Joint ESA public consultation on the first batch of draft technical standards for the development of Regulation 2022/2554 on digital operational resilience of the financial sector (DORA)

Links to the papers:

Consultation paper on draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under article 15 and 16.3 of Regulation 2022/2554

Consultation paper on draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation 2022/2554

Consultation paper on draft Implementation Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third party service providers as mandated by Regulation 2022/2554

Consultation paper on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandate by Regulation 2022/2554

1.- Target audience (potential stakeholders):

This consultation is aimed to all market participants, including third-party ICT (information and communications technology) service providers supplying the latter to financial institutions.

The CNMV would appreciate if all the above-mentioned potential stakeholders could send a copy of their responses to the consultation to the following e-mail address: Documentosinternacional@cnmv.es

2.- Information Note

On 19 June 2023, ESMA published four public consultations regarding a projects portfolio on technical standards for the development of Regulation 2022/2554 on digital operational resilience of the financial sector (DORA).

1) Public consultation on the project for regulatory technical standards to achieve greater harmonisation of tools, methods, processes, and risk management related to ICT, in line with Articles 15 and 16.3 of Regulation 2022/2554.

ESAs merged the term under Articles 15 and 16.3 given their interrelation to address ICT risk management frameworks in a comprehensive manner.

The technical standards for the development of Article 15 (general framework of risk management related to ICT) specify the requirements that all financial entities must comply in relation to the following:

i) ICT security policies, procedures, protocols and tools, including ICT governance, risk management and asset management requirements, encryption and cryptography techniques, ICT operational security, network security, project and change management, physical security and security awareness/training;

ii) Human resources policy and the new components of controls on logical and physical access management rights to information and ICT assets;

iii) Mechanisms to quickly identify anomalous activities and criteria to activate ICT-related incident detection processes and the corresponding response plans; and

iv) ICT business continuity policy.

Additionally, the content and format of the report on the review of the risk management framework for ICT to be carried out at least annually (periodically in the case of micro-enterprises) or in case of serious incidents is specified.

Such technical standards are additional to the requirements set in Articles 5-16 of the DORA Regulation and, therefore, should be read jointly.

The technical standards for the development of Article 16 (simplified ICT risk management framework) apply only to five categories of financial entities: Small and non-related ESIs, payment institutions exempted under Directive 2015/2366, entities exempted under Directive 2013/36 in cases where the Member State has not implemented the option in Art. 2.4 (exclude from the scope of application), exempted electronic money institutions confirming Directive 2009/110 and small occupational pension funds. These technical standards complement the requirements set in Article 16 in the following areas: ICT risk management framework, system elements, protocols and tools to reduce ICT risks, ICT business continuity policy and risk management review report.

In regards to the principle of proportionality, ESMA's proposal combines the two legislative policy options described in the draft impact assessment: option A for the general risk framework: a general principle (taking into account elements of complexity or risk) applicable to all financial entities under the scope of the DORA Regulation, while not subject to Article 16 to make the proportionality assessment; and option B for the simplified risk management framework: identify specific requirements to be applied differently, for example, review frequency or different levels of detail to be included in ICT policies or procedural aspects.

<u>Public consultation on the project of regulatory technical standards to specify the criteria for the classification of ICT related incidents, materiality thresholds to establish major incidents and significant cyber threats under Regulation 2022/2554 (Art. 18.3).</u>

Technical standards establish harmonised requirements for financial entities regarding:

i) Criteria for the classification ICT related incidents by financial entities;

ii) Criteria and materiality thresholds to establish major incidents related to ICT which financial entities must notify of to the competent authorities;

iii) Criteria and materiality thresholds to apply when classifying major or significant cyber threats; and

iv) The criteria to be applied by competent authorities in order to assess the relevance of major ICT-related incidents for relevant competent authorities in host Member States and the details of the information to be shared with them.

The purpose of such technical standards is to harmonise and facilitate the register of information regime for ICT-related incidents in the EU.

The document considers two types of criteria for classifying incidents: (i) primary, which are the following: "Clients, financial counterparts and transactions affected", "Data losses" and "Critical services affected", including the following criteria: "Reputational impact", "Duration and service downtime", "Geographical spread", and "Economic impact". In regard to the thresholds, some of them are more appropriate for larger institutions.

