are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;
Article 25, first paragraph, first subparagraph, point (8)(c)			
439	(c) ICT third-party service provider's evidenced weaknesses in its overall ICT risk management and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information;	(c) ICT third-party service provider's evidenced weaknesses ~~*in its*~~ ***pertaining to the*** overall ICT risk management ***of its contract with the financial entity*** and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information;	(c) ICT third-party service provider's evidenced weaknesses in its overall ICT risk management and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information;

	Commission Proposal	EP Mandate	Council Mandate
Article 25, first paragraph, first subparagraph, point (8)(d)			
440	(d) circumstances where the competent authority can no longer effectively supervise the financial entity as a result of the respective contractual arrangement.	(d) circumstances where the competent authority ***demonstrably*** can no longer effectively supervise the financial entity as a result of the respective contractual arrangement.	(d) circumstances where the competent authority can no longer effectively supervise the financial entity as a result of the respective contractual arrangement.
Article 25, first paragraph, first subparagraph, point (8a), introductory part			
440a		***(8a) With a view to reducing the risk of disruptions at the level of the financial entity, in duly justified circumstances and in agreement with its competent authorities, the financial entity may decide not to terminate the contractual arrangements with the ICT third-party service provider until it is able to switch to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided, in accordance with the exit strategy referred to in paragraph 9.***	
Article 25, first paragraph, first subparagraph, point (8a), first paragraph			
440b		***8b. In cases where contractual arrangements with ICT third-party service providers are terminated under any of the circumstances listed in paragraph 8, points (a) to (d),***	

	Commission Proposal	EP Mandate	Council Mandate
		financial entities shall not bear the cost of transferring out data from an ICT third-party service provider where such transfer exceeds the cost of transferring out data provided for in the initial contract.	
Article 25, first paragraph, first subparagraph, point (9), introductory part			
441	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. ***For ICT services related to critical or important functions,*** financial entities shall put in place exit strategies***, to be reviewed periodically. The exit strategies shall*** ~~*in order*~~ to take into account risks that may emerge at the level of ICT third-party service ~~*provider*~~***providers***, in particular a possible failure of the latter, a deterioration of the quality of the functions provided, any business disruption due to inappropriate or failed provision of services or material risk arising in relation to the appropriate and continuous deployment of the function~~.~~***, or in the event of termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 8, points (a) to (d).***	9. **For the use of ICT services concerning critical or important functions,** financial entities shall put in place exit strategies in order to take into account risks that may emerge at the level of ICT third-party service provider, in particular a possible failure of the latter, a deterioration of the quality of the functions provided, any business disruption due to inappropriate or failed provision of services or material risk arising in relation to the appropriate and continuous deployment of the function.
Article 25, first paragraph, first subparagraph, point (9), first paragraph, introductory part			
442	Financial entities shall ensure that they are able to exit contractual arrangements without:	Financial entities shall ensure that they are able to exit contractual arrangements without:	Financial entities shall ensure that they are able to exit contractual arrangements without:

	Commission Proposal	EP Mandate	Council Mandate
Article 25, first paragraph, first subparagraph, point (9), first paragraph(a)			
443	(a) disruption to their business activities,	(a) disruption to their business activities,	(a) **unreasonable** disruption to their business activities,
Article 25, first paragraph, first subparagraph, point (9), first paragraph(b)			
444	(b) limiting compliance with regulatory requirements,	(b) limiting compliance with regulatory requirements,	(b) limiting compliance with regulatory requirements,
Article 25, first paragraph, first subparagraph, point (9), first paragraph(c)			
445	(c) detriment to the continuity and quality of their provision of services to clients.	(c) detriment to the continuity and quality of their provision of services to clients.	(c) detriment to the continuity and quality of their provision of services to clients.
Article 25, first paragraph, first subparagraph, point (9), second paragraph			
446	Exit plans shall be comprehensive, documented and, where appropriate, sufficiently tested.	Exit plans shall be comprehensive, documented and, where appropriate, sufficiently tested.	Exit plans shall be comprehensive, documented and **in accordance with the size, nature, scale, complexity and overall risk profile of the financial entity**~~, where appropriate~~, sufficiently tested **and reviewed periodically**.
Article 25, first paragraph, first subparagraph, point (9), third paragraph			
447	Financial entities shall identify alternative	Financial entities shall identify alternative	Financial entities shall identify alternative

	Commission Proposal	EP Mandate	Council Mandate
	solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service provider and securely and integrally transfer them to alternative providers or reincorporate them in-house.	solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service provider and securely and integrally transfer them to alternative providers or reincorporate them in-house.	solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service provider and securely and integrally transfer them to alternative providers or reincorporate them in-house.
Article 25, first paragraph, first subparagraph, point (9), fourth paragraph			
448	Financial entities shall take appropriate contingency measures to maintain business continuity under all of the circumstances referred to in the first subparagraph.	Financial entities shall take appropriate contingency measures to maintain business continuity under all of the circumstances referred to in the first subparagraph.	Financial entities shall take appropriate contingency measures to maintain business continuity under all of the circumstances referred to in the first subparagraph.
Article 25, first paragraph, first subparagraph, point (10)			
449	10. The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the Register of Information referred to in paragraph 4. The ESAs shall submit those draft implementing technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force of this Regulation]. Power is conferred on the Commission to adopt the	10. The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the Register of Information referred to in paragraph 4. The ESAs shall submit those draft implementing technical standards to the Commission by [OJ: insert date 1 year after the date of entry into force of this Regulation]. Power is conferred on the Commission to adopt the	10. The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information referred to in paragraph 4**, including:** **(i) information that is common to all contractual arrangements on the use of ICT services;** **(ii) further details in relation to contractual arrangements on the use of ICT services concerning critical or important functions**.

	Commission Proposal	EP Mandate	Council Mandate
	implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	——————————— The ESAs shall submit those draft implementing technical standards to the Commission by [OJ: insert date ~~1 year~~**18 months** after the date of entry into force of this Regulation]. ——————————— ———————————Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
Article 25, first paragraph, first subparagraph, point (11), introductory part			
450	11. The ESAs shall, through the Joint Committee, develop draft regulatory standards:	11. The ESAs shall, through the Joint Committee, develop draft regulatory standards:	11. The ESAs shall, through the Joint Committee, develop draft regulatory **technical** standards~~:~~ **to further specify the detailed content of the policy referred to in paragraph 3 in relation to the contractual arrangements on the use of ICT services concerning critical or important functions, provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services;**
Article 25, first paragraph, first subparagraph, point (11)(a)			

	Commission Proposal	EP Mandate	Council Mandate
451	(a) to further specify the detailed content of the policy referred to in paragraph 3 in relation to the contractual arrangements on the use of ICT services provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services;	(a) to further specify the detailed content of the policy referred to in paragraph 3 in relation to the contractual arrangements on the use of ICT services provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services;	~~(a) to further specify the detailed content of the policy referred to in paragraph 3 in relation to the contractual arrangements on the use of ICT services provided by ICT third-party service providers, by reference to the main phases of the lifecycle of the respective arrangements on the use of ICT services;~~
Article 25, first paragraph, first subparagraph, point (11)(b)			
452	(b) the types of information to be included in the Register of Information referred to in paragraph 4.	(b) the types of information to be included in the Register of Information referred to in paragraph 4.	(b) ~~the types of information to be included in the Register of Information referred to in paragraph 4.~~
Article 25, first paragraph, first subparagraph a			
452a			**When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities.**
Article 25, first paragraph, second subparagraph			
453	The ESAs shall submit those draft regulatory technical standards to the Commission by [PO: insert date 1 year after the date of entry into force].	The ESAs shall submit those draft regulatory technical standards to the Commission by [PO: insert date ~~*1 year*~~***18 months*** after the date of entry into force].	The ESAs shall submit those draft regulatory technical standards to the Commission by [PO: insert date ~~1 year~~**18 months** after the date of entry into force].
Article 25, first paragraph, third subparagraph			

	Commission Proposal	EP Mandate	Council Mandate
454	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the second subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
Article 26			
455	Article 26 Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements	Article 26 Preliminary assessment of ICT concentration risk and further ~~*sub-outsourcing*~~ ***sub-contracting*** arrangements	Article 26 Preliminary assessment of ICT ~~concentration~~**related** risk and further ~~sub-outsourcing~~**subcontracting** arrangements **with regard to concentration risk.**
Article 26(1), first subparagraph, introductory part			
456	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*~~ ICT services ***supporting critical or important functions*** 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~~**on the use of** ICT services **concerning critical or important functions** would lead to any of the following:
Article 26(1), first subparagraph, point (a)			
457	(a) contracting with an ICT third-party service provider which is not easily substitutable; or	(a) contracting with an ICT third-party service provider ~~*which*~~***that*** is not easily substitutable; or	(a) contracting with an ICT third-party service provider which is not easily substitutable; or

	Commission Proposal	EP Mandate	Council Mandate
Article 26(1), first subparagraph, point (b)			
458	(b) having in place multiple contractual arrangements in relation to the provision of ICT services with the same ICT third-party service provider or with closely connected ICT third-party service providers.	(b) having in place multiple contractual arrangements in relation to the provision of ICT services ***supporting critical or important functions*** with the same ICT third-party service provider or with closely connected ICT third-party service providers.	(b) having in place multiple contractual arrangements ~~in relation to the provision~~**on the use** of ICT services **concerning critical or important functions** with the same ICT third-party service provider or with closely connected ICT third-party service providers.
Article 26(1), second subparagraph			
459	Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.	Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.	Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy.
Article 26(2), first subparagraph			
460	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 ***supporting critical or important functions*** includes the possibility that an ICT third-party service provider further sub-contracts a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such possible sub-contracting~~, *in particular in the case of an ICT sub-contractor established in a third-*~~	2. Where the contractual arrangement on the use of ICT services **concerning critical or important functions** includes the possibility that an ICT third-party service provider further ~~sub-contracts~~**subcontracts** a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such possible ~~sub-contracting~~**sub-contracting**, in particular in the case of an ICT

	Commission Proposal	EP Mandate	Council Mandate
		~~*country*~~.	~~sub-contractors~~**subcontractor** established in a third-country.
Article 26(2), second subparagraph, introductory part			
461	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 ***supporting critical or important functions*** 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 **concerning critical or important functions** are concluded with an ICT third-party service provider established in a third-country, financial entities shall ~~consider relevant, at least~~**as a minimum consider** the following **as relevant** factors:
Article 26(2), second subparagraph, point (a)			
462	(a) the respect of data protection;	(a) ~~*the respect of data protection;*~~	(a) the respect of data protection;
Article 26(2), second subparagraph, point (b)			
463	(b) the effective enforcement of the law;	(b) ~~*the effective enforcement of the law;*~~	(b) the effective– enforcement of the law;
Article 26(2), second subparagraph, point (c)			
464	(c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy;	(c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy; ***and***	(c) insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy;
Article 26(2), second subparagraph, point (d)			
465	(d) any constraints that may arise in respect to the urgent recovery of the financial entity's	(d) any constraints that may arise in respect to the urgent recovery of the financial entity's	(d) any ~~constraints~~**constraint** that may arise in respect to the urgent recovery of the financial

	Commission Proposal	EP Mandate	Council Mandate
	data.	data.	entity's data.
Article 26(2), second subparagraph a, introductory part			
465a		***Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third country, financial entities shall, in addition to the considerations referred to in the first and second subparagraphs, also consider:***	
Article 26(2), second subparagraph a, point (a)			
465b		***(i) the respect of Union data protection rules; and,***	
Article 26(2), second subparagraph a, point (b)			
465c		***(ii) the effective enforcement of the rules laid down in this Regulation.***	
Article 26(2), third subparagraph			
466	Financial entities shall assess whether and how potentially long or complex chains of sub-contracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.	***Where such contractual arrangements 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 the second and third subparagraphs to*** monitor the contracted functions and the ability of the competent	Financial entities shall assess whether and how potentially long or complex chains of ~~sub-contracting~~**subcontracting** may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

	Commission Proposal	EP Mandate	Council Mandate
		authority to effectively supervise the financial entity in that respect.	
Article 27			
467	Article 27 Key contractual provisions	Article 27 Key contractual provisions	Article 27 Key contractual provisions
Article 27(1)			
468	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 in ~~*one written document*~~***writing and be*** 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~~**shall include the service** level agreements, shall be documented in one written document available to the parties on paper**,** or in a **document with another** downloadable**, durable** and accessible format.
Article 27(2), introductory part			
469	2. The contractual arrangements on the use of ICT services shall include at least the following:	2. ~~*The*~~***Financial entities and ICT third-party service providers shall ensure that*** contractual arrangements on the use of ICT services shall include at least the following:	2. The contractual arrangements on the use of ICT services **concerning critical or important functions** shall include at least the following:
Article 27(2), point (a)			
470	(a) a clear and complete description of all functions and services to be provided by the ICT third-party service provider, indicating	(a) a clear and complete description of all functions and services to be provided by the ICT third-party service provider, indicating	(a) a clear and complete description of all functions and **ICT** services to be provided by the ICT third-party service provider, indicating

	Commission Proposal	EP Mandate	Council Mandate
	whether sub-contracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting;	whether sub-contracting of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such sub-contracting;	whether ~~sub-contracting~~**subcontracting** of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applying to such ~~sub-contracting~~**subcontracting**;
Article 27(2), point (b)			
471	(b) the locations where the contracted or sub-contracted functions and services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity if it envisages changing such locations;	(b) the locations***, namely the regions or countries,*** where the contracted or sub-contracted ***ICT*** functions and services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify ***in advance*** the financial entity if it envisages changing such locations;	(b) the ~~locations~~**location(s), namely the regions or countries,** where the contracted or ~~sub-contracted~~**subcontracted** functions and **ICT** services are to be provided and where **the** data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity if it envisages changing such ~~locations~~**location(s)**;
Article 27(2), point (c)			
472	(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;	(c) provisions on accessibility, availability, integrity, security***, confidentiality*** and protection of ~~*personal data and on ensuring access, recover and return in an easily accessible format of*~~***data, including*** 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*~~***data***;	(c) provisions on accessibility, availability, integrity, ~~security~~**confidentiality** and protection of **data including** personal data and on ensuring access, recover and return in an easily accessible format of ~~personal and non-personal~~ data processed by the financial entity in the case of insolvency, resolution or discontinuation of the business ~~operations~~ of the ICT third-party service provider;
Article 27(2), point (ca)			

	Commission Proposal	EP Mandate	Council Mandate
472a		***(ca) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the case of termination of the contractual arrangements;***	
Article 27(2), point (d)			
473	(d) full service level descriptions, including updates and revisions thereof, and precise quantitative and qualitative performance targets within the agreed service levels to allow an effective monitoring by the financial entity and enable without undue delay appropriate corrective actions when agreed service levels are not met;	(d) full service level descriptions, including updates and revisions thereof, and precise quantitative and qualitative performance targets within the agreed service levels to allow an effective monitoring by the financial entity and enable without undue delay appropriate corrective actions when agreed service levels are not met;	(d) full service level descriptions, including updates and revisions thereof, and precise quantitative and qualitative performance targets within the agreed service levels to allow an effective monitoring by the financial entity and enable without undue delay appropriate corrective actions **to be taken** when agreed service levels are not met;
Article 27(2), point (e)			
474	(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;	(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;*~~	(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 **the** agreed service levels;
Article 27(2), point (f)			

	Commission Proposal	EP Mandate	Council Mandate
475	(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;	(f) the obligation of the ICT third-party service provider to provide assistance in case of an ~~ICT~~**ICT-related** incident **that affects or connects to the ICT service they provide** at no additional cost or at a cost that is determined ex-ante;
Article 27(2), point (g)			
476	(g) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies which adequately guarantee a secure provision of services by the financial entity in line with its regulatory framework;	(g) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies ~~*which adequately guarantee a*~~***that provide an appropriate level of*** secure provision of services by the financial entity in line with its regulatory framework;	(g) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies which adequately guarantee a secure provision of services by the financial entity in line with its regulatory framework;
Article 27(2), point (h), introductory part			
477	(h) the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:	(h) ~~*the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:*~~	(h) the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:
Article 27(2), point (h)(i)			
478	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	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*~~	i) **unrestricted** rights of access, inspection and audit **by the competent authority,** by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which

