Discovery Phase - DORA

Key points:

Get a comprehensive understanding of DORA and its direct impact on your financial institution;

Navigate the complexities of DORA's directives and regulations, ensuring your organisation stays compliant;

Discover how DORA is a catalyst for enhancing digital operational resilience and staying ahead in the financial sector;

Recognise the tangible benefits and strategic importance of DORA compliance for your organisation; and

Learn how CyberComply can be your trusted partner on the journey to DORA compliance, simplifying the process and ensuring you're well prepared for the future.

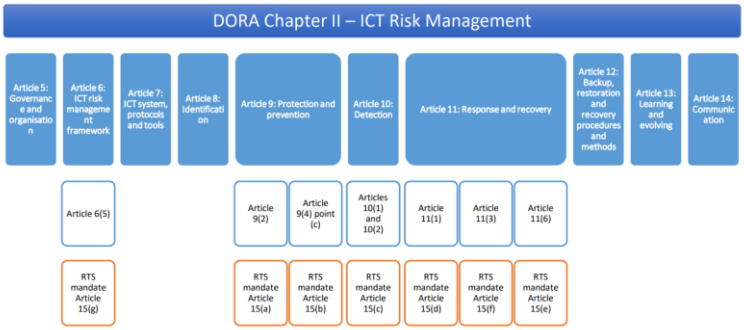
Scope: The scope of analysis includes requirements published under Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022, together with RTS/ITS documents published until 19 April 2024.

General Provisions

Article	Category	Policies
Article 1	Subject Matter	This Regulation lays down requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve high common level of digital operational resilience.
Article 2	Personal Scope	To whom financial entities regulation shall apply to and shall not apply to.
Article 3	Definitions	For Purpose of this regulation definitions for terms are explained.
Article 4	Proportionality Principle	Financial entities shall implement rules in accordance with the principle of proportionality.

Article	Category	Procedures
Article 1	Subject Matter	Requirements in relation to: · ICT Risk Management, reporting of Incidents - Cyberthreat, reporting of major operational or security payment related incidents, digital operational resilience testing, information and intelligence sharing, management of ICT Third party risk. · contractual arrangements. · Oversight framework for ICT third party service providers · Rules on supervision and enforcement. · state functions concerning public security, defence and national security in accordance with Union Law
Article 2	Personal Scope	Shall apply to: Credit Institutions, Investment Firms, Insurance Undertakings, IORPS, Investment management companies Market infrastructures (such as CCPs, stock exchanges, systemic internalises, trade repositories and MTFs), CRAs, authorized payment institutions and electronic money institutions, crowd funding entities, statutory auditors, audit firms, crypto assets service providers, benchmark administrators. Shall not apply to: Managers of alternative investment funds, insurance and reinsurance undertakings, institutions for occupational retirement provision, legal person exempted from application of Directive 2014/65/EU
Article 3	Definitions	Terms- digital operational resilience, network and information system, legacy ICT system, security of network and information system, ICT risk, information asset, ICT asset, ICT related incident, operational or security payment-related incident, major ICT related incident, major operational or security payment-related incident, cyber threat, significant cyber threat, defence-in-depth, vulnerability, threat led penetration testing penetration testing, ICT third party service provider, critical ICT third-party service provider, , subsidiary, group, parent undertaking, management body, credit institution, investment firm, electronic money institution, central counterparty, trade repository, central securities depository, data reporting service provider, insurance undertaking, reinsurance undertaking, insurance intermediary, ancillary insurance intermediary, reinsurance intermediary, institution For occupational retirement provision, small institution For occupational retirement provision, credit rating agency, crypto asset service provider, issuer of asset-referenced tokens, administrator of critical benchmarks, crowdfunding service provider, securitisation repository, microenterprise, lead overseer, joint committee, small enterprise, medium sized enterprise, public authority
Article 4	Proportionality Principle	application by financial entities of this regulation shall be proportionate to financial entities size, nature, scale and complexity of the services, activities and operations, and their overall risk profile.

Chapter 1: ICT Risk Management



Article	Category	Policies
Article 5	Governance and Organisation	Financial entities shall have in place internal governance and a control framework that ensure an effective and prudent management of all ICT risks, to achieve a high level of digital operational resilience
Article 6	ICT risk management framework	Financial entities shall have a sound comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enable them to address ICT risk quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience.
Article 7	ICT Systems, protocols, and tools	Financial entities shall use and maintain updated ICT systems, protocols, and tools to address and manage ICT risk
Article 8	Identification	Financial Entities shall Identify, classify, document and review all ICT supported business functions. Shall allocate roles, and responsibilities, their ICT Assets and dependencies with ICT risk and cyber threats.
Article 9	Protection and Prevention	Financial entities shall aim at ensuring the resilience, continuity and availability of ICT systems, maintaining high standards of confidentiality, integrity, and availability of data whether at rest, in use or in transit. ICT change management shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.
Article 10	Detection	Financial entities shall have in place mechanisms to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents and to identify potential material single points of failure.
Article 11	Response and recovery	Financial entities shall put in place ICT Business Continuity Policy, which may be adopted as a dedicated specific policy forming an integral part of the overall business continuity policy.
Article 12	Backup Policies, restoration and recovery methods	Restoration of ICT systems, data with least downtime, disruption, loss · Backup policies and procedures specifying the scope of the data, minimum frequency of backup, criticality of information, confidentiality level of data. · recovery methods and testing of backup and restoration procedures shall be undertaken on periodic basis
Article 13	Learning and evolving	Financial entities shall have in place capabilities and staff, to gather information on cyber threats and vulnerabilities, ICT-related incidents in particular cyber-attacks. Shall put in place post ICT-related incident reviews after major ICT-related incidents disrupting their core activities, analysing the causes of disruption, and identifying required improvements to the ICT operations or within the ICT Business continuity policy. Shall develop ICT security awareness program and digital operational resilience trainings as compulsory modules in their staff training schemes.

