Text of the provisional agreement of the European Parliament and of the Council on the draft Regulation on digital operational resilience for the financial sector. International Bulletin of November 2022.

The provisional agreement on the Regulation on digital operational resilience for the financial sector (the Digital Operational Resilience Act or DORA), between the European Parliament and the Council, took place on 11 May. This Regulation is part of the set of measures on digital finance that the European Commission (EC) published on 24 September 2020, also made up of the following initiatives: a) a new digital finance strategy to advance towards a European financial data space, promote new ways of channelling financing for SMEs and better financial products for consumers; b) a strategy of retail payments to offer secure, fast, reliable and cost-effective payment services; c) a Regulation regarding the crypto-asset markets that are outside the financial services legislation in force in the EU to regulate their issue and related services, the publication of which is expected shortly in the OJEU; and d) a Regulation with a pilot regime that allows temporary exceptions for market infrastructures that wish to trade and settle transactions in financial instruments in the form of crypto-assets based on distributed ledger technology, published in the OJEU of 2 June 2022.

The provisional agreement was published on 23 June on the Council's website and voted on in the Parliament's Economic and Monetary Affairs Committee on 13 July. Next, the formal adoption of the proposed Regulation by the Parliament and the Council will proceed, which each Member State will subsequently incorporate into its legislation. The respective NCAs will supervise compliance and application of the Regulation, without prejudice to the supervision of essential third-party providers of information and communication technology (ICT) services, which will fall to the ESAs in the manner described below.

The proposed Regulation on digital operational resilience aims to ensure that the financial sector in Europe can continue to operate in a resilient manner in the event of a severe operational disruption, so that all businesses need to ensure that they can withstand and respond to and recover from any type of ICT-related disruption and threat. To this end, it establishes uniform requirements for the security of the networks and information systems of financial institutions, as well as essential third-party providers of ICT services (providers of cloud computing services or data analysis services), which will promote IT security in the financial sector. The main aspects of the text of the agreement are the following:

Chapter I General provisions

The text establishes a very broad list that covers almost all entities in the financial sector, which under the name of **"financial entities"**, constitute the subjective scope of application of the DORA Regulation including, by way of example, credit institutions, investment firms, management companies, insurers and crypto-asset, crowdfunding and data supply service providers. Statutory auditors and audit firms will be included in a future review of the Regulation.

In addition, the agreement includes, unlike the EC proposal, a set of cases of non-application, such as natural or legal persons exempted from the application of MiFID or those financial or insurance intermediaries that are micro-enterprises or SMEs.

The agreement adds to the EC proposal a general article on the **principle of proportionality** in order for financial institutions to implement the rules on ICT risk management, incidents, tests and risk management of third parties related to ICT in accordance with this principle taking into account their size, nature, scale and complexity of services, activities and operations and overall risk profile.

For financial entities identified as operators of essential services, this Regulation is considered a sector-specific Union legal act. The interaction with the Cybersecurity Directive is approached from the application of the principle of *lex specialis* being applicable in all matters not provided in this Regulation.

Chapter II ICT risk management

Financial institutions must have internal governance and control requirements that guarantee effective and prudent management of all ICT risks to achieve a high level of operational resilience, assigning responsibility to a **control function** (not mandatory for micro-enterprises) that has an adequate level of independence to avoid conflicts of interest, separate from the general control and internal audit functions.

The management body of the financial institution will define, approve, supervise and be responsible for the application of the **ICT risk management framework** that will form part of the overall risk management system. Specifically, financial institutions must have available: a) mechanisms, subject to periodic testing, to quickly detect anomalous activities, including ICT network performance problems and related incidents to identify possible specific points of significant failure and b) a comprehensive ICT business continuity policy that will form part of the overall BCP. The agreement, once again unlike the EC proposal and in application of the principle of proportionality, incorporates the possibility of a **simplified ICT risk management framework** for several small, non-interconnected financial institutions.

The ESAs, through the Joint Committee, will develop: 1) guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents; 2) draft regulatory technical standards (RTS), in consultation with the European Union Agency for Cybersecurity (ENISA) on a fairly extensive set of regulatory and technical elements to achieve greater harmonisation of ICT risk management tools, methods, processes and policies.