	Commission Proposal	EP Mandate	Council Mandate
	arrangements or implementation policies;	~~*arrangements or implementation policies;*~~	is not impeded or limited by other contractual arrangements or implementation policies;
Article 27(2), point (h)(ii)			
479	ii) the right to agree alternative assurance levels if other clients' rights are affected;	ii) ~~*the right to agree alternative assurance levels if other clients' rights are affected;*~~	ii) the right to agree alternative assurance levels if other clients' rights **of the ICT third-party service provider** are affected;
Article 27(2), point (h)(iii)			
480	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;	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;*~~	iii) the commitment to fully cooperate during the ~~onsite~~ inspections **and audits** performed by the **competent authority, by the** financial entity **or by an appointed third-party** and details on the scope, modalities and frequency of ~~remote~~**such inspections and** audits;
Article 27(2), point (i)			
481	(i) the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them;	(i) the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them;	(i) the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them;
Article 27(2), point (j)			
482	(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities' expectations;	(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent ***and resolution*** authorities' expectations ***and, where***	(j) termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities' expectations;

	Commission Proposal	EP Mandate	Council Mandate
		that contractual arrangement impacts an ICT intra-group service provider within the same group, an analysis following a risk-based approach;	
Article 27(2), point (k), introductory part			
483	(k) exit strategies, in particular the establishment of a mandatory adequate transition period:	(k) exit strategies, in particular the establishment of a mandatory adequate transition period:	(k) exit strategies, in particular the establishment of a mandatory adequate transition period:
Article 27(2), point (k)(i)			
484	(i) during which the ICT third-party service provider will continue providing the respective functions or services with a view to reduce the risk of disruptions at the financial entity;	(i) during which the ICT third-party service provider will continue providing the respective functions or services with a view to reduce the risk of disruptions at the financial entity ***or to ensure its effective resolution and restructuring***;	(i) during which the ICT third-party service provider will continue providing the respective functions or **ICT** services with a view to reduce the risk of disruptions at the financial entity;
Article 27(2), point (k)(ii)			
485	(ii) which allows the financial entity to switch to another ICT third-party service provider or change to on-premises solutions consistent with the complexity of the provided service.	(ii) which allows the financial entity to switch to another ICT third-party service provider or change to on-premises solutions consistent with the complexity of the provided service~~.~~**;**	(ii) which allows the financial entity to ~~switch~~**migrate** to another ICT third-party service provider or change to ~~on-premises~~**in-house** solutions consistent with the complexity of the provided service.
Article 27(2), point (k)(IIa)			
485a		***(iia) where that contractual arrangement impacts an ICT intra-group service provider***	

	Commission Proposal	EP Mandate	Council Mandate
		within the same group, it shall be analysed following a risk-based approach;	
Article 27(2), point (l)			
485b			**(l) the obligation of the ICT-third party service provider to participate and fully cooperate in a threat led penetration test of the financial entity as referred to in Article 23;**
Article 27(2), point (ka)			
485c		***(ka) a provision on the processing of personal data by the ICT-third party service provider which is to be in conformity with Regulation (EU) 2016/679;***	
Article 27(2), point (m)			
485d			**(m) the obligation for the critical ICT-third party service provider to inform, without undue delay, the financial entity of the content of the recommendation referred to in Article 31(1)(d), in order to allow the financial entity to comply with the obligation set forth in Article 37(2).**
Article 27(2a), introductory part			
485e		***2a. The contractual arrangements for the provision of critical or important functions***	

	Commission Proposal	EP Mandate	Council Mandate
		shall, in addition to paragraph 2, include at least the following:	
Article 27(2a), point (a)			
485f		***(a) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively carry out critical or important functions in line with agreed service levels;***	
Article 27(2a), point (b), introductory part			
485g		***(b) the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:***	
Article 27(2a), point (b)(1)			
485h		***(i) rights of access, inspection and audit by the financial entity or by an appointed third party, and the right to review copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;***	
Article 27(2a), point (b)(2)			

	Commission Proposal	EP Mandate	Council Mandate
485i		***(ii) the right to agree on alternative assurance levels if other clients' rights are affected;***	
Article 27(2a), point (b)(3)			
485j		***(iii) the commitment by the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, lead overseer, financial entity or an appointed third party, and details on the scope, modalities and frequency of such inspections and audits;***	
Article 27(2a), point (c)			
485k		***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.***	
Article 27(2b), introductory part			
485l		***2b. The contractual arrangements for the provision of ICT services by an ICT third-party service provider established in a third country***	

	Commission Proposal	EP Mandate	Council Mandate
		and designated as critical pursuant to Article 28(9), shall, in addition to paragraphs 2 and 2a of this Article:	
Article 27(2b), point (a)			
485m		***(a) stipulate that the contract is governed by the law of a Member State; and***	
Article 27(2b), point (b)			
485n		***(b) guarantee that the Joint Oversight Body and Lead Overseer can carry out their duties specified in Article 30 on the basis of their competences set out in Article 31.***	
Article 27(2b), point (c)			
485o		***The services for which the contractual arrangements are concluded shall not be required to be performed by the undertaking constituted in the Union under the law of a Member State.***	
Article 27(3)			
486	3. When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed for specific services.	3. When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed for specific services.	3. ~~When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed for specific services.~~

	Commission Proposal	EP Mandate	Council Mandate
Article 27(3a)			
486a		***3a. Competent authorities shall be able to access the contractual arrangements referred to in this Article. The parties to those contractual arrangements may agree to redact commercially sensitive or confidential information prior to granting such access to the competent authorities, subject to the latter being fully informed as to the extent and nature of the redactions.***	
Article 27(4), first subparagraph			
487	4. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when sub-contracting critical or important functions to properly give effect to the provisions of point (a) of paragraph 2.	4. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when sub-contracting critical or important functions to properly give effect to the provisions of point (a) of paragraph 2. ***When developing those draft regulatory technical standards, the ESAs shall take into consideration the size of financial entities, the nature, scale and complexity of their services, activities and operations, and their overall risk profile.***	4. The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when ~~sub-contracting~~**subcontracting** critical or important functions to properly give effect to the provisions of point (a) of paragraph 2.
Article 27(4), first subparagraph a			
487a			**When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity**

	Commission Proposal	EP Mandate	Council Mandate
			and overall risk profile of the financial entities.
Article 27(4), second subparagraph			
488	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].	The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date ~~*1 year*~~ ***18 months*** after the date of entry into force].	The ESAs shall submit those draft regulatory technical standards to the Commission by [OJ: insert date ~~1 year~~**18 months** after the date of entry into force].
Article 27(4), third subparagraph			
489	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively.
SECTION II			
490	SECTION II Oversight framework of critical ICT third-party service providers	SECTION II Oversight framework of critical ICT third-party service providers	SECTION II ~~Oversight framework of critical ICT third-party service providers~~ **OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS**
Article 28			
491	Article 28 Designation of critical ICT third-party service	Article 28 Designation of critical ICT third-party service	Article 28 Designation of critical ICT third-party service

	Commission Proposal	EP Mandate	Council Mandate
	providers	providers	providers
Article 28(1), introductory part			
492	1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall:	1. The ESAs, through the Joint Committee and upon recommendation from the ***Joint*** Oversight ~~*Forum*~~***Body*** established pursuant ~~*to*~~ ***to*** Article 29(1)**, *after consultation with ENISA,*** shall:	1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant ~~to~~ **to** Article 29(1) shall:
Article 28(1), point (a)			
493	(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;	(a) designate the ICT third-party service providers that are critical for financial entities, taking into account the criteria specified in paragraph 2;
Article 28(1), point (b)			
494	(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	(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	(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~~**which of these three authorities is responsible, in accordance with** Regulations (EU) No 1093/2010 (EU), No 1094/2010 or (EU) No 1095/2010~~respectively, represents more than a half of~~ **, for the financial entities having together the largest share of total assets, from** the value of ~~the~~ total assets of all financial entities making use of the services of

	Commission Proposal	EP Mandate	Council Mandate
	consolidated, of those financial entities.	consolidated, of those financial entities.	the **relevant** critical ICT third-party service provider, as evidenced by the ~~consolidated balance sheets, or~~**sum of** the individual balance sheets ~~where balance sheets are not consolidated,~~ of those financial entities.
Article 28(1a)			
494a		***The Lead Overseer appointed in accordance with point (b) of the first subparagraph shall be responsible for the daily oversight of the critical ICT third-party service provider.***	
Article 28(2), introductory part			
495	2. The designation referred to in point (a) of paragraph 1 shall be based on all of the following criteria:	2. The designation referred to in point (a) of paragraph 1 shall be based on all of the following criteria:	2. The designation referred to in ~~point (a) of~~ paragraph 1 shall be based on all of the following criteria **in relation to ICT services provided by an ICT third-party service provider**:
Article 28(2), point (a)			
496	(a) the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant ICT third-party provider would face a large scale operational failure to provide its services, taking into account the number of financial entities to which the relevant ICT third-party service provider provides services;	(a) the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant ICT third-party provider would face a large scale operational failure to provide its services, taking into account the number of financial entities to which the relevant ICT third-party service provider provides services;	(a) the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant ICT third-party provider would face a large scale operational failure to provide its services, taking into account the number of financial entities **and the total value of assets of financial entities** to which the relevant ICT third-party service provider provides services;

	Commission Proposal	EP Mandate	Council Mandate
Article 28(2), point (b), introductory part			
497	(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the following parameters:	(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the following parameters:	(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the following parameters:
Article 28(2), point (b)(i)			
498	i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;	i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;	i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;
Article 28(2), point (b)(ii)			
499	ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;	ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;	ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;
Article 28(2), point (c)			
500	(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly	(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly	(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities **as defined in point (17) of Article 3** that ultimately involve the same ICT third-party service provider, irrespective of whether

	Commission Proposal	EP Mandate	Council Mandate
	or indirectly, by means or through subcontracting arrangements;	or indirectly, by means or through subcontracting arrangements;	financial entities rely on those services directly or indirectly, by means or through subcontracting arrangements;
Article 28(2), point (d), introductory part			
501	(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:	(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:	(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:
Article 28(2), point (d)(i)			
502	i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;	i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;	i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;
Article 28(2), point (d)(ii)			
503	ii) difficulties to partially or fully migrate the relevant data and workloads from the relevant to another ICT third-party service provider, due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration.	ii) difficulties to partially or fully migrate the relevant data and workloads from the relevant to another ICT third-party service provider, due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration.	ii) difficulties to partially or fully migrate the relevant data and workloads from the relevant to another ICT third-party service provider, due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration.

	Commission Proposal	EP Mandate	Council Mandate
Article 28(2), point (e)			
504	(e) the number of Member States in which the relevant ICT third-party service provider provides services;	(e) the number of Member States in which the relevant ICT third-party service provider provides services;	(e) ~~the number of Member States in which the relevant ICT third-party service provider provides services;~~
Article 28(2), point (f)			
505	(f) the number of Member States in which financial entities using the relevant ICT third-party service provider are operating.	(f) the number of Member States in which financial entities using the relevant ICT third-party service provider are operating.	(f) ~~the number of Member States in which financial entities using the relevant ICT third-party service provider are operating.~~
Article 28(2), point (fa)			
505a		***(fa) the materiality and importance of the services provided by the relevant ICT third-party service provider.***	
Article 28(2a)			
505b			**2a. Where the ICT third-party service provider belongs to a group, the criteria referred to in paragraph 2 shall be considered in relation to the ICT service provided by the group as a whole.**
Article 28(2b)			
505c			**2b. Critical ICT third-party service providers which are part of a group shall**

	Commission Proposal	EP Mandate	Council Mandate
			designate one legal person as coordination point to ensure adequate representation and communication with the Lead Overseer.
Article 28(2a)			
505d		***2a. The Joint Oversight Body shall notify the ICT third-party service provider before initiating its assessment for the purposes of the designation referred to paragraph 1, point (a).***	**5a. The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment referred in paragraph 2.** **Within 60 calendar days from the date of the notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement on the assessment which shall contain all relevant additional information which may be deemed appropriate by the ICT third-party service provider to support the completeness and accuracy of the designation procedure.** **Before taking a decision on designation pursuant to paragraph 1, the Lead Overseer shall take due consideration of the reasoned statement and may request the ICT third-party service provider to submit further information which may be needed within 30 calendar days.**
Article 28(2b)			
505e		***The Joint Oversight Body shall notify the ICT third-party service provider of the outcome of the assessment referred to in the first***	

	Commission Proposal	EP Mandate	Council Mandate
		subparagraph by providing a draft recommendation of criticality. Within 6 weeks from the date of receipt of that draft recommendation, the ICT third-party service provider may submit to the Joint Oversight Body a reasoned statement on the assessment. That reasoned statement shall contain all relevant additional information deemed to be appropriate by the ICT third-party service provider in order to support the completeness and accuracy of the designation procedure or to challenge the draft recommendation of criticality. The Joint Committee of the ESAs shall take due consideration of the reasoned statement and may request further information or evidence from the ICT third-party service provider prior to taking a decision on designation.	
Article 28(2c)			
505f		***The Joint Committee of the ESAs shall notify the ICT third-party service provider of its designation as critical. The ICT third-party service provider shall have at least three months, from the date of receipt of the notification, to make any necessary adjustments to allow the Joint Oversight Body to carry out its duties pursuant to Article 30, as well as to notify the financial entities to which the ICT third-party service provider provides services. The Joint Oversight Body may allow the adjustment period to be extended for a maximum period of three months if requested,***	

	Commission Proposal	EP Mandate	Council Mandate
		and duly justified, by the designated ICT third-party service provider.	
Article 28(3)			
506	3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement the criteria referred to in paragraph 2.	3. The Commission is empowered to adopt ***a*** delegated ~~*acts*~~***act*** in accordance with Article 50 to ~~*supplement*~~ ***specify further*** the criteria referred to in paragraph 2.	3. The Commission ~~is empowered to~~**shall** adopt **a** delegated ~~acts~~**act** in accordance with Article 50 to ~~supplement~~**further specify** the criteria referred to in paragraph 2 **and in point (iii) of paragraph 5, by [OJ: insert date 12 months after the date of entry into force]**.
Article 28(4)			
507	4. The designation mechanism referred to in point (a) of paragraph 1 shall not be used until the Commission has adopted a delegated act in accordance with paragraph 3.	4. The designation mechanism referred to in point (a) of paragraph 1 shall not be used until the Commission has adopted a delegated act in accordance with paragraph 3.	4. The designation mechanism referred to ~~in point (a) of~~ paragraph 1 shall not be used until the Commission has adopted a delegated act in accordance with paragraph 3.
Article 28(5)			
508	5. The designation mechanism referred to in point (a) of paragraph 1 shall not apply in relation to ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union.	5. The designation mechanism referred to in point (a) of paragraph 1 shall not apply in relation to ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union.	5. The designation mechanism referred to in point (a) of paragraph 1 shall not apply in relation to**:** **(i) financial entities providing ICT services to other financial entities;** **(ii) ICT** ~~ICT~~ third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty

	Commission Proposal	EP Mandate	Council Mandate
			on the Functioning of the European Union**, and** **(iii) ICT third-party service providers that are part of a financial group and provide services predominantly to their parent undertaking, subsidiaries and branches of its parent undertaking.** **(iv) ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State**.
Article 28(6)			
509	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 ~~*ESAs, through the Joint Committee*~~***Joint Oversight Body, in consultation with ENISA***, shall establish, publish and ~~*yearly*~~ ***regularly*** update the list of critical ICT third-party service providers at Union level.	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.
Article 28(7)			
510	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 ~~*Forum*~~ ***Body*** established pursuant to Article 29. The ~~*Oversight Forum*~~ ***Joint Oversight Body*** 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)~~**register of information,** 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.