Article 14	Communication	Financial entities shall have in place communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public as appropriate.
Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	The ESAs shall through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standard.
Article 16	Simplified ICT risk management framework	Articles 4 to 14 of this regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU

Chapter 2: ICT-Related Incidents Management, Classification and Reporting

Article	Category	Procedures
Article 5	Governance and Organisation	The management body of financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to ICT risk management framework. The management body shall, · bear responsibility for managing ICT risks. · put in place policies to ensure high standards of confidentiality, integrity, availability of data. · set clear roles and responsibilities for all ICT related functions. · shall bear responsibility for setting and approving the digital operational resilience strategy and set tolerance limit for ICT risks. · Approve, oversee, review ICT business Continuity Policy, and ICT response and recovery plans. · Approve and review ICT internal audit plan. · Allocate budget to digital operational resilience, ICT skills for staff. · Review arrangement regarding policy on arrangements regarding the use of ICT Services provided by ICT third party service providers. · Be duly informed of ICT third party planned changes and risk analysis. · Be informed of ICT incident's impact, response, recovery, corrective steps · Shall establish role to monitor arrangements. · Members of management body shall keep up to date ICT knowledge, skills
Article 6	ICT risk management framework	· The ICT risk management framework shall include strategies, policies, procedures, protocol and necessary tools to protect ICT information, assets. · Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions according to the three lines of defence model, or an internal risk management and control model. · The ICT risk management framework shall be documented and reviewed at least once a year. · Relevant digital operational resilience testing or audit processes, ICT risk management framework report log shall continuously be monitored. · Formal follow-up process, including rules for the timely verification and remediation of critical ICT audit reviews should be established. ·The digital operational resilience strategy shall include the methods to explain how ICT risk Management framework supports the financial entity's business strategy and objectives. · shall Establish the tolerance limit for ICT risk. · shall set clear security objectives including KPIs, key risk metrics. · shall explain ICT reference architecture and changes needed to reach business objectives. · shall outline mechanism to protect, prevent impacts of ICT related incidents · shall outline digital resilience situation on basis of ICT-related incidents. · shall outline communication strategy in case of ICT related incidents.

		· shall define multi-vendor strategy showing ICT Dependencies · Financial entities as per National and European sectoral legislation may outsource and be fully responsible for the tasks of verifying compliance with the ICT risk Management requirements
Article 7	ICT Systems, protocols and tools	ICT systems, protocols and tools are, · appropriate to the magnitude of operations to conduct of activities (Proportionally) · reliable · equipped with sufficient capacity to accurately process the data. · technologically resilient to adequately deal with information processing needs under stressed market conditions
Article 8	Identification	Financial entity, · shall perform risk assessment to map ICT asset with cyber threats. · shall map information assets those considered critical. · shall conduct specific ICT risk assessment on legacy ICT system atleast yearly before and after connecting technologies, application, or systems
Article 9	Protection and Prevention	Financial entities shall use ICT solution and processes that, · ensure the security of the means of transfer of data. · minimise risk of corruption of data. · prevent breaches of confidentiality, impairment of integrity of data · ensure that data is protected from risks arising in data management. · develop and document information security policy for patches, updates · following a risk-based approach establish a sound network and infrastructure management. · implement policies and protocols based on strong authentication mechanisms. · Implement documented policies, procedures, to ensure that all changes to ICT system are recorded, tested, assessed, approved, implemented, and verified in a controlled manner. · have comprehensive documented policies for patches, updates.
Article 10	Detection	The detection mechanisms shall, · Enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, automatic alert mechanism for relevant staff in charge of ICT-related incident response · Financial entities shall devote sufficient resources and capabilities to monitor user activity occurrence of ICT anomalies and cyber attacks. · have in place systems to check trade reports, identify omissions and errors
Article 11	Response and recovery	Financial entities shall implement ICT Business Continuity Policy through dedicate appropriate, documented arrangements, plans, procedures, and mechanism aim to, · ensuring continuity of financial entity's critical and important functions. · quickly, effectively responding and resolving all ICT related incidents. · activating tailored response-recovery procedures for ICT-related incident. · estimating impacts, damages, losses. · setting out communication and crisis management action. · Financial Entities shall be enabled to independent internal audit reviews. · Financial entities shall maintain appropriate ICT business Continuity plans. · Shall conduct Business Impact Analysis for severe business disruptions. · Business impact analysis shall consider criticality of identified and mapped functions, supporting functions.
Article 12	Backup Policies, restoration and recovery methods	The activation of backup system shall not jeopardize the security of networks. · Financial entities shall use ICT systems that are physically, logically segregated from the source ICT system. · Financial entities shall maintain at least one secondary processing site appropriate to ensure business needs. The secondary processing site shall be Located at a geographical distance from the primary processing site · providing the level of services necessary to ensure that financial entity performs its critical operations within the recovery objectives. · immediately accessible to financial entity's staff to ensure continuity of critical functions. · Financial entity shall consider impact of recovery time and point objective of