Chapter III Incidents related to ICT: management, classification, and reporting

Financial institutions shall establish an **ICT-related incident management process** that allows an adequate response and the identification of the underlying causes to prevent new incidents while keeping a record of incidents and significant cyber threats. The EC proposal did not include references to cyber threats.

The **classification** of incidents is carried out based on a set of criteria: number of people affected and the reputational impact, duration of the incident and service downtime, geographical extension, data loss, essential nature of the affected services and economic impact. Cyber threats will be considered significant based on the criticality of the services at risk, the number and/or relevance of clients or financial counterparts targeted and geographical spread of the areas at risk. The ESAs, through the Joint Committee and in consultation with the ECB and ENISA, will develop RTS projects to specify a) materiality thresholds to consider a major ICT-related incident; b) the criteria that the NCAs must apply to assess the relevance of an incident for the NCA of another Member State and 3) the materiality thresholds to determine when a cyber threat is significant.

The **notification** of major ICT-related incidents to the NCAs will be made through an initial notification, an intermediate report with updated information and a final report when the cause of the incident is known that, regardless of whether they have adopted mitigation measures, includes an impact analysis with real figures. The NCA will determine the significance of the major incident and assess the possible cross-border impacts and adopt (after coordination with the ESAs and the ECB) all the necessary measures to protect the immediate stability of the financial system.

Significant cyber threats can be reported, voluntarily, when they deem to be relevant to the financial system, service users or clients. In the case of credit institutions classified as significant, the NCA will report serious incidents and significant cyber threats to the ECB. Major incidents that have an impact on the financial interests of clients must be, without undue delay, communicated to clients together with the measures taken to mitigate the adverse effects of the incident.

The ESAs, through the Joint Committee and in consultation with ENISA and the ECB, will prepare: a) draft RTS to harmonize the content and templates of the reports taking into account the principle of proportionality, especially to ensure that the different deadlines for reporting may reflect, as appropriate, the specificities of the financial sectors and b) a report assessing the feasibility of establishing a single EU centre for serious incident reporting. The report will explore how to reduce associated costs and improve supervisory convergence.

Chapter IV Digital operational resilience testing

Financial entities -other than microenterprises- must establish, maintain and review a sound and comprehensive

digital operational resilience testing programme with a risk-based approach as part of the ICT risk management framework to assess incident preparedness and identify gaps in digital operational resilience. The tests will be carried out by independent parties, external or internal, although in the latter case sufficient resources must be dedicated and steps taken to ensure that conflicts of interest are avoided during the design and execution phases of the test. Testing may include, for example, vulnerability assessments and scans, open-source analysis, network security assessments, gap analysis, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based testing, compatibility testing, performance testing, end-to-end testing, or penetration testing. CSDs and CCPs shall conduct vulnerability assessments prior to deploying or re-deploying new or existing services that support critical functions, applications, and infrastructure. Micro-enterprises will test by combining a risk-based approach with strategic planning, balancing resources and time spent with urgency, type of risks, importance of assets/services, or other significant factors.

Financial entities – other than micro-enterprises and those subject to a simplified ICT risk management framework – will carry out, at least every three years, **threat-led penetration testing**. The NCA may request the financial entity to reduce or increase this frequency and identify the entities that must carry out the tests after evaluating the criticality of the services, impact on financial stability and ICT risk profile. The test will cover essential functions and services and will be carried out on the production systems that support them; the specific scope will be determined by the entity and validated by the NCA.

In the case of outsourced services, measures will be taken to ensure the participation of third-party providers. When internal testers are used, they must hire an external tester every three tests, although significant credit institutions will only use external testers. Member States may designate a single financial sector authority responsible for matters related to penetration testing.

The ESAs, after consulting the ECB and in accordance with the TIBER-EU framework, will develop draft RTS to specify: a) the criteria of financial stability and the systemic nature of the entity as determinants of the performance of the penetration tests and the requirements of internal testers; b) the requirements of the scope of the tests, the methodology of each phase and the results and adoption of corrective measures; and c) the type of supervision and other significant cooperation between NCAs for the implementation and mutual recognition of such tests.

Chapter V Management of ICT third-party risk

ICT-related third-party risk is one of the integral elements of the ICT risk management framework, subject to the principles of responsibility of financial institutions and proportionality. Financial institutions: a) must adopt a **strategy** taking into account the provision of essential services by third parties or multiple providers (except micro-enterprises or those with a simplified management framework); b) must maintain and update an **information record** with all contractual agreements on the use of ICT services provided by third-party providers, which will clearly distinguish whether they constitute critical or important services or not and 3) must inform the NCA of the agreements, in particular if they are related to critical or important functions, and will make the record available to it.