	Commission Proposal	EP Mandate	Council Mandate
Article 28(8), first subparagraph			
511	8. ICT third-party service providers that are not included in the list referred to in paragraph 6 may request to be included in that list.	8. ***The*** ICT third-party service providers that are not included in the list referred to in paragraph 6 may request to be included in that list.	8. ICT third-party service providers that are not included in the list referred to in paragraph 6 may request to be included in that list.
Article 28(8), second subparagraph			
512	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 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 ~~EBA, ESMA or EIOPA~~**the Lead Overseer**, 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.
Article 28(8), third subparagraph			
513	The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.	The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.	The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.
Article 28(8a), first subparagraph			
513a		***8a. The Joint Committee of the ESAs, upon recommendation from the Joint Oversight Body, shall designate the ICT third-party service providers established in a third country that are critical for financial entities in***	

	Commission Proposal	EP Mandate	Council Mandate
		accordance with paragraph 1, point (a).	
Article 28(8a), second subparagraph			
513b		***In making the designation referred to in the first subparagraph of this paragraph, the ESAs and the Joint Oversight Body shall follow the procedural steps set out in paragraph 2a.***	
Article 28(9)			
514	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~~***a critical*** ICT third-party service provider established in a third country ***unless that ICT third-party service provider has an undertaking constituted in the Union under the law of a Member State and has concluded contractual arrangements in accordance with Article 27(2b)*** ~~*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~~**refrain from using** 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~~**that did not establish a subsidiary** in the Union **within 12 months following the designation**.
Article 29			
515	Article 29 Structure of the Oversight Framework	Article 29 Structure of the Oversight Framework	Article 29 Structure of the Oversight Framework
Article 29(1), first subparagraph			
516	1. The Joint Committee, in accordance with Article 57 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010,	1. The Joint ~~*Committee, in accordance with Article 57 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010,*~~	1. The Joint Committee, in accordance with Article 57 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010,

	Commission Proposal	EP Mandate	Council Mandate
	shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and the Lead Overseer referred to in point (b) of Article 28(1) in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and common acts of the Joint Committee in that area.	~~*shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work*~~***Oversight Body shall be established for the purposes of overseeing ICT third-party risk across financial sectors and conducting direct oversight of ICT third-party service providers designated as critical pursuant to Article 28.*** ***The role*** of the Joint ~~*Committee and the Lead Overseer referred to in point (b) of Article 28(1) in the area of ICT third-party risk across*~~***Oversight Body shall be limited to oversight powers related to ICT risks concerning the ICT services provided to*** financial ~~*sectors. The Oversight Forum shall prepare the draft joint positions and common acts of the Joint Committee in that area*~~***entities by critical ICT third-party service providers***.	shall establish the Oversight Forum as a sub-committee for the purposes of supporting the work of the Joint Committee and the Lead Overseer ~~referred to in point (b) of Article 28(1)~~ in the area of ICT third-party risk across financial sectors. The Oversight Forum shall prepare the draft joint positions and common acts of the Joint Committee in that area.
Article 29(1), second subparagraph			
517	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 ~~*Forum*~~***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.	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.
Article 29(2)			
518	2. The Oversight Forum shall on a yearly basis undertake a collective assessment of the results and findings of Oversight activities conducted	2. The ***Joint*** Oversight ~~*Forum*~~***Body*** shall on a yearly basis undertake a collective assessment of the results and findings of ***the*** Oversight	2. The Oversight Forum shall on a yearly basis undertake a collective assessment of the results and findings of Oversight activities conducted

	Commission Proposal	EP Mandate	Council Mandate
	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.	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.	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.
Article 29(3)			
519	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 ~~*Forum*~~***Body*** shall submit comprehensive benchmarks of critical ICT third-party service providers to be adopted by the Joint Committee as joint positions of the ESAs in accordance with Articles 56(1) of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	~~3.~~ The Oversight Forum shall 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.
Article 29(4)			
520	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~~***3***. The ***Joint*** Oversight ~~*Forum*~~***Body*** shall be composed of the ~~*Chairpersons*~~ ***Executive Directors*** 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*~~***ESAs and one high-level representative from at least eight of the national competent authorities.*** One representative from the European Commission, from the ESRB, from ECB and from ENISA***, and at least one independent expert appointed in accordance with paragraph 3a of this Article shall***	4**3**. The Oversight Forum shall be composed of **:** **(a)** the Chairpersons of the ESAs, ~~and~~ **who shall be voting members;** **(b)** one high-level representative from the current staff of the relevant competent authority **referred to in Article 41** from each Member State~~.~~**, who shall be voting members;** **(c)** the Executive Directors of each ESA and one representative from the European

	Commission Proposal	EP Mandate	Council Mandate
		participate ~~*shall participate in the Oversight Forum*~~ as observers.	Commission, from the ESRB, from ECB and from ENISA**, who** shall ~~participate in the Oversight Forum as~~**be non-voting observers;** **(d) where appropriate, one representative per Member State of a national competent authority referred to in Article 41, who shall be non-voting observers;** **(e) where applicable, one representative of the national competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or a digital service provider listed in Annex III of that Directive, respectively, which has been designated as a critical ICT third-party service provider, who shall be non-voting** observers.
Article 29(4a), introductory part			
520a		***Following the annual designation of critical ICT third-party service providers, pursuant to point (a) of Article 28(1), the Joint Committee of the ESAs shall decide which national competent authorities shall be members of the Joint Oversight Body, taking into account the following factors:***	
Article 29(4a), point (a)			
520b			

	Commission Proposal	EP Mandate	Council Mandate
		(a) the number of critical ICT third-party service providers established or providing services in the Member State;	
Article 29(4a), point (b)			
520c		***(b) the reliance of the financial entities in a Member State on critical ICT third-party service providers;***	
Article 29(4a), point (c)			
520d		***(c) the relative expertise of a national competent authority;***	
Article 29(4a), point (d)			
520e		***(d) the available resources and capacity of a national competent authority;***	
Article 29(4a), point (e)			
520f		***(e) the need for the operation and decision making of the Joint Oversight Body to be streamlined, lean, and efficient.***	
Article 29(4a)			
520g			**3a. Each Member State shall designate the relevant competent authority whose staff member shall be the high-level**

	Commission Proposal	EP Mandate	Council Mandate
			representative referred in point (b) of paragraph 3 to ensure the Member State representation in the Oversight Forum and shall inform the Lead Overseer thereof. **The Lead Overseer shall publish on its website the list of high-level representatives designated by Member States.**
Article 29(4b)			
520h		***The Joint Oversight Body shall share its documentation and decisions with all national competent authorities that are not members of the Joint Oversight Body.***	
Article 29(4c)			
520i		***The work of the Joint Oversight Body shall be supported and assisted by dedicated staff from across the ESAs.***	
Article 29(4d)			
520j		***3a. The independent expert referred to in paragraph 3 of this Article shall be appointed as an observer by the Joint Oversight Body following a public and transparent application process.***	
Article 29(4e)			
520k			

	Commission Proposal	EP Mandate	Council Mandate
		The independent expert shall be appointed on the basis of their expertise on financial stability, digital operational resilience and ICT security matters for a two year term.	
Article 29(4f)			
520l		***The appointed independent expert shall not hold any office at national, Union, or international level. The independent expert shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body.***	
Article 29(4g)			
520m		***The Joint Oversight Body may decide to appoint more than one independent expert observer.***	
Article 29(5)			
521	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	~~5~~***4***. In accordance with Article 16 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs shall issue guidelines ***by [OJ: insert date 18 months after the date of entry into force of this Regulation]*** on the cooperation between the ~~*ESAs*~~ ***Joint Oversight Body, the Lead Overseer*** and the	~~5~~**4**. In accordance with Article 16 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs shall **by [OJ: insert date 18 months after the date of entry into force]** issue guidelines on the cooperation between the ESAs and the competent authorities for the purposes of this Section on the detailed

	Commission Proposal	EP Mandate	Council Mandate
	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.	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*~~ ***Joint Oversight Body*** and details on exchanges of information needed by competent authorities to ensure the follow-up of recommendations addressed by ~~*Lead Overseers*~~***the Joint Oversight Body*** pursuant to point (d) of Article 31(1) to critical ICT third-party providers.	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~~**Overseer** pursuant to point (d) of Article 31(1) to critical ICT third-party providers.
Article 29(6)			
522	6. The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2016/1148 and of other Union rules on oversight applicable to providers of cloud computing services.	~~6~~***5***. The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2016/1148 and of other Union rules on oversight applicable to providers of cloud computing services.	~~6~~**5**. The requirements set out in this Section shall be without prejudice to the application of Directive (EU) 2016/1148 and of other Union rules on oversight applicable to providers of cloud computing services.
Article 29(7)			
523	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~~***6***. ~~*The ESAs, through*~~ The Joint ~~*Committee and based on preparatory work conducted by the*~~ Oversight ~~*Forum*~~***Body***, shall present yearly to the European Parliament, the Council and the Commission a report on the application of this Section.	~~7~~**6**. The ESAs, through the Joint Committee and based on preparatory work conducted by the Oversight Forum, shall present yearly to the European Parliament, the Council and the Commission a report on the application of this Section.
Article 30			
524	Article 30 Tasks of the Lead Overseer	Article 30 Tasks of the Lead Overseer	Article 30 Tasks of the Lead Overseer

	Commission Proposal	EP Mandate	Council Mandate
Article 30(1)			
525	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 Lead Overseer***, appointed under Article 28(1), point (b), shall lead and coordinate the daily oversight of critical ICT third-party service providers and shall be the primary point of contact for those critical ICT third-party service providers*** ~~*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 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.
Article 30(1a)			
525a		***1a. The Lead Overseer shall assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which it may pose to financial entities. That assessment shall primarily focus on the ICT services supporting critical or important functions provided by the critical ICT third-party service providers to financial entities, but may also be broader if relevant to the assessment of the risks to those functions.***	
Article 30(2), introductory part			
526			

	Commission Proposal	EP Mandate	Council Mandate
	2. The assessment referred to in paragraph 1 shall include:	2. The assessment referred to in paragraph ~~1~~ ***1a*** shall include:	2. The assessment referred to in paragraph 1 shall include:
Article 30(2), point (a)			
527	(a) ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of security, confidentiality and integrity of data;	(a) ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of security, confidentiality and integrity of data;	(a) ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of ~~security, confidentiality and integrity~~**confidentiality, integrity and availability** of data;
Article 30(2), point (b)			
528	(b) the physical security contributing to ensuring the ICT security, including the security of premises, facilities, datacentres;	(b) the physical security contributing to ensuring the ICT security, including the security of premises, facilities, datacentres;	(b) the physical security contributing to ensuring the ICT security, including the security of premises, facilities, datacentres;
Article 30(2), point (c)			
529	(c) the risk management processes, including ICT risk management policies, ICT business continuity and ICT disaster recovery plans;	(c) the risk management processes, including ICT risk management policies, ICT business continuity and ICT disaster recovery plans;	(c) the risk management processes, including ICT risk management policies, ICT business continuity and ICT disaster recovery plans;
Article 30(2), point (d)			
530	(d) the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling an effective ICT	(d) the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling an effective ICT	(d) the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling an effective ICT

	Commission Proposal	EP Mandate	Council Mandate
	risk management;	risk management;	risk management;
Article 30(2), point (e)			
531	(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;	(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;
Article 30(2), point (f)			
532	(f) the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities;	(f) the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities;	(f) the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities;
Article 30(2), point (g)			
533	(g) the testing of ICT systems, infrastructure and controls;	(g) the testing of ICT systems, infrastructure and controls;	(g) the testing of ICT systems, infrastructure and controls;
Article 30(2), point (h)			
534	(h) the ICT audits;	(h) the ICT audits;	(h) the ICT audits;
Article 30(2), point (i)			
535	(i) the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.	(i) the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.	(i) the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities.

	Commission Proposal	EP Mandate	Council Mandate
Article 30(3)			
536	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,~~ ***1a undertaken by*** the Lead Overseer, ***the Joint Oversight Body, under the coordination and direction of the Lead Overseer, shall draft and propose a clear, detailed and reasoned individual Oversight plan for each*** ~~*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 Lead Overseer shall adopt a clear, detailed and reasoned individual Oversight plan **describing the annual oversight objectives and the main oversight actions foreseen** for each critical ICT third-party service provider. That plan shall be communicated each year to the critical ICT third-party service provider.
Article 30(3a)			
536a		***When preparing the draft Oversight Plan, the Joint Oversight Body shall consult all relevant competent authorities and single points of contact referred to in Article 8 of Directive (EU) 2016/1148 to ensure that there are no inconsistencies or duplications with the obligations of the critical ICT third-party service provider under that Directive.***	
Article 30(3b)			
536b		***The Oversight plan shall be adopted on a yearly basis by the board of the Lead Overseer.***	
Article 30(3c)			

	Commission Proposal	EP Mandate	Council Mandate
536c		***Prior to adoption, the draft Oversight plan shall be communicated to the critical ICT third-party service provider.***	
Article 30(3d)			
536d		***Upon receipt of the draft Oversight Plan, the critical ICT third-party service provider shall have a period of six weeks within which to review and submit a reasoned statement on the draft Oversight plan. Such reasoned statement may be submitted only if the critical ICT third-party service provider is able to produce evidences that the execution of the Oversight Plan would generate 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. If such a statement is submitted, the critical ICT third-party service provider shall suggest to the Joint Oversight Body a more effective or efficient solution to achieve the objectives of the draft Oversight Plan.***	
Article 30(3e)			
536e		***Prior to adopting the Oversight Plan, the board of the Lead Overseer shall take due consideration of the reasoned statement and may request further information or evidence from the ICT third-party service provider.***	

	Commission Proposal	EP Mandate	Council Mandate
Article 30(4)			
537	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 ~~*agreed*~~***adopted*** and notified to the critical ICT third-party service providers, competent authorities may only take measures concerning critical ICT third-party service providers in agreement with the ~~*Lead Overseer*~~***Joint Oversight Body***.	4. Once the annual Oversight plans referred to in paragraph 3 have been ~~agreed~~**adopted by the Lead Overseer** and notified to the critical ICT third-party service providers, competent authorities may only take measures concerning critical ICT third-party service providers in agreement with the Lead Overseer.
Article 31			
538	Article 31 Powers of the Lead Overseer	Article 31 ~~*Powers of the Lead Overseer*~~***Oversight Powers***	Article 31 Powers of the Lead Overseer
Article 31(1), introductory part			
539	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 Lead Overseer shall have the following powers ***in respect of the services provided by critical ICT third-party service providers to financial entities***:	1. For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the following powers:
Article 31(1), point (a)			
540	(a) to request all relevant information and documentation in accordance with Article 32;	(a) to request all relevant information and documentation in accordance with Article 32;	(a) to request all relevant information and documentation in accordance with Article 32;
Article 31(1), point (b)			
541			

	Commission Proposal	EP Mandate	Council Mandate
	(b) to conduct general investigations and inspections in accordance with Articles 33 and 34;	(b) to conduct general investigations and ***on-site*** inspections in accordance with Articles 33 and 34;	(b) to conduct general investigations and inspections in accordance with Articles 33 and 34;
Article 31(1), point (c)			
542	(c) to request reports after the completion of the Oversight activities specifying the actions which have been taken or the remedies which have been implemented by the critical ICT third-party providers in relation to the recommendations referred to in point (d) of this paragraph;	(c) to request reports after the completion of the Oversight activities specifying the actions ~~*which*~~***that*** have been taken or the remedies ~~*which*~~ ***that*** have been implemented by the critical ICT third-party ***service*** providers in relation to the recommendations referred to ~~*in point (d) of this paragraph;*~~***paragraph 1a;***	(c) to request reports after the completion of the Oversight activities specifying the actions which have been taken or the remedies which have been implemented by the critical ICT third-party providers in relation to the recommendations referred to in point (d) of this paragraph;
Article 31(1), point (d), introductory part			
543	(d) to address recommendations on the areas referred to in Article 30(2), in particular concerning the following:	~~*(d)*~~***1a. For the purposes of carrying out the duties laid down in this Section, and on the basis of the information obtained by the Lead Overseer and the outcomes of the investigations conducted by the Lead Overseer, the Joint Oversight Body shall have the power*** to address recommendations on the areas referred to in Article 30(2), in particular concerning the following:	(d) to address recommendations on the areas referred to in Article 30(2), ~~in particular~~ concerning the following:
Article 31(1), point (d)(i)			
544	(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	(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*~~	(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

	Commission Proposal	EP Mandate	Council Mandate
	Overseer deems relevant for ensuring the ICT security of services provided to financial entities;	~~Overseer~~ ***that the Joint Oversight Body*** deems relevant for ensuring the ICT security of services provided to financial entities;	Overseer deems relevant for ensuring the ICT security of services provided to financial entities;
Article 31(1), point (d)(ii)			
545	(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;	(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~~***that the Joint Oversight 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;	(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;
Article 31(1), point (d)(iii)			
546	(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 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~~ ***Joint Oversight Body*** 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~~**subcontracting** arrangements which the critical ICT third-party service providers plan to undertake with other ICT third-party service providers or with ICT ~~sub-contractors~~**subcontractors** established in a third country, any planned subcontracting, including ~~sub-outsourcing~~**subcontracting**, where the Lead Overseer deems that further subcontracting may trigger risks for the provision of services by the financial entity, or risks to the financial stability;