		each function on market efficiency. · Financial entities when Reconstructing data from external stakeholders, recovering from ICT-related incident shall perform necessary checks and reconciliation checks.
Article 13	Learning and evolving	The post ICT related incident reviews shall determine whether the established procedures were followed, and the actions taken were effective, including in relation to: · Promptness in responding to security alerts and determining impact of ICT related incidents and their severity. · Quality and speed in performing forensic analysis. · Effectiveness of incident escalation within the financial entity. · Effectiveness of internal and external communication. ICT risk assessment framework shall have components to review lessons derived, · from the Digital Operation resilience testing, · from ICT related incidents · from challenges faced upon activation of ICT business continuity plans and ICT response and recovery plans · from Information exchanged with counterparties and assessed during supervisory review · Financial entities shall monitor effectiveness of implementation of their resilience, strategy. Shall map the evolution of ICT risks over time, analyse the frequency, types, magnitude and evolution of ICT risks related incidents, in particular cyber-attacks and their patterns. Shall monitor relevant technological developments, ICT security requirements. · Senior ICT Staff shall review report at least yearly with management body.
Article 14	Communication	Financial entities shall consider the need to keep communication active between staff involved in the ICT risk management, response and recovery and external stakeholders. Atleast one person within the entity shall be tasked with implementing the communication strategy for ICT related incidents and fulfilling public and media function for that purpose.
Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies	The common draft regulatory technical standards for following purpose: · Specify elements to be included in ICT security policies, procedures, protocols, tools to ensure security of networks, to enable adequate safeguards against intrusions and data misuse, preserve the confidentiality, integrity, and availability of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and delays. · To develop components of the controls of access management rights. · To develop further elements for prompt detection of anomalous activities, criteria triggering ICT-related incident detection and response processes. · Specify further the components of the ICT business continuity policy. · Specify testing of ICT business continuity plans with qualitative scenarios · Specify further components of ICT response and recovery plans. · Specify content and format for report of ICT risk management framework. · When developing draft regulatory standards, the ESAs shall consider proportionality principle. · About when ESAs shall submit draft regulatory technical standards
Article 16	Simplified ICT risk management framework	Financial entities - Payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU, shall, · Put in place and maintain a documented ICT risk management framework that details mechanisms and measures aimed at a quick, efficient and comprehensive management of all ICT risks, for protection of relevant physical components and infrastructures. · Continuously monitor the security and functioning of all ICT systems. · minimize impact of ICT risks using sound, resilient, updated ICT systems, protocols and tools - appropriate to support the performance of entity's activities, provision of services and protect integrity and availability of data network and information systems. · Allow sources of ICT risk and anomalies in the network and information

		systems promptly identified, detected and ICT incidents swiftly handled. · Identify key dependencies on ICT third-party service providers. · ensure the continuity of critical and important functions, through business continuity plan, response-recovery measure, backup-restore measures. · test on a regular basis the plans and measures · implement, operational conclusions resulting from tests from post incident analysis into ICT risk assessment process and develop as per ICT risk profile. Initiate ICT security training and awareness programs for staff, management · risk management framework shall be documented reviewed periodically. · Submit to competent authority Report on ICT risk management framework. · The ESAs shall develop draft technical standards for following purpose: - specify elements to be included in ICT risk management framework - specify elements to minimize impact of ICT risks, integrity, availability, confidentiality of data - specify components of ICT business continuity plans - specify accepted quality on testing of Business continuity plans scenarios - specify content and format of report for ICT risk management framework risk - Shall consider size, nature, scale, and overall risk profile of financial entities - When ESAs shall submit those draft regulatory standards to the commission

Chapter 3: Digital Operational Resilience Testing

Article	Category	Policies
Article 17	Classification of ICT-related incidents and cyber threats	Financial entities shall classify threats as significant based on the criticality of 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 18	Harmonisation of reporting content and templates	
Article 19	Centralisation of reporting of major ICT-related incidents	The ESA 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 EY 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 20	Supervisory Feedback	Without prejudice to the technical input, advice or remedies and subsequent follow-up which may be provided, in accordance with national law by the national Computer Security Incident Response Teams pursuant to the tasks foreseen in Article 9 of Directive (EU) 2016/1148
Article 20a:	Operational or security payment-related incidents concerning credit institutions, payment institutions, account information services providers, and electronic money institutions.	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 credit institutions, payment institutions, account information service providers, and electronic money institutions.

Article	Category	Procedures
Article 17	Classification of ICT-related incidents and cyber threats	Financial entities shall classify ICT-related incidents and impact based on following criteria · number and/or relevance of financial counterparts, number of transactions affected and if the ICT related incident has caused reputational impact · duration of the ICT-related incident, including the service downtime · geographical spread of ICT related incident, particularly if it affects more than two member states · data losses that the ICT-related incident entails, such as confidentiality, integrity or availability loss · criticality of services affected · economic impact, I,e in absolute and relative terms, direct and indirect costs and losses The ESAs shall, through the Joint Committee and in consultation with the European Central Bank (ECB) and ENISA, develop common draft regulatory technical standards specifying the following, · the criteria set out for materiality thresholds for determining ICT-related incidents, major operational, security payment related incidents objections · ESAs shall consider the criteria, international standards, guidance and specifications developed and published by ENISA · ESAs shall duly consider the need for microenterprises, small and medium-sized enterprises to mobilise sufficient resources to ensure ICT-related incidents are managed swiftly. · About when The ESAs shall submit common draft regulatory technical standards to the commission
Article 18	Harmonisation of reporting content and templates	The ESAs, through the Joint Committee and in consultation with ENSIA and the ECB shall develop: · Common draft regulatory technical standards considering to, - establish the content of the reporting for major ICT-related incidents and incorporate elements for relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not: - determine the time-limits for the initial notification - establish the content of the notification for significant cyber threats. When developing draft regulatory technical standards, the ESAs shall consider proportionality principle. The ESAs shall, provide justification when deviating from the approaches taken in the context of NIS Directive · 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. Power is delegated to commission to supplement this Regulation by adopting the common regulatory technical standards considering articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010, respectively. Power is conferred on the commission to adopt the common implementing technical standards considering Article 15 of Regulations (EU) No 1093/2010, (EU) No 1095/2010 and (EU) No 1094/2010.
Article 19:	Centralisation of reporting of major ICT-related incidents	The report shall comprise atleast the following elements: · Prerequisites for the establishment of a single EU Hub · benefits, limitations and risks including risks associated with high concentration of sensitive information - the needed capability to ensure interoperability with regard to other relevant reporting schemes · elements of operational management · conditions of membership