The proposal includes a set of ex ante requirements for contractual agreements with third-party providers, such as evaluating whether the conditions for supervision are met and analysing the possible reinforcement of ICT concentration risk, as well as certain circumstances that end the agreement, notably the NCA’s no longer being able to effectively supervise the financial institution because of the agreement.

Financial institutions must have **exit strategies** of third-party providers that consider the risks that may arise – such as failures, deterioration of the quality of the service or any disturbance of the activity due to lack or inadequate provision of the service.

The ESAs, through the Joint Committee, will develop draft RTS in relation to the registration of information and on the policy to be followed in the contractual agreements on the use of ICT services concerning critical or important functions provided to ICT of third-party service providers.

Referring to **outsourcing**, where the contractual agreement includes the possibility for the third-party provider to subcontract, in turn, a critical or important function to other third parties, the benefits and risks must be weighed in the case of an ICT subcontractor established in a third country. In the latter case, the rules on insolvency, respect for data protection rules and the guarantees of effective compliance with the legislation in the third country will be taken into account. The ESAs, through the Joint Committee, will specify the elements that must be taken into account to assess the subcontracting of critical or important functions.

The ESAs, through the Joint Committee and on the recommendation of the Oversight Forum, will designate: a) the critical third-party providers of ICT services for financial institutions, in accordance with the criteria established in the Regulation (systemic nature, interdependence, degree of substitutability, etc.); b) a Lead Overseer – which will be ESMA, EBA or EIOPA – for each critical third party provider of ICT services, depending on whether the largest share of total assets out of the value of total assets of the financial entities using the services of the relevant critical ICT third-party service provider according to the individual balance sheets of those financial entities and c) they will notify to the third party provider the date from which they will be subject to supervision.

Supervision (assessment of standards and procedures to manage ICT risks) will focus on third-party providers that perform critical or important functions or services for financial institutions and, when necessary, it will be extended to other non-critical functions. Based on this assessment and after coordination by the Joint Oversight Network, the Lead Overseer will adopt an **individual supervision plan** clear, detailed and reasoned description of the annual supervision objectives and the main supervisory actions planned for each essential third-party provider of ICT services. In particular, the Lead Overseer will prepare a series of recommendations (and, among them, the prohibition of entering into an additional subcontracting agreement in certain circumstances) for third-party providers and will inform the NCA and the financial entities of the risks identified and of the measures taken by third parties.

The Joint Committee will establish the **Oversight Forum** as a permanent subcommittee in order to support the work of the joint committee and the main supervisor formed by: i) the chair persons of the ESAs, ii) a high-level representative of the CA of each Member State, iii) executive directors of the ESAs, a representative of the EC, the ESRB (European Systemic Risk Board), the ECB and ENISA as observers, iv) an additional representative of the NCA of each Member State as an observer, v) a representative of the NCAs appointed to the identification of operators of essential services in accordance with Directive 2016/1148. Furthermore, to move towards greater s**upervisory convergence**: a) the Senior Supervisor may, after consulting the Oversight Forum, issue **non-binding opinions** and non-public to the NCAs to promote consistent and convergent supervisory monitoring measures and b) the three ESAs will establish a **joint oversight network** to coordinate in the preparatory stages and in carrying out supervisory activities, with the aim of adopting overall coordinated supervisory strategies. The ESAs, through the Joint Committee, will prepare draft RTS to specify a set of conditions (information to be provided by the essential third-party provider, details of the NCA evaluations, etc.) that allow greater harmonisation of supervision.

Chapter VI Information sharing arrangements

The text envisages financial entities entering into information exchange agreements in relation to information on cyber threats to improve digital operational resilience, especially through awareness, limitation of propagation capacity, support for defensive capabilities, detection techniques, mitigation strategies or response and recovery phases.

Chapter VII Competent Authorities

Without prejudice to the provisions of the supervision framework for essential third-party providers of ICT services, the NCAs are the authorities designated in the different legal acts of the European financial sector for each type of financial institution included in the subjective scope of this Regulation.

Useful link:

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 (DORA)