	Commission Proposal	EP Mandate	Council Mandate
Article 31(1), point (d)(iv), introductory part			
547	(iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:	(iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:	(iv) refraining from entering into a further subcontracting arrangement, where the following cumulative conditions are met:
Article 31(1), point (d)(iv), first indent			
548	- 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 an undertaking constituted in the Union under the law of a Member State***;	- the envisaged ~~sub-contractor~~**subcontractor** is an ICT third-party service provider or an ICT ~~sub-contractor~~**subcontractor** established in a third country;
Article 31(1), point (d)(iv), second indent			
549	- the subcontracting concerns a critical or important function of the financial entity.	- the subcontracting concerns a critical or important function of the financial entity.	- the subcontracting concerns a critical or important function of ~~the~~ financial ~~entity.~~**entities;**
Article 31(1), point (d)(iv), third indent			
549a		***- the sub-contracting will result in serious and clear risks to the financial entity or the financial stability of the Union financial system.***	**- the Lead Overseer deems that the use of such subcontracting poses a clear and serious risk to the financial stability of the Union or to financial entities, including to the ability of the latter to comply with supervisory requirements.**
Article 31(1), point (d)(iv), fourth indent			

	Commission Proposal	EP Mandate	Council Mandate
549b			**For the purpose of point (iv), ICT third-party service providers shall transmit to the Lead Overseer the information regarding subcontracting using the template referred to in Article 36 (1)c).**
Article 31(1), point (e)			
549c			**(e) to adopt the Oversight Plan in accordance with the assessment referred in Article 30(2).**
Article 31(1a)			
549d		***1b. The powers referred to in paragraphs 1 and 1a shall be exercised with regard to the ICT services supporting non-critical or important functions provided by the critical ICT third-party service provider when necessary.***	
Article 31(1b)			
549e		***1c. When exercising the powers referred to in paragraphs 1 and 1a of this Article, the Lead Overseer and the Joint Oversight Body shall take due account of the framework established by Directive (EU) 2016/1148 and, where necessary, consult the relevant competent authorities established by that Directive, in order to avoid unnecessary duplication of***	

	Commission Proposal	EP Mandate	Council Mandate
		technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that Directive.	
Article 31(2)			
550	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 paragraph 1a, the Joint Oversight Body*** ~~*The Lead Overseer*~~ shall ~~*consult the Oversight Forum*~~***inform the critical ICT third-party service provider of its intentions and give the ICT third-party service provider an opportunity to provide information which it reasonably believes should be taken into account*** before ~~*exercising the powers referred to in paragraph 1*~~***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.***.	2. The Lead Overseer shall consult the Oversight Forum before exercising the powers referred to in paragraph 1.
Article 31(2a)			
550a			**2a. The Lead Overseer shall, without undue delay, transmit the reports referred in point (c) of paragraph 1 to the competent authorities of the financial entities using that critical ICT third-party service provider.**

	Commission Proposal	EP Mandate	Council Mandate
Article 31(3)			
551	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 ***and assist*** the Lead Overseer and ~~*assist the Lead Overseer*~~***the Joint Oversight Body*** in the fulfilment of ~~*its*~~***their*** tasks.	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.
Article 31(4)			
552	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 Lead Overseer may ~~*impose a periodic penalty payment to compel*~~***decide, in the case of whole or partial non-compliance with the measures required to be taken in accordance with paragraph 1, points (a),(b) or (c), and after the expiry of a period of at least 60 calendar days from the date on which*** the critical ICT third-party service provider ~~*to comply with points (a), (b) and (c) of paragraph 1*~~***received notification of the measure, to impose a periodic penalty payment to compel the critical ICT third-party service provider to comply***.	~~4.~~ The Lead Overseer ~~may~~**shall, by decision, in case of non-compliance with the appropriate measures taken in accordance with points (a), (b) or (c) of paragraph 1, within 30 calendar days** 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.
Article 31(4a)			
552a		***4a. The periodic penalty payment referred to in paragraph 4 shall be imposed by the Lead Overseer only as a last resort and in cases where the critical ICT third-party service provider has failed to comply with the measures required to be taken in accordance with paragraph 1, points (a), (b) or (c).***	

	Commission Proposal	EP Mandate	Council Mandate
Article 31(5)			
553	5. The periodic penalty payment referred to in paragraph 4 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification to the critical ICT third-party service provider.	5. The periodic penalty payment referred to in paragraph 4 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification to the critical ICT third-party service provider.	5. The periodic penalty payment referred to in paragraph 4 shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification to the critical ICT third-party service provider.
Article 31(6)			
554	6. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be 1% of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year.	6. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be ***up to*** 1% of the average daily worldwide turnover ***related to services provided to financial entities covered by this Regulation*** of the critical ICT third-party service provider in the preceding business year.	6. The amount of the periodic penalty payment, calculated from the date stipulated in the decision imposing the periodic penalty payment, shall be 1% of the average daily worldwide turnover of the critical ICT third-party service provider in the preceding business year.
Article 31(7)			
555	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	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	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

	Commission Proposal	EP Mandate	Council Mandate
	payments shall be allocated to the general budget of the European Union.	payments shall be allocated to the general budget of the European Union.	payments shall be allocated to the general budget of the European Union.
Article 31(8)			
556	8. The ESAs shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure to the public would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.	8. The ESAs shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure to the public would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.	8. The ~~ESAs~~**Lead Overseer** shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure to the public would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.
Article 31(9)			
557	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 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 Lead Overseer shall give the representatives of the critical ICT third-party **service** provider subject to the proceedings the opportunity to be heard on the findings and shall base its decisions only on findings on which the critical ICT third-party provider subject to the proceedings has had an opportunity to comment. The rights of the defence of the persons subject to the proceedings shall be fully respected in the proceedings. They shall be entitled to have access to file, subject to the legitimate interest of other persons in the protection of their business secrets. The right of access to the file shall not extend to confidential information or Lead Overseer's internal preparatory documents.

	Commission Proposal	EP Mandate	Council Mandate
Article 32			
558	Article 32 Request for information	Article 32 Request for information	Article 32 Request for information
Article 32(1)			
559	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 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 Lead Overseer may by simple request or by decision require the critical ICT third-party **service** providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party provider has outsourced operational functions or activities.
Article 32(1a)			
559a		***Critical ICT third-party service providers shall only be required to provide the information referred to in the first subparagraph in respect of the services provided to financial entities that are subject to this Regulation and that use the services of critical ICT third-party service providers for critical or important functions. Critical ICT third-party service providers shall give notice to the relevant financial entity of the requests specific to that financial entity.***	

	Commission Proposal	EP Mandate	Council Mandate
Article 32(2), introductory part			
560	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 Lead Overseer shall:	2. When sending a simple request for information under paragraph 1, the Lead Overseer shall:
Article 32(2), point (a)			
561	(a) refer to this Article as the legal basis of the request;	(a) refer to this Article as the legal basis of the request;	(a) refer to this Article as the legal basis of the request;
Article 32(2), point (b)			
562	(b) state the purpose of the request;	(b) state the purpose of the request;	(b) state the purpose of the request;
Article 32(2), point (c)			
563	(c) specify what information is required;	(c) specify what information is required;	(c) specify what information is required;
Article 32(2), point (d)			
564	(d) set a time limit within which the information is to be provided;	(d) set a time limit within which the information is to be provided;	(d) set a time limit within which the information is to be provided;
Article 32(2), point (e)			
565	(e) inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but that in	(e) inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but that in	(e) inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information, but that in

	Commission Proposal	EP Mandate	Council Mandate
	case of a voluntary reply to the request the information provided must not be incorrect or misleading.	case of a voluntary reply to the request the information provided must not be incorrect or misleading.	case of a voluntary reply to the request the information provided must not be incorrect or misleading.
Article 32(3), introductory part			
566	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 Lead Overseer shall:	3. When requiring to supply information under paragraph 1, the Lead Overseer shall:
Article 32(3), point (a)			
567	(a) refer to this Article as the legal basis of the request;	(a) refer to this Article as the legal basis of the request;	(a) refer to this Article as the legal basis of the request;
Article 32(3), point (b)			
568	(b) state the purpose of the request;	(b) state the purpose of the request;	(b) state the purpose of the request;
Article 32(3), point (c)			
569	(c) specify what information is required;	(c) specify what information is required;	(c) specify what information is required;
Article 32(3), point (d)			
570	(d) set a time limit within which the information is to be provided;	(d) set a ***reasonable*** time limit within which the information is to be provided;	(d) set a time limit within which the information is to be provided;
Article 32(3), point (e)			
571			

	Commission Proposal	EP Mandate	Council Mandate
	(e) indicate the periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete;	(e) indicate the periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete ***or when such information is not provided within the time limit referred to in point (d)***;	(e) indicate the periodic penalty payments provided for in Article 31(4) where the production of the required information is incomplete **or when such information is not provided within the time limit established in point (d)**;
Article 32(3), point (f)			
572	(f) indicate the right to appeal the decision before ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union ('Court of Justice') in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.	(f) indicate the right to appeal the decision before ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union ('Court of Justice') in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.	(f) indicate the right to appeal the decision before ESA's Board of Appeal and to have the decision reviewed by the Court of Justice of the European Union ('Court of Justice') in accordance with Articles 60 and 61 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.
Article 32(4)			
573	4. Representatives of critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.	4. Representatives of critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.	4. Representatives of critical ICT third-party service providers shall supply the information requested. Lawyers duly authorised to act may supply the information on behalf of their clients. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading.
Article 32(5)			
574	5. The Lead Overseer shall, without delay, send a copy of the decision to supply information to	5. The Lead Overseer shall, without delay, send a copy of the decision to supply information to	5. The Lead Overseer shall, without delay, send a copy of the decision to supply information to

	Commission Proposal	EP Mandate	Council Mandate
	the competent authorities of the financial entities using the critical ICT third-party providers' services.	the competent authorities of the financial entities using the critical ICT third-party providers' services.	the competent authorities of the financial entities using the critical ICT third-party providers' services.
Article 33			
575	Article 33 General investigations	Article 33 General investigations	Article 33 General investigations
Article 33(1)			
576	1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the examination team referred to in Article 34(1), may conduct the necessary investigations of ICT third-party service providers:	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)~~***35(1)***, may conduct the necessary investigations of ICT third-party service providers ***in accordance with the principle of proportionality. When conducting investigations, the Lead Overseer shall exercise caution and ensure that the rights of the 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***:	1. In order to carry out its duties under this Regulation, the Lead Overseer, assisted by the **joint** examination team referred to in Article 34(1), may conduct the necessary investigations of **critical** ICT third-party service providers:
Article 33(2), introductory part			
577	2. The Lead Overseer shall be empowered to:	2. The Lead Overseer shall be empowered to:	2. The Lead Overseer shall be empowered to:
Article 33(2), point (a)			
578			

	Commission Proposal	EP Mandate	Council Mandate
	(a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;	(a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;	(a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;
Article 33(2), point (b)			
579	(b) take or obtain certified copies of, or extracts from, such records, data, procedures and other material;	(b) ~~*take or obtain*~~ ***review, in a secured way,*** certified copies of, or extracts from, such records, data, procedures and other material;	(b) take or obtain certified copies of, or extracts from, such records, data, procedures and other material;
Article 33(2), point (c)			
580	(c) summon representatives of the ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;	(c) summon representatives of the ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;	(c) summon representatives of the **critical** ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;
Article 33(2), point (d)			
581	(d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;	(d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;	(d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;
Article 33(2), point (e)			
582	(e) request records of telephone and data traffic.	(e) request records of telephone and data traffic.	(e) request records of telephone and data traffic.

	Commission Proposal	EP Mandate	Council Mandate
Article 33(3), first subparagraph			
583	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 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 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.
Article 33(3), second subparagraph			
584	That authorisation shall also indicate the periodic penalty payments provided for in Article 31(4) where the production of the required records, data, procedures or any other material, or the answers to questions asked to representatives of the ICT third -party service provider are not provided or are incomplete.	That authorisation shall also indicate the periodic penalty payments provided for in Article 31(4) where the production of the required records, data, procedures or any other material, or the answers to questions asked to representatives of the ICT third -party service provider are not provided or are incomplete.	That authorisation shall also indicate the periodic penalty payments provided for in Article 31(4) where the production of the required records, data, procedures or any other material, or the answers to questions asked to representatives of the ICT third -party service provider are not provided or are incomplete.
Article 33(4)			
585	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 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 **critical** ICT third-party service providers are required to submit to the investigations on the basis of a decision of the Lead Overseer. The decision shall specify the subject matter and purpose of the investigation, the periodic penalty payments provided for in Article 31(4), the legal remedies available under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 and the right to have the decision reviewed by the Court of Justice.

	Commission Proposal	EP Mandate	Council Mandate
Article 33(5)			
586	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, 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, **the Lead Overseer**~~Lead Overseers~~ shall inform competent authorities of the financial entities using that **critical** ICT third-party service provider of the investigation and of the identity of the authorised persons.
Article 34			
587	Article 34 On-site inspections	Article 34 On-site inspections	Article 34 On-site inspections
Article 34(1)			
588	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 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 ***service*** 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 Lead Overseer, assisted by the **joint** examination teams referred to in Article 35(1), may enter and conduct all necessary on-site inspections on any business premises, land or property of the ICT third-party providers, such as head offices, operation centres, secondary premises, as well as to conduct off-line inspections.
Article 34(1a), introductory part			
588a		***The power to conduct on-site inspections referred to in the first subparagraph shall not be limited to sites in the Union, provided that the inspection of a site in a third country meets***	

	Commission Proposal	EP Mandate	Council Mandate
		all of the following requirements:	
Article 34(1a), point (a)			
588b		***- it is necessary for the Lead Overseer to carry out its duties under this Regulation;***	
Article 34(1a), point (b)			
588c		***- it has a direct connection to the provision of ICT services to Union financial entities;***	
Article 34(1a), point (c)			
588d		***- it is relevant to an ongoing investigation.***	
Article 34(1b)			
588e		***1a. When performing on-site inspections, the Lead Overseer and the examination team shall exercise caution and ensure that the rights of the 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.***	
Article 34(2), first subparagraph			
589	2. The officials and other persons authorised by the Lead Overseer to conduct an on-site	2. The officials and other persons authorised by the Lead Overseer to conduct an on-site	2. The officials and other persons authorised by the Lead Overseer to conduct an on-site

	Commission Proposal	EP Mandate	Council Mandate
	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.	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.	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.
Article 34(2), second subparagraph			
590	They shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection and the periodic penalty payments provided for in Article 31(4) where the representatives of the ICT third-party service providers concerned do not submit to the inspection.	They shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection and the periodic penalty payments provided for in Article 31(4) where the representatives of the ICT third-party service providers concerned do not submit to the inspection.	They shall exercise their powers upon production of a written authorisation specifying the subject matter and the purpose of the inspection and the periodic penalty payments provided for in Article 31(4) where the representatives of the **critical** ICT third-party service providers concerned do not submit to the inspection.
Article 34(3)			
591	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, Lead Overseers shall inform the competent authorities of the financial entities using that ICT third-party provider.	3. In good time before the inspection, **the Lead Overseer**~~Lead Overseers~~ shall inform the competent authorities of the financial entities using that ICT third-party provider.
Article 34(4)			
592	4. Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of services to financial entities.	4. Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data ***that the Lead Overseer deems appropriate and technologically relevant,*** either used for, or contributing to, the provision of services to financial entities.	4. Inspections shall cover the full range of relevant ICT systems, networks, devices, information and data either used for, or contributing to, the provision of services to financial entities.