		· modalities for financial entities and national competent authorities to access the single EU Hub. · a preliminary assessment for financial costs entailed by the setting-up the operational platform supporting single EU Hub including required expertise.
Article 20:	Supervisory Feedback	The competent authority shall, upon receipt of each initial notification and reports as referred to in Article 17(3), acknowledge receipt of each initial notification and reports as referred to in Article 17(3) acknowledge receipt of notification and may, where feasible, provide in a timely manner relevant and proportionate feedback or high-level guidance to the financial entity, in particular to make available any relevant anonymised information and intelligence on similar threats, discuss remedies applied at the level of the entity 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 and consequences of the ICT-related incidents reported pursuant to Article 17(1) The ESAs shall, through the Joint Committee, report yearly on an anonymised and aggregated basis on the major ICT-related incidents, the details of which are provided by competent authorities in accordance with Article 17(5) setting out at least the number of major ICT-related incidents, their nature, impact on the operations of financial entities or clients, costs and remedial actions taken The ESAs shall issue warning and produce high-level statistics to support ICT threat and vulnerability assessments
Article 20a:	Operational or security payment-related incidents concerning credit institutions, payment institutions, account information services providers, and electronic money institutions.	

Chapter 4: Managing of ICT Third Party Risk

Article	Category	Policies
Article 21	General requirements for the performance of digital operational resilience testing	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 microenterprises shall, consider the criteria, establish, maintain and review, a sound a comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework
Article 22	Testing of ICT tools and systems	
Article 23	Advanced testing of ICT tools, systems and processes based on threat led penetration testing	Financial entities shall carry out every 3 years advanced testing by means of TLPT. Based on the risk profile considering operational circumstances, the competent authority may request financial entity to reduce or extend this frequence. Each threat led penetration test shall cover important functions and services of financial entity, and shall be performed on live production system supporting such functions. The precise scope of threat led penetration testing shall be determined by financial entities and shall be validated by the competent authorities.

Article 24	Requirements for testers for the development of threat led penetration testing	
Article 25	General Provisions: Key Principles for a sound management of ICT Third Party Risk	
Article 26	Preliminary assessment of ICT concentration risk	
Article 27	Key Contractual Provisions	The rights and obligations of the financial entity and the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall be documented in one written/printable/downloadable document and include the service level agreements.
Article 28	Designation of critical ICT third-party service providers	
Article 29	Structure of the oversight framework	The Joint Committee shall establish Oversight Forum as a subcommittee for the purpose of supporting work of Joint Committee and lead Overseer, in area of ICT third-party risk across financial sectors. The Oversight Forum shall, regularly discuss relevant developments on ICT risks and vulnerabilities and promote concise approach in monitoring of ICT third-party risk at Union scale
Article 30	Task of the Lead Overseer	The Lead Overseer shall conduct the oversight of assigned critical ICT third-party service providers and shall be the primary point of contact for those critical ICT third-party service providers. 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.
Article 31	Powers of the Lead Overseer	The Lead Overseer shall have the following powers: - To request all relevant documentation in accordance with Article 32 - To conduct general investigations and inspections as per Articles 33 and 34 - To request reports after completion of Oversight activities specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers.
Article 32	Powers of the Lead Overseer outside the union	When oversight objectives cannot be attained by means of interacting with the subsidiary setup or by exercising oversight activities on premises located in a third-country recommendations to be provided.
Article 33	Request for Information	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 has outsourced operational functions or activities.
Article 34	General Investigation	To carry out its duties under this Regulation, Lead Overseer, assisted by Joint Examination team may conduct the necessary investigations of critical ICT third-party service providers.
Article 35	Inspections	To carry out its duties under this Regulation, the Lead Overseer, assisted by the Joint Examination teams 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, operations centers, secondary premises, as well as to conduct off-line inspections. For the purposes of exercising the powers, the Lead Overseer shall consult the Joint Oversight Network.
Article 36	Ongoing Oversight	· Where conducting oversight activities notably general investigations or inspections, the Lead Overseer shall be assisted by a joint examination team established for each critical ICT third party service provider.
Article 37	Harmonisation of conditions enabling the conduct of the oversight	Recommendations for the ESAs shall to develop draft technical standards
Article 38	Follow-up by competent authorities	Within 60 calendar days after the receipt the recommendations issued by the Lead Overseer critical ICT third-party service providers shall either notify the

Commented [SD1]: To be improvised

		Lead Overseer on their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations. The Lead Overseer shall immediately transmit this information to competent authorities of the financial entities concerned.
Article 39	Oversight Fees	The Lead Overseer shall, in accordance with the delegated act, charge critical ICT third-party service providers fees that fully cover the Lead Overseer's necessary expenditure including the reimbursement of any costs, as well as including the cost of advice provided by the independent experts in relation to matters falling under the remit of direct Oversight activities.
Article 40		

Article	Category	Procedures
Article 21	General requirements for the performance of digital operational resilience testing	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 · Financial entities shall follow a risk-based approach considering criteria referred to in Article 3a(2) when conducting the digital operational resilience testing programme, duly considering 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 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. · shall establish procedures and policies to prioritise, classify and remedy all issues acknowledge throughout the performance of the tests. · shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed. · shall ensure that appropriate tests are conducted on all critical ICT systems and applications at least yearly.
Article 22	Testing of ICT tools and systems	The digital operational resilience testing programme shall provide, for the execution of appropriate tests, 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 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. Microenterprises shall perform the tests 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	Advanced testing of ICT tools, systems and processes based on threat led penetration testing	Financial entities shall identify all ICT processes, systems and technologies supporting functions and ICT services, including important functions outsourced or contracted to ICT third party service providers. the financial entity and the ICT third-party service provider may agree in writing 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 arrangement with an external tester, for purpose of conducting, under the