For the classification of incidents as major, the materiality thresholds for two primary criteria or one primary criterion and two secondary criteria is proposed to be met.
Recurring incidents with the same apparent root cause, nature and impact that individually are not major but cumulatively meet the classification criteria are to be classified as major.

For cyber threats to be classified as major, an approach is proposed based on the probability of materialisation of the threat, whether the threat could affect critical services, and whether it could fulfil the conditions for major incident should it eventually materialise.

Lastly, the ESA propose that the assessment of the relevance to competent authorities in other Member States is to be based on the significance of the impact in the respective jurisdiction, notifying all details of major incidents to other competent authorities.

<u>Public consultation on the project for the implementation of technical standards to establish standardised templates for the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by Regulation 2022/2554 (Art. 28.9).</u>

To guarantee appropriate monitoring of ICT third-party risk in the financial sector, financial entities shall adopt a strategy that allows continuous screening of all activities of ICT third-party service providers. To achieve the latter, financial entities shall maintain and update the register of information in relation to all contractual arrangements concerning the use of ICT services provided by ICT third-party service providers.

The technical standards include standardised templates for the register of information to be maintained and updated at the entity level and at sub-consolidated and consolidated levels, in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

The templates have been designed taking into account the threefold purpose of the information register: i) it is part of ICT risk management within the ICT risk management framework; ii) it enables effective supervision of financial entities; and iii) it facilitates the designation of critical ICT third-party service providers by ESAs at EU level in the context of the oversight framework.

In order to simplify the development of the register by financial entities, the draft technical standards include two different sets of templates for registers, the first at the individual entity level and the second at sub-consolidated and consolidated level.

The templates aim to ensure a minimum level of information common to all contractual agreements on the use of ICT services and have been designed taking into account a management and referral perspective of the information to be included to ensure consistency and harmonisation and to avoid duplication in the processing of data for information purposes. The technical standards do not include specifications on the process of information exchange between financial entities and competent authorities or between competent authorities and the Oversight Forum. Financial entities shall complement the information required by the templates by adjusting it to their internal and individual risk management purposes.

For proportionality purposes, the document indicates that the set of templates is proportionate as the amount of information to be included depends on the degree of reliance on services provided by ICT third-party service providers. Therefore, a financial entity relying on a significant amount of ICT third-party service providers must register more information than a less dependent one. Moreover, financial entities are required to provide certain additional information, such as complementary information on risk assessment, the ICT supply chain or the involvement of sub-outsourcers if the ICT service provided supports a critical or important function.

Public consultation on the project for regulatory technical standards to specify the detailed content of the policy on the use of ICT services in relation to the contractual arrangement on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation 2022/2554 (Art. 28.10).

Financial entities shall adopt and review, as part of their ICT risk management framework, a strategy on risk related to ICT service providers which shall include a policy on the use of ICT services that support critical or important functions provided by ICT service providers.

The technical standards aim to enable the entity to maintain control of its operational risks, information security and business continuity throughout the life of the contractual agreement with ICT third-party service providers. To such end, the technical standards establish the requirements for financial entities at each stage in relation to the lifecycle management of contractual arrangements for the use of ICT services that support critical or important functions provided by ICT third-party service providers: i) the pre-contractual phase: planning of contractual arrangements, including risk assessment, due diligence processes and the approval process for new or material changes to said contractual arrangements with third parties; ii) the implementation, monitoring and management of contractual arrangements; and iii) the exit strategy and processes for the termination of arrangements to ensure business continuity in the case of unacceptable performance or service failure.

Next steps. ESAs shall take into account the comments received when drafting the technical standards to be sent to the European Commission reported no later than the 17 January 2023.

3.- Submission of comments

The deadline for submitting comments is **11 September 2023**.

Respondents may send their comments through ESMA's website: **www.esma.europa.eu.** On the page ***Consultations*** (set the cursor on the word to access the link to the four online response form).

A public hearing shall take place on 13 July from 9:00 to 18:00 where ESA welcome all interested parties. To attend the public hearing you must register before 10 July at 16:00 with the following form (set the cursor on the word to access the form).

Likewise, as indicated above, the CNMV would also appreciate if stakeholders could send a copy of their responses to the consultation to the following address: Documentosinternacional@cnmv.es

CNMV
Department of International Affairs
c/ Edison 4
28006 Madrid