	Commission Proposal	EP Mandate	Council Mandate
Article 34(5)			
593	5. Before any planned on-site visit, Lead Overseers shall give a reasonable notice to the critical ICT third-party service providers, unless such notice is not possible due to an emergency or crisis situation, or if it would lead to a situation where the inspection or audit would no longer be effective.	5. Before any planned on-site ~~visit~~***inspection***, Lead Overseers shall give a reasonable notice to the critical ICT third-party service providers, unless such notice is not possible due to an emergency or crisis situation, or if it would lead to a situation where the inspection or audit would no longer be effective.	5. Before any planned on-site visit, **the Lead Overseer**~~Lead Overseers~~ shall give a reasonable notice to the critical ICT third-party service providers, unless such notice is not possible due to an emergency or crisis situation, or if it would lead to a situation where the inspection or audit would no longer be effective.
Article 34(6)			
594	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 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 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.
Article 34(7)			
595	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,	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,	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,

	Commission Proposal	EP Mandate	Council Mandate
	the Lead Overseer shall inform the critical ICT provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.	the Lead Overseer shall inform the critical ICT ***third-party service*** provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.	the Lead Overseer shall inform the critical ICT provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.
Article 35			
596	Article 35 Ongoing Oversight	Article 35 Ongoing Oversight	Article 35 Ongoing Oversight
Article 35(1)			
597	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 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 Lead ~~Overseers~~**Overseer** shall be assisted by ~~an~~**a joint** examination team established for each critical ICT third-party service provider.
Article 35(2)			
598	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	2. The joint examination team referred to in paragraph 1 shall be composed of staff members from the Lead Overseer***, from the other 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	2. The joint examination team referred to in paragraph 1 shall be composed of staff members from ~~the Lead Overseer and from~~**:** **(a) the ESAs;** **(b) ,** the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider

	Commission Proposal	EP Mandate	Council Mandate
	shall have expertise in ICT and operational risk. The joint examination team shall work under the coordination of a designated ESA staff member (the 'Lead Overseer coordinator').	members of the joint examination shall have expertise in ICT and operational risk. The joint examination team shall work under the coordination of a designated ESA staff member (the 'Lead Overseer coordinator').	provides services**;** **(c) the national competent authority referred to in Article 29(3)e), on a voluntary basis;** **(d) one national competent authority from the Member State where the critical ICT third-party service provider is established, on a voluntary basis.** **Members of the joint examination team will join the preparation and execution**~~, who will join the preparation and execution of the Oversight activities, with a maximum of 10 members. All members~~ of the ~~joint examination~~**Oversight activities and** shall have expertise in ICT and operational risk. The joint examination team shall work under the coordination of a designated ~~ESA~~**Lead Overseer** staff member (the 'Lead Overseer coordinator').
Article 35(3), first subparagraph			
599	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	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	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:

	Commission Proposal	EP Mandate	Council Mandate
	date of entry into force].	date of entry into force].	insert date ~~1 year~~**18 months** after the date of entry into force].
Article 35(3), second subparagraph			
600	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.	Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively.
Article 35(4)			
601	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 ~~*Lead Overseer, after consultation of the*~~***Joint*** Oversight ~~*Forum,*~~ ***Body*** 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 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.
Article 35(5), first subparagraph			
602	5. The recommendations referred to in paragraph 4 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides services.	5. The recommendations referred to in paragraph 4 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides services.	5. The recommendations referred to in paragraph 4 shall be immediately communicated to the critical ICT third-party service provider and to the competent authorities of the financial entities to which it provides services.

	Commission Proposal	EP Mandate	Council Mandate
Article 35(5), second subparagraph			
603	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, Lead Overseers ***and the Joint Oversight 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.	For the purposes of fulfilling the Oversight activities, Lead ~~Overseers~~**Overseer** may take into consideration any relevant third-party certifications and ICT third-party internal or external audit reports made available by the critical ICT third-party service provider.
Article 35(5a)			
603a			**5a. The Lead Overseer, assisted by the joint examination team, shall assess the compliance with the recommendations referred to in paragraph 4. The Lead Overseer shall, without undue delay, inform the competent authorities of the financial entities using that critical ICT third-party service provider of the result of such assessment.**
Article 36			
604	Article 36 Harmonisation of conditions enabling the conduct of the Oversight	Article 36 Harmonisation of conditions enabling the conduct of the Oversight	Article 36 Harmonisation of conditions enabling the conduct of the Oversight
Article 36(1), introductory part			
605	1. The ESAs shall, through the Joint Committee, develop draft regulatory technical	1. The ESAs shall, through the Joint Committee, develop draft regulatory technical	1. The ESAs shall, through the Joint Committee, develop draft regulatory technical

	Commission Proposal	EP Mandate	Council Mandate
	standards to specify:	standards to specify:	standards to specify:
Article 36(1), point (a)			
606	(a) the information to be provided by a critical ICT third-party service provider in the application for a voluntary opt-in set out in Article 28(8);	(a) the information to be provided by a critical ICT third-party service provider in the application for a voluntary opt-in set out in Article 28(8);	(a) the information to be provided by a critical ICT third-party service provider in the application for a voluntary opt-in set out in Article 28(8);
Article 36(1), point (b)			
607	(b) the content and format of reports which may be requested for the purposes of point (c) of Article 31(1);	(b) the content and format of reports which may be requested for the purposes of point (c) of Article 31(1);	(b) the content and format of reports which may be requested for the purposes of point (c) of Article 31(1);
Article 36(1), point (c)			
608	(c) the presentation of the information, including the structure, formats and methods that a critical ICT third-party service provider shall be required to submit, disclose or report pursuant to Article 31(1);	(c) the presentation of the information, including the structure, formats and methods that a critical ICT third-party service provider shall be required to submit, disclose or report pursuant to Article 31(1);	(c) the presentation of the information, including the structure, formats and methods that a critical ICT third-party service provider shall be required to submit, disclose or report pursuant to Article 31(1) **including the template to provide information on subcontracting arrangements**;
Article 36(1), point (ca)			
608a			**(ca) the criteria for determining the composition of the joint examination team established for each critical ICT third-party service provider pursuant to Article 35(2) ensuring a balanced participation of staff**

	Commission Proposal	EP Mandate	Council Mandate
			members from the Lead Overseer and from relevant competent authorities in accordance with Article 41, appointed on the basis of their knowledge, skills and experience in ICT and operational risk.
Article 36(1), point (d)			
609	(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 competent authorities' assessment of measures taken by critical ICT third-party service providers based on the recommendations of ~~*Lead Overseers*~~ ***the Joint Oversight Body*** pursuant to Article 37(2).	(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~~**Overseer** pursuant to Article 37(2).
Article 36(2), first subparagraph			
610	2. The ESAs shall submit those draft regulatory technical standards to the Commission by 1 January 20xx [OJ: insert date 1 year after the date of entry into force].	2. The ESAs shall submit those draft regulatory technical standards to the Commission by 1 January 20xx [OJ: insert date 1 year after the date of entry into force].	2. The ESAs shall submit those draft regulatory technical standards to the Commission by 1 January 20xx [OJ: insert date ~~1 year~~**18 months** after the date of entry into force].
Article 36(2), second subparagraph			
611	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.	Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 respectively.

	Commission Proposal	EP Mandate	Council Mandate
Article 37			
612	Article 37 Follow-up by competent authorities	Article 37 Follow-up by competent authorities	Article 37 Follow-up by competent authorities
Article 37(1)			
613	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 ~~*Lead Overseers*~~ ***the Joint Oversight Body*** pursuant to ~~*point (d) of*~~ Article ~~*31(1)*~~***31(1a)***, critical ICT third-party service providers shall notify the ~~*Lead Overseer*~~ ***Joint Oversight Body*** whether they intend to follow those recommendations. ~~*Lead Overseers*~~ ***The Joint Oversight Body*** shall immediately transmit this information to competent authorities ***of the financial entities concerned***.	1. Within ~~30~~**60** calendar days after the receipt of the recommendations issued by **the Lead Overseer**~~Lead Overseers~~ pursuant to point (d) of Article 31(1), critical ICT third-party service providers shall **either** notify the Lead Overseer ~~whether they intend~~**on their intention** to follow ~~those~~**the recommendations or provide a reasoned explanation for not following such** recommendations. **The Lead Overseer** ~~Lead Overseers~~ shall immediately transmit this information to competent authorities.
Article 37(1a)			
613a			**1a. The Lead Overseer shall publicly disclose where a critical ICT third-party service provider fails to notify the Lead Overseer in accordance with paragraph 1 or in case the explanation provided by the critical ICT third-party service provider is not deemed as sufficient. The information published shall disclose the identity of the critical ICT third-party service provider as well as information on the type and nature of the non-compliance. It shall be limited to what is relevant and proportionate for the**

	Commission Proposal	EP Mandate	Council Mandate
			purpose of ensuring public awareness, unless such publication causes disproportionate damage to the parties involved or could seriously jeopardise the orderly functioning and integrity of financial markets or the stability of the whole or part of the financial system of the Union.
Article 37(2)			
614	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*~~***inform*** financial entities ~~*take into account*~~***that have concluded contractual arrangements with critical ICT third-party service providers of*** the risks identified in the recommendations addressed to ***those*** critical ICT third-party ***service*** providers by the ~~*Lead Overseer*~~***Joint Oversight Body*** in accordance with ~~*points (d) of Article 31(1)*~~***Article 31(1a) and monitor whether financial entities take into account the risks identified***. ***The Joint Oversight Body shall monitor whether the critical ICT third-party providers have addressed the risks identified in those recommendations.***	2. ~~Competent authorities shall monitor whether~~**When managing ICT third-party risk,** 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). **Competent authorities shall monitor financial entities' compliance with this obligation.**
Article 37(2a)			
614a			**2a. Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third party risk the specific risks identified in the recommendations referred**

	Commission Proposal	EP Mandate	Council Mandate
			to in paragraph 2, it shall notify the financial entity of the possibility of a decision being taken pursuant to paragraph 3 within 60 working days, in the absence of appropriate contractual arrangements aimed at addressing such risks.
Article 37(2b)			
614b			**2b. Upon receiving the reports referred to in Article 31(2a) and the assessment referred to in Article 35(5a), and prior to taking any of the decisions referred to in paragraph 3, competent authorities may, on a voluntary basis, consult the national competent authorities designated under Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or digital service provider listed in Annex III of that Directive which has been designated as a critical ICT third-party service provider.**
Article 37(3)			
615	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	3. ***Where regulatory objectives cannot be ensured by other measures, and warnings have been issued to the affected financial entities by the national*** competent authorities ***on the basis of information communicated by the Joint Oversight Board, the board of the Lead Overseer may decide, upon recommendation from the Joint Oversight Body and after***	3. Competent authorities may, **as a measure of last resort, following the notification and, if appropriate, the consultation as set out in paragraph 2a and 2b,** in accordance with Article 44, require financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third-party **service**

	Commission Proposal	EP Mandate	Council Mandate
	may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the critical ICT third-party service providers.	***consultation with the competent authorities of the affected*** ~~*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*~~***to financial entities exposed to*** the risks identified in the recommendations addressed to critical ICT third-party ***service*** providers ***until those risks*** have been addressed. Where necessary, ***and as a measure of last resort,*** they may require ~~*financial entities*~~ ***the critical ICT third-party service providers*** to terminate, in part or completely, the relevant contractual arrangements concluded with the ~~*critical ICT third-party service providers*~~***financial entities exposed to the identified risks***.	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.
Article 37(4), introductory part			
616	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 the decisions referred to in paragraph 3, ~~*competent authorities*~~***the Board of the Lead Overseer*** 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. **Upon receiving the reports referred to in Article 31(2a) and the assessment referred to in Article 35(5a), competent authorities,** 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:
Article 37(4), point (a)			
617			

	Commission Proposal	EP Mandate	Council Mandate
	(a) the gravity and the duration of the non-compliance;	(a) the gravity and the duration of the non-compliance;	(a) the gravity and the duration of the non-compliance;
Article 37(4), point (b)			
618	(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;	(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;	(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;
Article 37(4), point (c)			
619	(c) whether financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;	(c) whether financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;	(c) whether financial crime was facilitated, occasioned or otherwise attributable to the non-compliance;
Article 37(4), point (d)			
620	(d) whether the non-compliance has been committed intentionally or negligently.	(d) whether the non-compliance has been committed intentionally or negligently.	(d) whether the non-compliance has been committed intentionally or negligently.
Article 37(4), point (da)			
620a		***(da) whether the suspension or termination introduces a continuity risk for the business operations of the service user of the critical ICT third-party service provider.***	
Article 37(4), point (e)			
620b			

	Commission Proposal	EP Mandate	Council Mandate
			(e) where applicable, the opinion of the national competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 responsible for the supervision of an operator of essential services listed in point (7) of Annex II or a digital service provider listed in Annex III of that Directive, respectively, which has been designated as a critical ICT third-party service provider, requested on a voluntary basis in accordance with paragraph 2.b.
Article 37(4a)			
620c		***4a. The decisions provided for in paragraph 3 shall only be implemented once all affected financial entities have been duly notified thereof. The affected financial entities shall be afforded a period of time, which shall not go beyond what is strictly necessary, to adjust their outsourcing and contractual arrangements with critical ICT third-party service providers in such a way as to not jeopardise digital operational resilience and to execute their exit strategies and transition plans referred to in Article 25.***	
Article 37(4a)			
620d			**4a. The decision referred in paragraph 3 shall be notified to the members of the Oversight Forum referred in letters (a) to (c) of Article 29(3).**

	Commission Proposal	EP Mandate	Council Mandate
Article 37(4b)			
620e		***The critical ICT third-party service providers subject to the decisions provided for in paragraph 3 shall fully cooperate with the affected financial entities.***	
Article 37(5)			
621	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 ~~*Lead Overseers*~~***Joint Oversight Body*** 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 Lead ~~Overseers~~**Overseer** on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual ~~measures~~**arrangements** taken by the latter where critical ICT third-party service have not endorsed in part or entirely recommendations addressed by the Lead ~~Overseers~~**Overseer**.
Article 38			
622	Article 38 Oversight fees	Article 38 Oversight fees	Article 38 Oversight fees
Article 38(1), first subparagraph			
623	1. The ESAs shall charge critical ICT third-party service providers fees that fully cover ESAs' necessary expenditure in relation to the conduct of Oversight tasks pursuant to this Regulation, including the reimbursement of any	1. The ESAs shall charge critical ICT third-party service providers fees that fully cover ESAs' necessary expenditure in relation to the conduct of Oversight tasks pursuant to this Regulation, including the reimbursement of any	1. The ~~ESAs~~**Lead Overseer** shall**, in accordance with the delegated act referred to in paragraph 2,** charge critical ICT third-party service providers fees that fully cover ESAs' necessary expenditure in relation to the conduct

	Commission Proposal	EP Mandate	Council Mandate
	costs which may be incurred as a result of work carried out by competent authorities joining the Oversight activities in accordance with Article 35.	costs which may be incurred as a result of work carried out by competent authorities joining the Oversight activities in accordance with Article 35.	of Oversight tasks pursuant to this Regulation, including the reimbursement of any costs which may be incurred as a result of work carried out by competent authorities joining the Oversight activities in accordance with Article 35.
Article 38(1), second subparagraph			
624	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 ~~*administrative costs*~~***costs derived from the execution of the duties foreseen in this Section*** and shall be proportionate to their turnover.	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.
Article 38(1a)			
624a		***1a. If an administrative arrangement is entered into 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).***	
Article 38(2)			
625	2. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid.	2. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid.	2. The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by determining the amount of the fees and the way in which they are to be paid.
Article 39			

	Commission Proposal	EP Mandate	Council Mandate
626	Article 39 International cooperation	Article 39 International cooperation	Article 39 International cooperation
Article 39(1)			
627	1. EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, notably by developing best practices for the review of ICT risk-management practices and controls, mitigation measures and incident responses.	1. EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, notably by developing best practices for the review of ICT risk-management practices and controls, mitigation measures and incident responses.	1. EBA, ESMA and EIOPA may, in accordance with Article 33 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, respectively, conclude administrative arrangements with third-country regulatory and supervisory authorities to foster international cooperation on ICT third-party risk across different financial sectors, notably by developing best practices for the review of ICT risk-management practices and controls, mitigation measures and incident responses.
Article 39(2)			
628	2. The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission summarising the findings of relevant discussions held with the third countries authorities referred to in paragraph 1, focussing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection or the functioning of the single market.	2. The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission summarising the findings of relevant discussions held with the third countries authorities referred to in paragraph 1, focussing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection or the functioning of the single market.	2. The ESAs shall, through the Joint Committee, submit every five years a joint confidential report to the European Parliament, to the Council and to the Commission summarising the findings of relevant discussions held with the third countries authorities referred to in paragraph 1, focussing on the evolution of ICT third-party risk and the implications for financial stability, market integrity, investor protection or the functioning of the single market.
CHAPTER VI			

	Commission Proposal	EP Mandate	Council Mandate
629	CHAPTER VI INFORMATION SHARING ARRANGEMENTS	CHAPTER VI INFORMATION SHARING ARRANGEMENTS	CHAPTER VI INFORMATION SHARING ARRANGEMENTS
Article 40			
630	Article 40 Information-sharing arrangements on cyber threat information and intelligence	Article 40 Information-sharing arrangements on cyber threat information and intelligence	Article 40 Information-sharing arrangements on cyber threat information and intelligence
Article 40(1), introductory part			
631	1. Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:	1. Financial entities ~~*may*~~ ***shall endeavour to*** exchange amongst themselves ***and ICT third-party service providers*** cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:	1. Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:
Article 40(1), point (a)			
632	(a) aims at enhancing the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting financial entities' range of defensive capabilities, threat detection techniques, mitigation strategies or response and recovery stages;	(a) aims at enhancing the digital operational resilience of financial entities ***and ICT third-party service providers***, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting ~~*financial entities' range of*~~ defensive capabilities, threat detection techniques, mitigation strategies or response	(a) aims at enhancing the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting financial entities' range of defensive capabilities, threat detection techniques, mitigation strategies or response and recovery stages;