		direction of one designated financial entity - 'Pooled Testing'. The pooled testing shall be considered as threat led penetration testing carried out by respective pooled financial entities. Financial entities shall, with the cooperation of ICT third-party service providers, including the testers but excluding the competent authorities, apply effective risk management controls to mitigate the risks of any potential impact on data, damage to assets and disruption to critical or important functions, services or operations at the financial entity itself, its counterparties or to the financial sector. At the end of the test, financial entity and external testers shall provide to authorities a summary of the relevant findings, remediation plans and documentation demonstrating that the threat led penetration testing has been conducted in accordance with the requirements. Those authorities shall provide financial entities with an attestation to allow for mutual recognition of threat led penetration tests between competent authorities. The financial entity shall share the attestation, the summary of relevant findings and the remediation plans with relevant competent authority. Competent authorities shall identify financial entities required to perform threat led penetration testing considering the criteria based on the assessment of the following: · impact-related factors, in particular the criticality of services provided, and activities undertaken by the financial entity. · possible financial stability concerns, including the systematic character of the financial entity at national or Union level, as appropriate. · Specific ICT risk profile, level of ICT maturity of the financial entity or technology features which are involved. Financial entity shall contact testers to perform penetration led testing The ESAs shall in agreement with the ECB, develop joint draft regulatory technical standards in accordance with TIBER-EU framework to specify further. · the criteria used for the purpose of the application. · the requirements and standards governing the use of internal testers. · the requirements in relation to: - the scope of threat led penetration testing - the testing methodology and approach to be followed for each specific phase of the testing process - the results, closure, and remediation stages of the testing · the type of supervisory and other relevant cooperation needed for the implementation of threat led penetration testing 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 sector
Article 24	Requirements for testers for the development of threat led penetration testing	Financial entities shall only use testers for the deployment of threat led penetration testing which: · are of the highest suitability and reputability · possess technical and organisation capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing. · are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks. · 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. · are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence. · The use of internal testers shall be subject to following conditions. - Their use has been approved by the relevant competent authority or respectively by the single public authority. - The relevant competent authorities have verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are

		avoided throughout the design and execution phases of the test - the threat intelligence provider is external to the financial entity · Financial entities shall ensure that contracts concluded with external testers require a sound management of the threat led penetration testing results that any processing thereof including any generation, draft, store, aggregation, report, communication or destruction do not create risks to the financial entity.
Article 25	General Provisions – Key Principles for a sound management of ICT third party Risk	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 that have in place contractual arrangements for the use of ICT services to run their business operations shall remain fully responsible for complying with and discharge of all obligations under this Regulation. · Financial entities management of ICT third party risk shall be implemented in light of the principle of proportionality, considering - the nature, scale, complexity and importance of ICT-related dependencies - the risk 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 availability of financial services and activities, at individual and at group level. · As part of ICT risk management framework, financial entities shall review a strategy on ICT Third party risk, considering multi-vendor strategy, if applicable. The strategy shall include a policy on the use of ICT services concerning critical or important functions provided by ICT third-party service providers. The management body on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services shall regularly review the risks identified in respect to contractual arrangements on the use of ICT services concerning critical or important functions. As part of ICT risk management framework, financial entities shall maintain and update an entity level, 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 shall be documented distinguishing between those cover critical or important functions and those that do not, and should made available upon request and inform about any planned contractual arrangement on use of ICT services to competent authority. · Before entering into a contractual arrangement on the use of ICT services, financial entities shall: - assess whether the contractual arrangement covers the use of the ICT services concerning a critical or important function, - assess if supervisory conditions for contracting are met; - identify and assess all relevant risks in relation to the contractual arrangement, including possibility that such contractual arrangements may contribute to reinforcing ICT related concentration risk. - undertake all due diligence throughout selection and assessment processes that ICT third-party service provider is suitable - identify and assess conflicts of interest that the contractual arrangement may cause. Financial entities shall, · prior to concluding the arrangement take into consideration the use of ICT third party service providers of the most up-to-date and highest information security standards. · verify that auditors, whether internal or external auditors or pool of auditors posses appropriate skills and knowledge to effectively perform relevant audits and assessments. · ensure that contractual arrangements on the use of ICT services may be terminated at least under the following circumstances:

		- significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms - identified 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. - ICT Third party service provider's evidenced weaknesses pertaining to the overall ICT risk management, security and integrity of confidential personal, sensitive data - where the competent authority can no longer effectively supervise the financial entity as result of respective contractual arrangement · For ICT services related to critical or important functions, financial entities shall put in place, exit strategies. · The exit strategies shall consider risks, a possible failure, a deterioration of quality of functions proved, any business disruption due to failed provision of services or material risk arising in relation to appropriate and continuous deployment of the function, or in event of termination of contractual arrangements with ICT third-party service providers. Financial entities shall ensure that they are able to exit contractual arrangements without: - disruption to their business activities - limiting compliance with regulatory requirements - detriment to the continuity and quality of services, exit plans shall be comprehensively documented, tested, reviewed periodically · Financial entities shall identify alternative solutions and develop transition plans to remove the contracted functions and sensitive data from ICT Third party service provider and incorporate them in-house · Financial entities shall take measures to main business continuity · The ESAs shall develop implementing technical standards templates for information registry common to all contractual arrangements of ICT services
Article 26	Preliminary assessment of ICT concentration risk	· When performing the identification and assessment of ICT concentration risk financial entities shall take into account whether the conclusion of contractual arrangement in relation to ICT services supporting critical would lead to following circumstances, - contracting is not easily substitutable - having in place multiple contractual arrangements in relation to the provision of ICT services. Financial entities shall weigh the benefits and costs of alternative solutions and consider how envisaged solutions match the business needs and objectives set out in their digital resilience strategy. · Possibility of ICT services supporting critical or important functions includes possibility of subcontracting. · Financial entity shall consider the insolvency law provisions that would apply in the event of the ICT-Third party service provider's bankruptcy and constraint that may arise in respectto the urgent recovery of the financial entity's data. · Financial entity shall consider the respect of Union protection rules and the effective enforcement of the law · Financial shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and ability of the competent authority to effectively supervise the financial entity.
Article 27	Key Contractual Provisions	The contractual arrangements on the use of ICT services shall include at least the following: · a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating conditions applying to subcontracting if permitted · the locations, namely the regions or countries where the contracted or subcontracted functions ICT services, data are to be provided and is to be processed, including storage location, and the requirements for the ICT third-party service provider to notify in advance the financial entity if it envisages changing such locations.

		· provisions on accessibility, availability, integrity, security, confidentiality and protection of data, including personal data. - 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 business operations of the ICT third party service provider, or in case of termination of the contractual arrangements - Full service level descriptions, including updates and revisions with qualitative, quantitative performance targets to allow an effective monitoring by the financial entity and enable appropriate corrective actions when agreed service levels are not met; - 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 - 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 that provide an appropriate level of secure provision of services by the financial entity in line with its regulatory framework. - the obligation of 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, 24. - The right to monitor on an ongoing basis the ICT third-party service provider's performance + unrestricted rights of access, inspection and audit by financial entity + the right to agree on alternative assurance levels if other client's rights are affected + the commitment by the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, led overseer, financial entity or an appointed third party and details on the scope, modalities and frequency of such inspections and audit - exit strategies, in particular the establishment of a mandatory adequate transition period: + during which ICT third-party service provider will continue providing respective functions or ICT services with a view to reduce the risk of disruptions at financial entity or to ensure its effective resolution and restructuring: + which allows financial entity to migrate to another ICT third-party service provider or to in-house solutions consistent with complexity of provided services. · When negotiating contractual arrangements, financial entities, ICT third-party service providers shall consider use of standard contractual clauses developed by public authorities for specific services · The ESAs shall through the Join Committee develop draft regulatory technical standards to specify further the elements which a financial entity needs to determine and assess when subcontracting critical or important functions.
Article 28	Designation of critical ICT third-party service providers	· The ESAs through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall: - designate the ICT third-party service providers that are critical for financial entities, following an assessment. - Appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible in accordance with Regulations (EU) No 1093/2010, (EU) No 1094/2010 or (EU) No 1095/2010 · The designation of third-party service provider being critical shall be based on all of the following criteria in relation to ICT services provided by an ICT third-party service provider: - 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.

		- the systemic character on importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the following parameters: + 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 interdependence between the G-SIIs or O-SIIs referred to in point 1 and other financial entities including situations where the G-SIIs or O-SIIs provider financial infrastructure services to other financial entities: · Irrelevance of subcontracting arrangements, reliance of financial entities on services provided by relevant ICT third-party service provider. · the degree of substitutability of the ICT third-party service provider, taking into account the following parameters, - the lack of real alternatives - difficulties to partially or fully migrate the relevant data and workloads due to significant financial costs, time or other type of resources that the migration process may entail. · Critical ICT third-party service providers which are part of a group shall designate one legal person as coordination point to ensure adequate representation and communication with the lead overseer · The Lead Overseer shall notify the ICT third-party service provider of the out come of the assessment leading to designation within 6 weeks from the date of notification. The lead Overseer shall consider the reasoned statement to be submitted within 30 calendar days. After designating a ICT third-party service provider as critical the ESA's through the Joint Committee shall notify the ICT third-party about designation and about starting date as from which they will be effective subject to oversight activities. · The designation mechanism shall not be used until the commission has adopted a delegated act. The designation mechanism shall not apply in relation to: - Financial entities providing ICT services to other financial entities. - ICT Third-party service providers that are subject to oversight frameworks referred in Article 127(2) of the Treaty on the Functioning of the European Union. - ICT infra-group service providers - ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State. · The ESAs shall establish, publish and yearly update the list of critical ICT third-party service providers at Union Level · The ICT third-Party service providers that are not included in the list may request to be designated as critical by submitting a reasoned application to EBA, ESMA or EIOPA which through the Joint Committee, shall decide whether to designate that ICT third-party service provider as critical.
Article 29	Structure of the oversight framework	· The Oversight Forum shall on a yearly basis, undertake collective assessment, promote co-ordination measures to increase the digital operational resilience of financial entities, foster best practices on addressing ICT concentration risk and explore mitigants for cross-sector risk transfers · The Oversight Forum shall submit comprehensive benchmarks of critical ICT third-party service providers to be adopted by the Joint Committee as joint positions of the ESAs · The oversight Forum shall be composed of: - the Chairpersons of the ESAs - 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 ESRB, ECB and ENISA as observers

		- where appropriate, one additional representative of competent authority from each member state as observer - where applicable one representative of national competent authorities responsible from the supervision of an operator of essential services or digital service provider which has been designated as a critical ICT third-party service provider as observer The oversight forum may, where appropriate, seek the advice of independent experts appointed. · The ESAs shall publish on their website the list of high-level representatives designated by Member States · The independent experts shall be appointed on the basis of their expertise on financial stability, digital operational resilience and ICT security matters. · 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. · The ESAs, through the Joint committee and based on preparatory work conducted by the Oversight Forum, shall present yearly the European Parliament, the Council and the commission a report on the application of this Section.
Article 30	Task of the Overseer	· The assessment shall include: - ICT requirement 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 confidentiality, integrity and availability of data. - The physical security contributing to ensuring the ICT security, including the security of premises, facilities, datacenters. - the risk management processes, including ICT risk management policies, ICT business continuity and ICT response and recovery plans - the governance arrangements, including an organisational structure with clear transparent and consistent lines of responsibility and accountability rules enabling an effective ICT risk management - The identification, monitoring and prompt reporting of major ICT-related incidents to the financial entities, the management and resolution cyber attacks - the mechanisms for data profitability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities; - testing of ICT systems, infrastructure and controls - ICT audits - Use of relevant national and international standards applicable to the provision of its ICT services to the financial entities · Based on the assessment, the lead overseer in coordination with Joint Oversight Network 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. Prior to adoption of the oversight plan, the Lead Overseer shall communicate the draft Oversight plan to the critical ICT third-party service provider. Upon receipt of the draft Oversight Plan, the critical ICT third-party service provider may submit a reasoned statement within 15 calendar days evidencing expected impact on customers not subject to this regulation and where appropriate, formulating solutions to mitigate risks.
Article 31	Powers of the lead Overseer	· The Lead Overseers shall also have, power to address recommendations concerning the following: - 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.