	Commission Proposal	EP Mandate	Council Mandate
		and recovery stages;	
Article 40(1), point (b)			
633	(b) takes places within trusted communities of financial entities;	(b) takes places within trusted communities of financial entities ***and ICT third-party service providers***;	(b) takes places within trusted communities of financial entities;
Article 40(1), point (c)			
634	(c) is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data[1] and guidelines on competition policy.[2] _____ 1. In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). 2. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01.	(c) is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data[1] and guidelines on competition policy~~.~~[2] **.** _____ 1. In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). 2. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01.	(c) is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal**1** data[1] and guidelines on competition policy.[2] _____ 1. In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). 2. Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01.
Article 40(2)			
635	2. For the purpose of point (c) of paragraph 1, the information sharing arrangements shall define the conditions for participation and,	2. For the purpose of point (c) of paragraph 1, the information sharing arrangements shall define the conditions for participation and,	2. For the purpose of point (c) of paragraph 1, the information sharing arrangements shall define the conditions for participation and,

	Commission Proposal	EP Mandate	Council Mandate
	where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, as well as on operational elements, including the use of dedicated IT platforms.	where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, as well as on operational elements, including the use of dedicated IT platforms.	where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, as well as on operational elements, including the use of dedicated IT platforms.
Article 40(3)			
636	3. Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once the latter takes effect.	3. Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once the latter takes effect.	3. ~~Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once the latter takes effect.~~
CHAPTER VII			
637	CHAPTER VII COMPETENT AUTHORITIES	CHAPTER VII COMPETENT AUTHORITIES	CHAPTER VII COMPETENT AUTHORITIES
Article 41			
638	Article 41 Competent authorities	Article 41 Competent authorities	Article 41 Competent authorities
Article 41, first paragraph, introductory part			
639	Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Section II of Chapter V of this Regulation, compliance	Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Section II of Chapter V of this Regulation, compliance	Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Section II of Chapter V of this Regulation, compliance

	Commission Proposal	EP Mandate	Council Mandate
	with the obligations set out in this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:	with the obligations set out in this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:	with the obligations set out in this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts:
Article 41, first paragraph, point (a)			
640	(a) for credit institutions, the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, without prejudice to the specific tasks conferred on the ECB by Regulation (EU) No 1024/2013;	(a) for credit institutions, the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, without prejudice to the specific tasks conferred on the ECB by Regulation (EU) No 1024/2013;	(a) for credit institutions~~,~~**:** **(i)** the competent authority designated in accordance with Article 4 of Directive 2013/36/EU, ~~without prejudice to the specific tasks conferred on~~**including for credit institutions exempted under Directive 2013/36/EU and;** **(ii) in the case of credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013,** the ECB **in accordance with the powers and tasks conferred** by Regulation (EU) No 1024/2013;
Article 41, first paragraph, point (b)			
641	(b) for payment service providers, the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366;	(b) for payment service providers, the competent authority designated in accordance with Article 22 of Directive (EU) 2015/2366;	(b) for payment service providers, **payment institutions exempted under Directive (EU) 2015/2366, electronic money institutions exempted under Directive 2009/110/EC and account information service providers as referred to in Article 33(1) of Directive (EU) 2015/2366,** the competent authority designated in accordance with Article 22 of Directive (EU)

	Commission Proposal	EP Mandate	Council Mandate
			2015/2366;
Article 41, first paragraph, point (c)			
642	(c) for electronic payment institutions, the competent authority designated in accordance with Article 37 of Directive 2009/110/EC;	(c) for electronic payment institutions, the competent authority designated in accordance with Article 37 of Directive 2009/110/EC;	(c) ~~for electronic payment institutions, the competent authority designated in accordance with Article 37 of Directive 2009/110/EC;~~
Article 41, first paragraph, point (d)			
643	(d) for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034;	(d) for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034;	(d) for investment firms, the competent authority designated in accordance with Article 4 of Directive (EU) 2019/2034;
Article 41, first paragraph, point (e)			
644	(e) for crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens, the competent authority designated in accordance with the first indent of point (ee) of Article 3 (1) of [Regulation (EU) 20xx MICA Regulation];	(e) for crypto-asset service providers, issuers ***and offerors*** of crypto-assets, issuers ***and offerors*** of asset-referenced tokens and issuers of significant asset-referenced tokens, the competent authority designated in accordance with the first indent of point (ee) of Article 3 (1) of [Regulation (EU) 20xx MICA Regulation];	(e) for crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens, the competent authority designated in accordance with the first indent of point (ee) of Article 3 (1) of [Regulation (EU) 20xx MICA Regulation];
Article 41, first paragraph, point (f)			
645	(f) for central securities depositories, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;	(f) for central securities depositories ***and operators of securities settlement systems***, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;	(f) for central securities depositories, the competent authority designated in accordance with Article 11 of Regulation (EU) No 909/2014;

	Commission Proposal	EP Mandate	Council Mandate
Article 41, first paragraph, point (g)			
646	(g) for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;	(g) for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;	(g) for central counterparties, the competent authority designated in accordance with Article 22 of Regulation (EU) No 648/2012;
Article 41, first paragraph, point (h)			
647	(h) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU;	(h) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU;	(h) for trading venues and data reporting service providers, the competent authority designated in accordance with Article 67 of Directive 2014/65/EU;
Article 41, first paragraph, point (i)			
648	(i) for trade repositories, the competent authority designated in accordance with Article 55 of Regulation (EU) No 648/2012;	(i) for trade repositories, the competent authority designated in accordance with Article 55 of Regulation (EU) No 648/2012;	(i) for trade repositories, the competent authority designated in accordance with Article 55 of Regulation (EU) No 648/2012;
Article 41, first paragraph, point (j)			
649	(j) for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;	(j) for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;	(j) for managers of alternative investment funds, the competent authority designated in accordance with Article 44 of Directive 2011/61/EU;
Article 41, first paragraph, point (k)			
650	(k) for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;	(k) for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;	(k) for management companies, the competent authority designated in accordance with Article 97 of Directive 2009/65/EC;

	Commission Proposal	EP Mandate	Council Mandate
Article 41, first paragraph, point (l)			
651	(l) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;	(l) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;	(l) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of Directive 2009/138/EC;
Article 41, first paragraph, point (m)			
652	(m) for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;	(m) for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;	(m) for insurance intermediaries~~, reinsurance intermediaries and ancillary insurance~~ **and reinsurance** intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97;
Article 41, first paragraph, point (n)			
653	(n) for institutions for occupational retirement pensions, the competent authority designated in accordance with Article 47 of Directive 2016/2341;	(n) for institutions for occupational retirement ~~*pensions*~~***provisions***, the competent authority designated in accordance with Article 47 of Directive 2016/2341;	(n) for institutions for occupational retirement ~~pensions~~**provision**, the competent authority designated in accordance with Article 47 of Directive 2016/2341;
Article 41, first paragraph, point (o)			
654	(o) for credit rating agencies, the competent authority designated in accordance Article 21 of Regulation (EC) No 1060/2009;	(o) for credit rating agencies, the competent authority designated in accordance Article 21 of Regulation (EC) No 1060/2009;	(o) for credit rating agencies, the competent authority designated in accordance Article 21 of Regulation (EC) No 1060/2009;
Article 41, first paragraph, point (p)			
655			

	Commission Proposal	EP Mandate	Council Mandate
	(p) for statutory auditors and audit firms, the competent authority designated in accordance Articles 3(2) and 32 of Directive 2006/43/EC;	(p) for statutory auditors and audit firms, the competent authority designated in accordance Articles 3(2) and 32 of Directive 2006/43/EC;	(p) ~~for statutory auditors and audit firms, the competent authority designated in accordance Articles 3(2) and 32 of Directive 2006/43/EC;~~
Article 41, first paragraph, point (q)			
656	(q) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of Regulation xx/202x;	(q) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of Regulation ~~xx/202x~~***(EU) 2016/1011***;	(q) for administrators of critical benchmarks, the competent authority designated in accordance with Articles 40 and 41 of ~~Regulation xx/202x~~**Regulation 2016/1011**;
Article 41, first paragraph, point (r)			
657	(r) for crowdfunding service providers, the competent authority designated in accordance with Article x of Regulation xx/202x;	(r) for crowdfunding service providers, the competent authority designated in accordance with Article ~~x~~ ***29*** of Regulation***(EU) 2020/1503*** ~~xx/202x~~;	(r) for crowdfunding service providers, the competent authority designated in accordance with Article ~~x of Regulation xx/202x~~**29 of Regulation 2020/1503**;
Article 41, first paragraph, point (s)			
658	(s) for securitisation repositories, the competent authority designated in accordance with Article 10 and 14 (1) of Regulation (EU) 2017/2402.	(s) for securitisation repositories, the competent authority designated in accordance with Article 10 and 14 (1) of Regulation (EU) 2017/2402.	(s) for securitisation repositories, the competent authority designated in accordance with Article 10 and 14 (1) of Regulation (EU) 2017/2402.
Article 42			
659	Article 42 Cooperation with structures and authorities established by Directive (EU) 2016/1148	Article 42 Cooperation with structures and authorities established by Directive (EU) 2016/1148	Article 42 Cooperation with structures and authorities established by Directive (EU) 2016/1148
Article 42(1)			

	Commission Proposal	EP Mandate	Council Mandate
660	1. To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs and the competent authorities, may request to be invited to the workings of Cooperation Group.	1. To foster cooperation and enable supervisory exchanges between the competent authorities designated under this Regulation and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs and the competent authorities, ~~*may request to be invited to the workings of Cooperation Group*~~***shall be invited to participate in the work of the Cooperation Group. insofar as that work concerns supervisory and oversight activities, respectively, in relation to entities listed under point (7) of Annex II to Directive (EU) 2016/1148 that have also been designated as critical ICT third-party service providers pursuant to Article 28 of this Regulation***.	1. To foster cooperation and enable supervisory exchanges between ~~the~~ competent authorities designated under this Regulation and the Cooperation Group established by Article 11 of Directive (EU) 2016/1148, the ESAs and the competent authorities, may request to be invited to the workings of **the** Cooperation Group.
Article 42(2)			
661	2. Competent authorities may consult where appropriate with the single point of contact and the national Computer Security Incident Response Teams referred to respectively in Articles 8 and 9 of Directive (EU) 2016/1148.	2. Competent authorities may consult where appropriate with the single point of contact and the national Computer Security Incident Response Teams referred to respectively in Articles 8 and 9 of Directive (EU) 2016/1148.	2. **Where appropriate,** competent authorities may consult ~~where appropriate~~**and share information** with the single point of contact and the national Computer Security Incident Response Teams referred to respectively in Articles 8 and 9 of Directive (EU) 2016/1148.
Article 42(2a)			
661a		***2a. The Lead Overseer shall inform and cooperate with the competent authorities designated under Directive (EU) 2016/1148 before conducting general investigations and on-site inspections in accordance with Articles***	

	Commission Proposal	EP Mandate	Council Mandate
		33 and 34 of this Regulation.	
Article 42(3)			
661b			**3. Where appropriate competent authorities may request any relevant technical advice and assistance from the competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 and establish cooperation arrangements to allow the set-up of effective and fast-response coordination mechanisms.**
Article 42(3a)			
661c			**3a. The arrangements referred to in paragraph 3 may, amongst other, specify the procedures for the coordination of supervisory and oversight activities, respectively, in relation to operators of essential services listed under point (7) of Annex II or digital service providers listed in Annex III of the Directive (EU) 2016/1148 which have been designated as critical ICT third-party service providers pursuant to Article 28, including for the conduct, in accordance with national law, of investigations and on-site inspections, as well as mechanisms for the exchange of information between competent authorities and authorities designated in accordance with Article 8 of Directive (EU) 2016/1148 which include access to information**

	Commission Proposal	EP Mandate	Council Mandate
			requested by the latter authorities.
Article 42a			
661d			**Article 42a** **Cooperation between authorities**
Article 42a(1)			
661e			**1. Competent authorities shall cooperate closely among themselves and, where applicable, with the Lead Overseer.**
Article 42a(2)			
661f			**2. Competent authorities and the Lead Overseer shall, in a timely manner, mutually exchange all relevant information concerning critical ICT third-party service providers which is necessary for them to carry out the respective duties resulting from this Regulation, notably in relation to identified risks, approaches and measures taken as part of the Lead Overseer's oversight tasks.**
Article 43			
662	Article 43 Financial cross-sector exercises, communication and cooperation	Article 43 Financial cross-sector exercises, communication and cooperation	Article 43 -Financial cross-sector exercises, communication and cooperation

	Commission Proposal	EP Mandate	Council Mandate
Article 43(1), first subparagraph			
663	1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB and the ESRB, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors.	1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB***, the Single Resolution Board in respect of information relating to entities falling under the scope of Regulation (EU) No 806/2014*** and the ESRB, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors.	1. The ESAs, through the Joint Committee and in collaboration with competent authorities, the ECB ~~and~~**,** the ESRB **and ENISA as appropriate**, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors.
Article 43(1), second subparagraph			
664	They may develop crisis-management and contingency exercises involving cyber-attack scenarios with a view to develop communication channels and gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the Union's financial sector as a whole.	They may develop crisis-management and contingency exercises involving cyber-attack scenarios with a view to develop communication channels and gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident or ~~*related*~~ ***significant cyber*** threat having a systemic impact on the Union's financial sector as a whole.	They may develop crisis-management and contingency exercises involving cyber-attack scenarios with a view to develop communication channels and gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the Union's financial sector as a whole.
Article 43(1), third subparagraph			
665	These exercises may as appropriate also test the financial sector' dependencies on other economic sectors.	These exercises may as appropriate also test the financial sector' dependencies on other economic sectors.	These exercises may as appropriate also test the financial sector' dependencies on other economic sectors.
Article 43(2)			

	Commission Proposal	EP Mandate	Council Mandate
666	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, national resolution authorities*** and the ~~*ECB*~~***Single Resolution Board in respect of information relating to entities falling under the scope of Regulation (EU) No 806/2014*** 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 and the ECB shall cooperate closely with each other and exchange information to carry out their duties pursuant to Articles 42 to 48. They shall closely coordinate their supervision in order to identify and remedy breaches of this Regulation, develop and promote best practices, facilitate collaboration, foster consistency of interpretation and provide cross-jurisdictional assessments in the event of any disagreements.
Article 44			
667	Article 44 Administrative penalties and remedial measures	Article 44 Administrative penalties and remedial measures	Article 44 Administrative penalties and remedial measures
Article 44(1)			
668	1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.	1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.	1. Competent authorities shall have all supervisory, investigatory and sanctioning powers necessary to fulfil their duties under this Regulation.
Article 44(2), introductory part			
669	2. The powers referred to in paragraph 1 shall include at least the powers to:	2. The powers referred to in paragraph 1 shall include at least the powers to:	2. The powers referred to in paragraph 1 shall include at least the powers to:

	Commission Proposal	EP Mandate	Council Mandate
Article 44(2), point (a)			
670	(a) have access to any document or data held in any form which the competent authority considers relevant for the performance of its duties and receive or take a copy of it;	(a) have access to any document or data held in any form ~~*which*~~***that*** the competent authority considers relevant for the performance of its duties and receive or take a copy of it;	(a) have access to any document or data held in any form which the competent authority considers relevant for the performance of its duties and receive or take a copy of it;
Article 44(2), point (aa)			
670a			**(aa) summon representatives of the financial entities for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;**
Article 44(2), point (ab)			
670b			**(ab) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;**
Article 44(2), point (b)			
671	(b) carry out on-site inspections or investigations;	(b) carry out on-site inspections or investigations;	(b) carry out on-site inspections or investigations;
Article 44(2), point (c)			
672	(c) require corrective and remedial measures	(c) require corrective and remedial measures	(c) require corrective and remedial measures

	Commission Proposal	EP Mandate	Council Mandate
	for breaches of the requirements of this Regulation.	for breaches of the requirements of this Regulation.	for breaches of the requirements of this Regulation.
Article 44(3), first subparagraph			
673	3. Without prejudice to the right of Member States to impose criminal penalties according to Article 46, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.	3. Without prejudice to the right of Member States to impose criminal penalties according to Article 46, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.	3. Without prejudice to the right of Member States to impose criminal penalties according to Article 46, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation.
Article 44(3), second subparagraph			
674	Those penalties and measures shall be effective, proportionate and dissuasive.	Those penalties and measures shall be effective, proportionate and dissuasive.	Those penalties and measures shall be effective, proportionate and dissuasive.
Article 44(4), introductory part			
675	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. 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. 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:
Article 44(4), point (a)			
676	(a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;	(a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;	(a) issue an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;