		- the use of conditions and terms, including their technical implementation, under which the critical ICT third-party service providers provide services to financial entities, - upon the examination of any planned subcontracting, including 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. · When exercising the powers, Lead Overseer shall: - Ensure regular coordination with the Joint Oversight Network, and in particular seek as appropriate consistent approaches with regard to the oversight of critical ICT third-party service providers. - Take due account of framework, consult the relevant competent authorities established by that Directive to avoid duplication of technical and organisational measures that might apply to critical ICT third-party service providers pursuant to that directive; - seek to minimise to the extent possible the risk of disruption to services provided by the critical ICT third-party service provider to customer not subject to this regulation. - In the case of whole or partial non-compliance with the measures required the Lead Overseer shall adopt a decision imposing a periodic penalty to compel the critical ICT third-party service provider to comply with those measures. - The periodic penalty payment 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 - When determining the amount of the penalty payment, the Lead Overseer shall take into account the following criteria regarding the non-compliance + The gravity and the duration + whether it has been committed intentionally or negligently + the level of cooperation of the ICT third-party service provider with the Lead Overseer. - Penalty payment shall be of 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 inspection and access shall be carried out. The amounts of the penalty payment shall be allocated to the general budget of the European Union.
Article 32	Powers of the Lead Overseer outside the union	Powers of Lead overseer may be subject to all of the following conditions - the conduction of an inspection in a third-country is deemed necessary by the Lead Overseer to allow it to fully and effectively perform its duties under this Regulation: - the inspection in a third-country is directly related to the provision of ICT services to financial entities in the union - the critical ICT third-party service provider concerned consents to the conduction of an inspection in a third-country - the relevant authority of the third-country concerned has been officially notified by the Lead Overseer and raised no objection thereto. Member states and the Union institution shall conclude with relevant authority of third country concerned administrative cooperation arrangements enabling the smooth conduct of inspections in a third-country by the Lead Overseer and its designated team for its mission in the third country, shall not give rise to any legal obligations. The mechanism for the transmission of any relevant information between EBA, ESMA or EIOPA may be requested by the Lead Overseer
Article 33	Request for Information	When sending a simple request for information, Lead Overseer shall, - Refer to this Article as the legal basis of the request - State the purpose of the request - Specify what information is required - Set a time limit within which the information is to be provided - inform the representative of the critical ICT third-party service provider from whom the information is requested that he or she is not obliged to provide the information but that in case of a voluntary reply to the request the information provided must not be incorrect or misleading.

		· When requiring by decision to supply information, the lead overseer shall - refer to this Article ((EC) No 10602009, (EU) No 6482012, (EU) No 6002014) as the legal basis of the request - State the purpose of the request - Specify what information is required - Set a time limit within which the information is to be provide - indicate periodic penalities - indicate the right to appeal the decision before ESA's board of Appeal and to have the decisions reviewed by the court of justice of European Union in accordance with Article 60 and 61 of Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. · Representatives of critical ICT Third party service providers shall supply the information requested. The critical ICT third-party service provider shall remain fully responsible if the information supplied is incomplete, incorrect or misleading · The lead Overseer without delay, transmit a copy of the decision to supply information to the competent authorities, of the financial entities using the critical ICT third-party providers services and to the Joint Oversight Network
Article 34	General Investigations	The Lead Overseer shall be empowered to: - Examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored. - Take or obtain certified copies of, or extracts from, such records, data, procedures and other materials - summon representatives of the critical ICT third-party service provider for explanations on facts or documents, to the subject matter of an investigation - request records of telephone and data traffic · 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 provided, the legal remedies and the right to have the discussion reviewed by the Court of Justice. In good time before the investigation, the Lead Overseer shall inform competent authorities of the financial entities using that critical third-party service provider of the investigation and of the identify of the authorised persons.
Article 35	Inspections	· The officials and other persons authorised by the Lead Overseer to conduct an on-site inspection shall have the power to: - enter any such business premises, land or property and - seal any such business premises, books or records, for the period of, and to the extent necessary for the inspection. They shall exercise their powers upon production of a written authorization specifying the subject matter and the purpose of the inspection and the periodic penalty payments provided. - In good time before the inspection, the Lead Overseer shall inform the competent authorities of the financial entities using that ICT third-party provider. - Inspections shall cover the full range of relevant ICT systems, network, devices, information and data either used for, or contributing to, the provision of services to financial entities. - Before any planned on-site inspection, the Lead Overseer 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 - 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, legal

		remedies, as well as rights to have the decision reviewed by the court of justice, Regulation (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 - Where the officials and other persons authorised by the lead Overseer find that a critical ICT Third-party service provider opposes an inspection ordered pursuant to this Article, the Lead Overseer shall inform the critical ICT third-party service provider of the consequences of such opposition.
Article 36	Ongoing Oversight	· The joint examination team shall be composed of staff members from: - The ESAs - The relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides services - The national competent authority, on a voluntary basis - One National Competent authority from the Member State where the critical ICT third Party service provider is established on a voluntary basis. Member of the joint examination team shall have expertise in ICT and operational risk. The joint examination team shall work under the coordination of a designated Lead Overseer staff member ('Lead Overseer Coordinator') · Within 3 months after completion of an investigation or inspection, the Lead Overseer shall adopt recommendations to be addressed by the Lead Overseer. · For the purposes of fulfilling the Oversight activities, the Lead 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 37	Harmonisation of conditions enabling the conduct of the oversight	The ESAs shall develop draft technical standards to specify - 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) - the content, structure and format of the information to be submitted, disclosed or reported by the ICT third-party service provider pursuant to Article 31(1), including the template to provide information on subcontracting arrangements + the criteria for determining the composition ensuring a balanced participation of the staff members from the ESAs and from the relevant competent authorities, their designation, tasks and the working arrangements of the joint examination team - the details of the competent authority assessment, based on recommendations provided by the Lead OverSeer
Article 38	Follow-up by competent authorities	The Lead Overseer shall publicly disclose where a critical ICT third-party service provider fails to notify the Lead Overseer in accordance, the information published shall disclose the information published shall disclose information on type of nature of the non-compliance. It shall be limited to what is relevant and proportionate for the 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. Competent authorities shall inform relevant financial entities of the risks identified in the recommendations addressed to critical ICT third-party service. Where a competent authority deems that a financial entity fails to sufficiently address, the risk identified in the recommendations, it shall notify the financial entity of the possibility of a decision being taken, in absence of appropriate contractual arrangements aimed at addressing such risks. Upon receiving the reports and prior to taking any of the decisions, competent authorities may on a voluntary basis, consult the national competent authorities responsible, for the supervision of an operator of essential services.

		Competent authorities may, as a measure of last resort, following the notification 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 service providers have been addressed. Where a refusal by a critical ICT third-party to endorse recommendations is grounded on a divergent approach from the one advised by the Lead Overseer, and this may adversely impact a large number of financial entities, or a significant part of a financial sector providing critical or important functions, and individual warnings issued by competent authorities have not resulted in consistent approaches mitigating the potential risk to financial stability, the Lead Overseer may after consulting the Oversight Forum, issue non-binding and non-public opinions to competent authorities to promote consistent and convergent supervisory follow-up measures, as appropriate. upon receiving the reports, referred to in point (c) of Article 31(1), competent authorities, when taking the decisions, 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: - the gravity and the duration of the non-compliance - 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, - whether financial crime was facilitated, occasioned or otherwise attributable to the non compliance - whether the non-compliance has been committed intentionally or negligently. + whether the suspension or termination introduces a continuity risk for the business operations of the financial entity nothwistanding the latter's efforts to avoid disruption in the provision of its services. + Where applicable, the opinion of the national competent authorities responsible for the supervision of an operator of essential service or a digital service provider, which has been designated as a critical ICT third-party service provider. Competent authorities shall grant financial entities the necessary period of time for the latter to adjust the contractual arrangements with critical ICT third-party service providers to avoid detrimental effects on their digital operational resilience and to allow them to deploy exit strategies and transition plans. + The decision, shall be notified to the members of the oversight forum and the Joint Oversight Network. The critical ICT third-party service providers impacted by the decisions provided shall fully cooperate with the affected financial entities in particular in the context of the process of suspension or termination of their contractual arrangements.
Article 39	Oversight Fees	The Lead Overseer shall, in accordance with the delegated act, charge critical ICT third-party service providers fees that fully cover the Lead Overseer's necessary expenditure including the reimbursement of any costs, as well as including the cost of advice provided by the independent experts in relation to matters falling under the remit of direct Oversight activities. The amount of fee charged in relation to critical ICT third-party shall cover all costs derived from execution of the duties foreseen in this Section and shall be proportionate to their turnover. The commission is empowered to adopt this delegated act in accordance to article 50 by determining the amount of fee and way in which they are to be paid
Article 40	International Cooperation	Without prejudice to Article 31a, 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. 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 focusing 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 5: Information Sharing Arrangements

Article	Category	Policies
Article 40	Information-sharing arrangements on cyber threat information and intelligence	

Article	Category	Procedures
Article 40	Information-sharing arrangements on cyber threat information and intelligence	· 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: - aims at enhancing the digital operational resilience of financial entities, in particular trough raising awareness in relation to cyber threats, limiting or impeding the cyber threats ability to spread, supporting defensive capabilities, threat detection techniques, mitigation strategies or response and recovery stages - takes places within trusted communities of financial entities; - is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules conduct in full respect of business confidentiality, a protection of personal data and guidelines on competition policy · The information sharing arrangements shall define the conditions for participation and where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements on the involvement of ICT third-party service providers, and on operational elements including the use of dedicated IT platforms · Financial entities shall notify competent authorities of their participation in the information-sharing arrangements upon validation of their membership or as applicable of the cessation of their membership once the latter takes effect.

Article	Category	Policies	
5	Governance and Organisation	1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.	
		2. Financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).	

Document Reference link:

https://www.eba.europa.eu/sites/default/files/2024-01/bf5a2976-1a48-44f3-b5a7-56acd23ba55c/JC%202023%2086%20-%20Final%20report%20on%20draft%20RTS%20on%20ICT%20Risk%20Management%20Framework%20and%20on%20simplified%20ICT%20Risk%20Management%20Framework.pdf

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2554

Abbreviations, acronyms

APA	Approved Publication Arrangements
ARM	Approved Reporting Mechanisms
BCBS	Basel Committee on Banking Supervision
BIA	Business Impact Analysis
BIS	Bank for International Settlements
CCP	Central counterparty, as defined under EMIR
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payments and Settlement Systems
CSD	Central securities depositories, as defined under CSDR
DRSP	Data reporting service providers, as defined in MiFID II
ENISA	European Union Agency on Cybersecurity
ESCB	European System of Central Banks

FSB	Financial Stability Board
ICT	Information and Communication Technologies
IOSCO	International Organization of Securities Commissions
ISO	
NCA	