	Commission Proposal	EP Mandate	Council Mandate
Article 44(4), point (b)			
677	(b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;	(b) require the temporary or permanent cessation of any practice or conduct ~~*that the competent authority considers*~~***considered*** to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;	(b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;
Article 44(4), point (c)			
678	(c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;	(c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;	(c) adopt any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements;
Article 44(4), point (d)			
679	(d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and	(d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and	(d) require, in so far as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and
Article 44(4), point (e)			
680	(e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.	(e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.	(e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.
Article 44(5)			

	Commission Proposal	EP Mandate	Council Mandate
681	5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.	5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.	5. Where the provisions referred to in point (c) of paragraph 2 and in paragraph 4 apply to legal persons, Member States shall confer on competent authorities the power to apply the administrative penalties and remedial measures, subject to the conditions provided for in national law, to members of the management body, and to other individuals who under national law are responsible for the breach.
Article 44(6)			
682	6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.	6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.	6. Member States shall ensure that any decision imposing administrative penalties or remedial measures set out in point (c) of paragraph 2 is properly reasoned and is subject to a right of appeal.
Article 45			
683	Article 45 Exercise of the power to impose administrative penalties and remedial measures	Article 45 Exercise of the power to impose administrative penalties and remedial measures	Article 45 Exercise of the power to impose administrative penalties and remedial measures
Article 45(1), introductory part			
684	1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 44 in accordance with their national legal frameworks, as appropriate:	1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 44 in accordance with their national legal frameworks, as appropriate:	1. Competent authorities shall exercise the powers to impose administrative penalties and remedial measures referred to in Article 44 in accordance with their national legal frameworks, as appropriate:

	Commission Proposal	EP Mandate	Council Mandate
Article 45(1), point (a)			
685	(a) directly;	(a) directly;	(a) directly;
Article 45(1), point (b)			
686	(b) in collaboration with other authorities;	(b) in collaboration with other authorities;	(b) in collaboration with other authorities;
Article 45(1), point (c)			
687	(c) under their responsibility by delegation to other authorities;	(c) under their responsibility by delegation to other authorities;	(c) under their responsibility by delegation to other authorities;
Article 45(1), point (d)			
688	(d) by application to the competent judicial authorities.	(d) by application to the competent judicial authorities.	(d) by application to the competent judicial authorities.
Article 45(2), introductory part			
689	2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate:	2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate:	2. Competent authorities, when determining the type and level of an administrative penalty or remedial measure to be imposed under Article 44, shall take into account the extent to which the breach is intentional or results from negligence and all other relevant circumstances, including, where appropriate:
Article 45(2), point (a)			

	Commission Proposal	EP Mandate	Council Mandate
690	(a) the materiality, gravity and the duration of the breach;	(a) the materiality, gravity and the duration of the breach;	(a) the materiality, gravity and the duration of the breach;
Article 45(2), point (b)			
691	(b) the degree of responsibility of the natural or legal person responsible for the breach;	(b) the degree of responsibility of the natural or legal person responsible for the breach;	(b) the degree of responsibility of the natural or legal person responsible for the breach;
Article 45(2), point (c)			
692	(c) the financial strength of the responsible natural or legal person;	(c) the financial strength of the responsible natural or legal person;	(c) the financial strength of the responsible natural or legal person;
Article 45(2), point (d)			
693	(d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;	(d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;	(d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;
Article 45(2), point (e)			
694	(e) the losses for third parties caused by the breach, insofar as they can be determined;	(e) the losses for third parties caused by the breach, insofar as they can be determined;	(e) the losses for third parties caused by the breach, insofar as they can be determined;
Article 45(2), point (f)			
695	(f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses	(f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses	(f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses

	Commission Proposal	EP Mandate	Council Mandate
	avoided by that person;	avoided by that person;	avoided by that person;
Article 45(2), point (g)			
696	(g) previous breaches by the responsible natural or legal person.	(g) previous breaches by the responsible natural or legal person.	(g) previous breaches by the responsible natural or legal person.
Article 46			
697	Article 46 Criminal penalties	Article 46 Criminal penalties	Article 46 Criminal penalties
Article 46(1)			
698	1. Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches which are subject to criminal penalties under their national law.	1. Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches ~~which~~***that*** are subject to criminal penalties under their national law.	1. Member States may decide not to lay down rules for administrative penalties or remedial measures for breaches which are subject to criminal penalties under their national law.
Article 46(2)			
699	2. Where Member States have chosen to lay down criminal penalties for breaches of this Regulation they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other competent	2. Where Member States have chosen to lay down criminal penalties for breaches of this Regulation they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other competent	2. Where Member States have chosen to lay down criminal penalties for breaches of this Regulation they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for breaches of this Regulation, and to provide the same information to other competent

	Commission Proposal	EP Mandate	Council Mandate
	authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.	authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.	authorities, as well as EBA, ESMA or EIOPA to fulfil their obligations to cooperate for the purposes of this Regulation.
Article 47			
700	Article 47 Notification duties	Article 47 Notification duties	Article 47 Notification duties
Article 47, first paragraph			
701	Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by [OJ: insert date 1 year after the date of entry into force]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.	Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by [OJ: insert date ~~*1 year*~~ ***12 months*** after the date of entry into force]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.	Member States shall notify the laws, regulations and administrative provisions implementing this Chapter, including any relevant criminal law provisions, to the Commission, ESMA, the EBA and EIOPA by [OJ: insert date ~~1 year~~**24 months** after the date of entry into force]. Member States shall notify the Commission, ESMA, the EBA and EIOPA without undue delay of any subsequent amendments thereto.
Article 48			
702	Article 48 Publication of administrative penalties	Article 48 Publication of administrative penalties	Article 48 Publication of administrative penalties
Article 48(1)			
703	1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the	1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the	1. Competent authorities shall publish on their official websites, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the

	Commission Proposal	EP Mandate	Council Mandate
	addressee of the sanction has been notified of that decision.	addressee of the sanction has been notified of that decision.	addressee of the sanction has been notified of that decision.
Article 48(2)			
704	2. The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the identity of the persons responsible and the penalties imposed.	2. The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the ***penalties imposed, and, exceptionally, the*** identity of the persons responsible ~~*and the penalties imposed*~~.	2. The publication referred to in paragraph 1 shall include information on the type and nature of the breach, the identity of the persons responsible and the penalties imposed.
Article 48(3), introductory part			
705	3. Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt either of the following solutions in respect to the decision imposing an administrative sanction:	3. Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt either of the following solutions in respect to the decision imposing an administrative sanction:	3. Where the competent authority, following a case-by-case assessment, considers that the publication of the identity, in the case of legal persons, or of the identity and personal data, in the case of natural persons, would be disproportionate, jeopardise the stability of financial markets or the pursuit of an on-going criminal investigation, **create disproportionate risks to the protection of personal data of individuals,** or cause, insofar as these can be determined, disproportionate damages to the person involved, it shall adopt either of the following solutions in respect to the decision imposing an administrative sanction:
Article 48(3), point (a)			
706	(a) defer its publication until the moment where all reasons for non-publication cease to exist;	(a) defer its publication until the moment where all reasons for non-publication cease to exist;	(a) defer its publication until the moment where all reasons for non-publication cease to exist;

	Commission Proposal	EP Mandate	Council Mandate
Article 48(3), point (b)			
707	(b) publish it on an anonymous basis, in accordance with national law; or	(b) publish it on an anonymous basis, in accordance with national law; or	(b) publish it on an anonymous basis, in accordance with national law; or
Article 48(3), point (c)			
708	(c) refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportional with the leniency of the imposed sanction.	(c) refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportional with the leniency of the imposed sanction.	(c) refrain from publishing it, where the options set out in points (a) and (b) are deemed either insufficient to guarantee a lack of any danger for the stability of financial markets, or where such a publication would not be proportional with the leniency of the imposed sanction.
Article 48(4)			
709	4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with point (b) of paragraph 3, the publication of the relevant data may be postponed.	4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with point (b) of paragraph 3, the publication of the relevant data may be postponed.	4. In the case of a decision to publish an administrative penalty on an anonymous basis in accordance with point (b) of paragraph 3, the publication of the relevant data may be postponed.
Article 48(5)			
710	5. Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and at later stages any subsequent related information on	5. Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and at later stages any subsequent related information on	5. Where a competent authority publishes a decision imposing an administrative penalty against which there is an appeal before the relevant judicial authorities, competent authorities shall immediately add on their official website that information and at later stages any subsequent related information on

	Commission Proposal	EP Mandate	Council Mandate
	the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.	the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.	the outcome of such appeal. Any judicial decision annulling a decision imposing an administrative penalty shall also be published.
Article 48(6)			
711	6. Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website for at least five years after its publication. Personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules.	6. Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website for at least five years after its publication. Personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules.	6. Competent authorities shall ensure that any publication referred to in paragraphs 1 to 4 shall remain on their official website ~~for at least five years after its publication. Personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules~~**only for the period which is necessary to bring forth this Article. This period shall not exceed t five years after its publication**.
Article 49			
712	Article 49 Professional secrecy	Article 49 Professional secrecy	Article 49 Professional secrecy
Article 49(1)			
713	1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.	1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.	1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraph 2.
Article 49(2)			
714			

	Commission Proposal	EP Mandate	Council Mandate
	2. The obligation of professional secrecy applies to all persons who work or who have worked for the competent authorities under this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.	2. The obligation of professional secrecy applies to all persons who work or who have worked for the competent authorities under this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.	2. The obligation of professional secrecy applies to all persons who work or who have worked for the competent authorities under this Regulation, or for any authority or market undertaking or natural or legal person to whom those competent authorities have delegated their powers, including auditors and experts contracted by them.
Article 49(3)			
715	3. Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law.	3. Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law.	3. Information covered by professional secrecy may not be disclosed to any other person or authority except by virtue of provisions laid down by Union or national law**, including the exchange of information among competent authorities and competent authorities designated in accordance with Article 8 of Directive (EU) 2016/1148**.
Article 49(4)			
716	4. All information exchanged between the competent authorities under this Regulation that concerns business or operational conditions and other economic or personal affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states at the time of communication that such information may be disclosed or where such disclosure is necessary for legal proceedings.	4. All information exchanged between the competent authorities under this Regulation that concerns business or operational conditions and other economic or personal affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states at the time of communication that such information may be disclosed or where such disclosure is necessary for legal proceedings.	4. All information exchanged between the competent authorities under this Regulation that concerns business or operational conditions and other economic or personal affairs shall be considered confidential and shall be subject to the requirements of professional secrecy, except where the competent authority states at the time of communication that such information may be disclosed or where such disclosure is necessary for legal proceedings.

	Commission Proposal	EP Mandate	Council Mandate
Article 49a			
716a			**Article 49a** **Data Protection**
Article 49a(1)			
716b			**1. The ESAs and the competent authorities shall be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations and duties under this Regulation, in particular for investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight plans. The personal data shall be processed in accordance with Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, whichever is applicable.**
Article 49a(2)			
716c			**2. Except otherwise provided in other sectoral acts, the personal data referred to in paragraph 1 shall be retained until the discharge of the applicable supervisory duties and in any case for a maximum period of 15 years, except in case of pending court proceedings requiring further retention of such data.**
CHAPTER VIII			

	Commission Proposal	EP Mandate	Council Mandate
717	CHAPTER VIII DELEGATED ACTS	CHAPTER VIII DELEGATED ACTS	CHAPTER VIII DELEGATED ACTS
Article 50			
718	Article 50 Exercise of the delegation	Article 50 Exercise of the delegation	Article 50 Exercise of the delegation
Article 50(1)			
719	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
Article 50(2)			
720	2. The power to adopt delegated acts referred to in Articles 28(3) and 38(2) shall be conferred on the Commission for a period of five years from [PO: insert date 5 years after the date of entry into force of this Regulation].	2. The power to adopt delegated acts referred to in Articles 28(3) and 38(2) shall be conferred on the Commission for a period of five years from [PO: insert date 5 years after the date of entry into force of this Regulation]. ***The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.***	2. The power to adopt delegated acts referred to in Articles 28(3) and 38(2) shall be conferred on the Commission for a period of five years from [PO: insert date ~~5 years~~**12 months** after the date of entry into force of this Regulation].
Article 50(3)			

	Commission Proposal	EP Mandate	Council Mandate
721	3. The delegation of power referred to in Articles 28(3) and 38(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Articles 28(3) and 38(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Articles 28(3) and 38(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
Article 50(4)			
722	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
Article 50(5)			
723	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
Article 50(6)			
724	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	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	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

	Commission Proposal	EP Mandate	Council Mandate
	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.	European Parliament or by the Council within a period of ~~two~~***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 ~~two~~ ***three*** months at the initiative of the European Parliament or of the Council.	European Parliament or by the Council within a period of ~~two~~**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 ~~two~~**three** months at the initiative of the European Parliament or of the Council.
CHAPTER IX			
725	CHAPTER IX TRANSITIONAL AND FINAL PROVISIONS	CHAPTER IX TRANSITIONAL AND FINAL PROVISIONS	CHAPTER IX TRANSITIONAL AND FINAL PROVISIONS
SECTION I			
726	SECTION I	SECTION I	SECTION I
Article 51			
727	Article 51 Review clause	Article 51 Review clause	Article 51 Review clause
Article 51, first paragraph			
728	By [PO: insert date 5 years after the date of entry into force of this Regulation], the Commission shall, after consulting EBA, ESMA, EIOPA, and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council,	By [PO: insert date 5 years after the date of entry into force of this Regulation], the Commission shall, after consulting EBA, ESMA, EIOPA, and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council,	**1.** By [PO: insert date 5 years after the date of entry into force of this Regulation], the Commission shall, after consulting EBA, ESMA, EIOPA, and the ESRB, as appropriate, carry out a review and submit a report to the European Parliament and the Council,

	Commission Proposal	EP Mandate	Council Mandate
	accompanied, if appropriate, by a legislative proposal, regarding the criteria for the designation of critical ICT third-party service providers in Article 28(2).	accompanied, if appropriate, by a legislative proposal~~, regarding the criteria for the designation of critical ICT third-party service providers in Article 28(2)~~. ***The report shall review at least the following:***	accompanied, if appropriate, by a legislative proposal, regarding ~~the criteria for the designation of critical ICT third-party service providers in Article 28(2).~~**:**
Article 51, first paragraph, point (a)			
728a		***(a) the possibility of extending the scope of application of this Regulation to operators of payment systems;***	
Article 51, first paragraph, point (a)			
728b			**(a) the criteria for the designation of critical ICT third-party service providers in Article 28(2), and:**
Article 51, first paragraph, point (b)			
728c		***(b) the voluntary nature of the reporting of significant cyber threats;***	
Article 51, first paragraph, point (b)			
728d			**(b) the regime, referred to in Article 28(9) of this Regulation, applicable to critical ICT third-party providers established in a third country, and the powers of the Lead Overseer provided for in the first indent of Article 31 (1) d) (iv), with a view to evaluating the need to continue requiring**

	Commission Proposal	EP Mandate	Council Mandate
			establishment in the Union. This review should entail an analysis of this requirement, including in terms of access for European financial entities to competitive and innovative services from third countries and it should take into account further developments in the markets for the services covered by this Regulation, the practical experience of financial entities and financial supervisors with the application and, respectively, supervision of this regime, and any relevant regulatory and supervisory developments taking place at international level.
Article 51, first paragraph, point (c)			
728e		***(c) the criteria for the designation of critical ICT third-party service providers in Article 28(2); and***	
Article 51, first paragraph, point (d)			
728f		***(d) the efficiency of the decision-making of the Joint Oversight Body and the exchange of information between the Joint Oversight Body and non-member national competent authorities.***	
Article 51, first paragraph a			
728g			**2. No later than [PO: insert date 6 months**

	Commission Proposal	EP Mandate	Council Mandate
			after the date of entry into force], the Commission shall submit a report to the European Parliament and the Council assessing the need for an increased cyber resilience in payment systems and payment-processing activities and the appropriateness of extension of the scope of this Regulation to these entities.
Article 51, first paragraph b			
728h			**In the review of Directive 2015/2366 (PSD2), in light of this report, the Commission shall submit, after consulting EBA, ESMA, EIOPA, ECB and the ESRB, if appropriate, a legislative proposal in order to ensure that all operators of payment systems and entities involved in payment-processing activities are subject to an appropriate oversight, while taking into account existing central bank oversight.**
SECTION II			
729	SECTION II AMENDMENTS	SECTION II AMENDMENTS	SECTION II AMENDMENTS
Article 52			
730	Article 52 Amendments to Regulation (EC) No 1060/2009	Article 52 Amendments to Regulation (EC) No 1060/2009	Article 52 Amendments to Regulation (EC) No 1060/2009
Article 52, first paragraph, introductory part			

	Commission Proposal	EP Mandate	Council Mandate
731	In Annex I to Regulation (EC) No 1060/2009, the first subparagraph of point 4 of Section A is replaced by the following:	In Annex I to Regulation (EC) No 1060/2009, the first subparagraph of point 4 of Section A is replaced by the following:	In Annex I to Regulation (EC) No 1060/2009, the first subparagraph of point 4 of Section A is replaced by the following:
Article 52, first paragraph, amending provision, first paragraph			
732	‘ A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].	‘ A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].	‘ **‘**A credit rating agency shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for managing ICT systems in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].
Article 52, first paragraph, amending provision, second paragraph			
733	* Regulation (EU) 2021/xx of the European Parliament and of the Council […] (OJ L XX, DD.MM.YYYY, p. X).. ,	* Regulation (EU) 2021/xx of the European Parliament and of the Council […] (OJ L XX, DD.MM.YYYY, p. X).. ,	*——— Regulation (EU) 2021/xx of the European Parliament and of the Council […] (OJ L XX, DD.MM.YYYY, p. X).**’**. ,
Article 53			
734	Article 53 Amendments to Regulation (EU) No 648/2012	Article 53 Amendments to Regulation (EU) No 648/2012	Article 53 Amendments to Regulation (EU) No 648/2012
Article 53, first paragraph, introductory part			

	Commission Proposal	EP Mandate	Council Mandate
735	Regulation (EU) No 648/2012 is amended as follows:	Regulation (EU) No 648/2012 is amended as follows:	Regulation (EU) No 648/2012 is amended as follows:
Article 53, first paragraph, point (1), introductory part			
736	(1) Article 26 is amended as follows:	(1) Article 26 is amended as follows:	(1) Article 26 is amended as follows:
Article 53, first paragraph, point (1)(a), introductory part			
737	(a) paragraph 3 is replaced by the following:	(a) paragraph 3 is replaced by the following:	(a) paragraph 3 is replaced by the following:
Article 53, first paragraph, point (1)(a), amending provision, numbered paragraph (3), introductory part			
738	‘ 3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].	‘ 3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].	‘ 3. A CCP shall maintain and operate an organisational structure that ensures continuity and orderly functioning in the performance of its services and activities. It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].
Article 53, first paragraph, point (1)(a), amending provision, numbered paragraph (3), first paragraph			
739	* Regulation (EU) 2021/xx of the European Parliament and of the Council	* Regulation (EU) 2021/xx of the European Parliament and of the Council	*——— Regulation (EU) 2021/xx of the European Parliament and of the Council

	Commission Proposal	EP Mandate	Council Mandate
	[…](OJ L XX, DD.MM.YYYY, p. X).; ,	[…](OJ L XX, DD.MM.YYYY, p. X).; ,	[…](OJ L XX, DD.MM.YYYY, p. X).**'**; ,
Article 53, first paragraph, point (1)(b)			
740	(b) paragraph 6 is deleted;	(b) paragraph 6 is deleted;	(b) paragraph 6 is deleted;
Article 53, first paragraph, point (2), introductory part			
741	(2) Article 34 is amended as follows:	(2) Article 34 is amended as follows:	(2) Article 34 is amended as follows:
Article 53, first paragraph, point (2)(a), introductory part			
742	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:	(a) paragraph 1 is replaced by the following:
Article 53, first paragraph, point (2)(a), amending provision, numbered paragraph (1)			
743	‘ 1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.; ,	‘ 1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.; ,	‘ 1. A CCP shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan, which shall include ICT business continuity and disaster recovery plans set up in accordance with Regulation (EU) 2021/xx [DORA], aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the CCP's obligations.**'**; ,
Article 53, first paragraph, point (2)(b), introductory part			

	Commission Proposal	EP Mandate	Council Mandate
744	(b) in paragraph 3, the first subparagraph is replaced by the following:	(b) in paragraph 3, the first subparagraph is replaced by the following:	(b) in paragraph 3, the first subparagraph is replaced by the following:
Article 53, first paragraph, point (2)(b), amending provision, first paragraph			
745	‘ In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity and disaster recovery plans.; ’	‘ In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity and disaster recovery plans.; ’	‘ **‘**In order to ensure consistent application of this Article, ESMA shall, after consulting the members of the ESCB, develop draft regulatory technical standards specifying the minimum content and requirements of the business continuity policy and of the disaster recovery plan, excluding ICT business continuity and disaster recovery plans.**’**; ’
Article 53, first paragraph, point (3), introductory part			
746	(3) in Article 56, the first subparagraph of paragraph 3 is replaced by the following:	(3) in Article 56, the first subparagraph of paragraph 3 is replaced by the following:	(3) in Article 56, the first subparagraph of paragraph 3 is replaced by the following:
Article 53, first paragraph, point (3), amending provision, numbered paragraph (3)			
747	‘ 3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for	‘ 3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for	‘ 3. In order to ensure consistent application of this Article, ESMA shall develop draft regulatory technical standards specifying the details, other than for requirements related to ICT risk management, of the application for

	Commission Proposal	EP Mandate	Council Mandate
	registration referred to in paragraph 1.; ,	registration referred to in paragraph 1.; ,	registration referred to in paragraph 1.**'**; ,
Article 53, first paragraph, point (4), introductory part			
748	(4) in Article 79, paragraphs 1 and 2 are replaced by the following:	(4) in Article 79, paragraphs 1 and 2 are replaced by the following:	(4) in Article 79, paragraphs 1 and 2 are replaced by the following:
Article 53, first paragraph, point (4), amending provision, numbered paragraph (1)			
749	‘ 1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx [DORA].	‘ 1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx [DORA].	‘ 1. A trade repository shall identify sources of operational risk and minimise them also through the development of appropriate systems, controls and procedures, including ICT systems managed in accordance with Regulation (EU) 2021/xx [DORA].
Article 53, first paragraph, point (4), amending provision, numbered paragraph (2)			
750	2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity and disaster recovery plans established in accordance with Regulation (EU) 2021/xx[DORA], aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations.; ,	2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity and disaster recovery plans established in accordance with Regulation (EU) 2021/xx[DORA], aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations.; ,	2. A trade repository shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan including ICT business continuity and disaster recovery plans established in accordance with Regulation (EU) 2021/xx[DORA], aiming at ensuring the maintenance of its functions, the timely recovery of operations and the fulfilment of the trade repository's obligations.**'**; ,

	Commission Proposal	EP Mandate	Council Mandate
Article 53, first paragraph, point (5)			
751	(5) in Article 80, paragraph 1 is deleted.	(5) in Article 80, paragraph 1 is deleted.	(5) in Article 80, paragraph 1 is deleted.
Article 54			
752	Article 54 Amendments to Regulation (EU) No 909/2014	Article 54 Amendments to Regulation (EU) No 909/2014	Article 54 Amendments to Regulation (EU) No 909/2014
Article 54, first paragraph, introductory part			
753	Article 45 of Regulation (EU) No 909/2014 is amended as follows:	Article 45 of Regulation (EU) No 909/2014 is amended as follows:	Article 45 of Regulation (EU) No 909/2014 is amended as follows:
Article 54, first paragraph, point (1), introductory part			
754	(1) paragraph 1 is replaced by the following:	(1) paragraph 1 is replaced by the following:	(1) paragraph 1 is replaced by the following:
Article 54, first paragraph, point (1), amending provision, numbered paragraph (1), introductory part			
755	‘ 1. A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council*[DORA], as well as through any other relevant appropriate tools,	‘ 1. A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council*[DORA], as well as through any other relevant appropriate tools,	‘ 1. ——A CSD shall identify sources of operational risk, both internal and external, and minimise their impact also through the deployment of appropriate ICT tools, processes and policies set up and managed in accordance with Regulation (EU) 2021/xx of the European Parliament and of the Council*[DORA], as well as through any other relevant appropriate tools,

	Commission Proposal	EP Mandate	Council Mandate
	controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.	controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.	controls and procedures for other types of operational risk, including for all the securities settlement systems it operates.
Article 54, first paragraph, point (1), amending provision, numbered paragraph (1), first paragraph			
756	* Regulation (EU) 2021/xx of the European Parliament and of the Council […](OJ L XX, DD.MM.YYYY, p. X).; ,	* Regulation (EU) 2021/xx of the European Parliament and of the Council […](OJ L XX, DD.MM.YYYY, p. X).; ,	*——— Regulation (EU) 2021/xx of the European Parliament and of the Council […](OJ L XX, DD.MM.YYYY, p. X).**'**; ,
Article 54, first paragraph, point (2)			
757	(2) paragraph 2 is deleted;	(2) paragraph 2 is deleted;	(2) paragraph 2 is deleted;
Article 54, first paragraph, point (3), introductory part			
758	(3) paragraphs 3 and 4 are replaced by the following:	(3) paragraphs 3 and 4 are replaced by the following:	(3) paragraphs 3 and 4 are replaced by the following:
Article 54, first paragraph, point (3), amending provision, numbered paragraph (3)			
759	‘ 3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity and disaster recovery plan, including ICT business continuity and disaster recovery plans	‘ 3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity and disaster recovery plan, including ICT business continuity and disaster recovery plans	‘ 3. For services that it provides as well as for each securities settlement system that it operates, a CSD shall establish, implement and maintain an adequate business continuity and disaster recovery plan, including ICT business continuity and disaster recovery plans

	Commission Proposal	EP Mandate	Council Mandate
	established in accordance with Regulation (EU) 2021/xx [DORA], to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations.	established in accordance with Regulation (EU) 2021/xx [DORA], to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations.	established in accordance with Regulation (EU) 2021/xx [DORA], to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations.
Article 54, first paragraph, point (3), amending provision, numbered paragraph (4)			
760	4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in paragraphs (5) and (7) of Article 11 of Regulation (EU) 2021/xx [DORA].; '	4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in paragraphs (5) and (7) of Article 11 of Regulation (EU) 2021/xx [DORA].'; '	4. The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can resume operations from the time of disruption as provided for in paragraphs (5) and (7) of Article 11 of Regulation (EU) 2021/xx [DORA].'; '
Article 54, first paragraph, point (4), introductory part			
761	(4) in paragraph 6, the first subparagraph is replaced by the following:	(4) ~~*in paragraph 6, the first subparagraph is replaced by the following:*~~	(4) ~~in~~ paragraph 6~~, the first subparagraph~~ is replaced by the following:
Article 54, first paragraph, point (4), amending provision, first paragraph			
762	' A CSD shall identify, monitor and manage the	' ~~*A CSD shall identify, monitor and manage the*~~	' A CSD shall identify, monitor and manage the

	Commission Proposal	EP Mandate	Council Mandate
	risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of any operational incidents, other than in relation to ICT risk, resulting from such risks.; ,	~~*risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of any operational incidents, other than in relation to ICT risk, resulting from such risks.;*~~ ,	risks that key participants in the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified. It shall also inform the competent authority and relevant authorities without delay of any operational incidents, other than in relation to ICT risk, resulting from such risks.**'**; ,
Article 54, first paragraph, point (5), introductory part			
763	(5) in paragraph 7, the first subparagraph is replaced by the following:	(5) ~~*in paragraph 7, the first subparagraph is replaced by the following:*~~	(5) in paragraph 7, the first subparagraph is replaced by the following:
Article 54, first paragraph, point (5), amending provision, first paragraph			
764	‘ ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risks, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.. ,	‘ ~~*ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risks, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof..*~~ ,	‘ ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the operational risks referred to in paragraphs 1 and 6, other than ICT risks, and the methods to test, to address or to minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof.**'**. ,

	Commission Proposal	EP Mandate	Council Mandate
Article 55			
765	Article 55 Amendments to Regulation (EU) No 600/2014	Article 55 Amendments to Regulation (EU) No 600/2014	Article 55 Amendments to Regulation (EU) No 600/2014
Article 55, first paragraph, introductory part			
766	Regulation (EU) No 600/2014 is amended as follows:	Regulation (EU) No 600/2014 is amended as follows:	Regulation (EU) No 600/2014 is amended as follows:
Article 55, first paragraph, point (1), introductory part			
767	(1) Article 27g is amended as follows:	(1) Article 27g is amended as follows:	(1) Article 27g is amended as follows:
Article 55, first paragraph, point (1)(a)			
768	(a) paragraph 4 is deleted;	(a) paragraph 4 is deleted;	(a) paragraph 4 is deleted;
Article 55, first paragraph, point (1)(b)			
769	(b) in paragraph 8, point (c) is replaced by the following:	(b) in paragraph 8, point (c) is replaced by the following:	(b) in paragraph 8, point (c) is replaced by the following:
Article 55, first paragraph, point (1)(c)			
770	(c) '(c) the concrete organisational requirements laid down in paragraphs 3 and 5.';	(c) '(c) the concrete organisational requirements laid down in paragraphs 3 and 5.';	~~(c)~~ '(c) the concrete organisational requirements laid down in paragraphs 3 and 5.';
Article 55, first paragraph, point (2), introductory part			
771			

	Commission Proposal	EP Mandate	Council Mandate
	(2) Article 27h is amended as follows:	(2) Article 27h is amended as follows:	(2) Article 27h is amended as follows:
Article 55, first paragraph, point (2)(a)			
772	(a) paragraph 5 is deleted;	(a) paragraph 5 is deleted;	(a) paragraph 5 is deleted;
Article 55, first paragraph, point (2)(b), introductory part			
773	(b) in paragraph 8, point (e) is replaced by the following:	(b) in paragraph 8, point (e) is replaced by the following:	(b) in paragraph 8, point (e) is replaced by the following:
Article 55, first paragraph, point (2)(b), amending provision, first paragraph			
774	‘ (e) the concrete organisational requirements laid down in paragraph 4.; ’	‘ (e) the concrete organisational requirements laid down in paragraph 4.; ’	‘ (e) the concrete organisational requirements laid down in paragraph 4.’; ’
Article 55, first paragraph, point (3), introductory part			
775	(3) Article 27i is amended as follows:	(3) Article 27i is amended as follows:	(3) Article 27i is amended as follows:
Article 55, first paragraph, point (3)(a)			
776	(a) paragraph 3 is deleted;	(a) paragraph 3 is deleted;	(a) paragraph 3 is deleted;
Article 55, first paragraph, point (3)(b), introductory part			
777	(b) in paragraph 5, point (b) is replaced by the	(b) in paragraph 5, point (b) is replaced by the	(b) in paragraph 5, point (b) is replaced by the

	Commission Proposal	EP Mandate	Council Mandate
	following:	following:	following:
Article 55, first paragraph, point (3)(b), amending provision, first paragraph			
778	‘ (b) the concrete organisational requirements laid down in paragraphs 2 and 4.. ,	‘ (b) the concrete organisational requirements laid down in paragraphs 2 and 4.. ,	‘ (b) the concrete organisational requirements laid down in paragraphs 2 and 4.**’**. ,
Article 56			
779	Article 56 Entry into force and application	Article 56 Entry into force and application	Article 56 Entry into force and application
Article 56, first paragraph			
780	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
Article 56, second paragraph			
781	It shall apply from [PO: insert date - 12 months after the date of entry into force].	It shall apply from [PO: insert date ~~- 12~~***24*** months after the date of entry into force].	It shall apply from [PO: insert date - ~~12~~**24** months after the date of entry into force].
Article 56, third paragraph			
782	However, Articles 23 and 24 shall apply from [PO: insert date - 36 months after the date of entry into force of this Regulation].	However, Articles 23 and 24 shall apply from [PO: insert date - 36 months after the date of entry into force of this Regulation].	~~However, Articles 23 and 24 shall apply from [PO: insert date - 36 months after the date of entry into force of this Regulation].~~

	Commission Proposal	EP Mandate	Council Mandate
Article 56, fourth paragraph			
783	This Regulation shall be binding in entirety and directly applicable in all Member States.	This Regulation shall be binding in entirety and directly applicable in all Member States.	This Regulation shall be binding in entirety and directly applicable in all Member States.
Formula			
784	Done at Brussels,	Done at Brussels,	Done at Brussels,
Formula			
785	For the European Parliament	For the European Parliament	For the European Parliament
Formula			
786	The President	The President	The President
Formula			
787	For the Council	For the Council	For the Council
Formula			
788	The President	The President	The President