Filters applied:
Legal act = Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Download date: Tuesday, October 7, 2025 - 11:52

Title	Submission Date
ESMA_QA_2496	27-03-2025
ESMA_QA_2459	11-03-2025
ESMA_QA_2457	07-03-2025
ESMA_QA_2456	07-03-2025
ESMA_QA_2435	10-02-2025
ESMA_QA_2431	04-02-2025
ESMA_QA_2428	03-02-2025
ESMA_QA_2399	14-01-2025
ESMA_QA_2396	10-01-2025
ESMA_QA_2386	20-12-2024
ESMA_QA_2382	18-12-2024
ESMA_QA_2381	17-12-2024
ESMA_QA_2379	17-12-2024
ESMA_QA_2378	17-12-2024
ESMA_QA_2356	03-12-2024
ESMA_QA_2328	06-11-2024
ESMA_QA_2313	23-10-2024
ESMA_QA_2311	22-10-2024
ESMA_QA_2310	22-10-2024
ESMA_QA_2301	08-10-2024
ESMA_QA_2248	12-08-2024
ESMA_QA_2241	23-07-2024
ESMA_QA_2240	23-07-2024
ESMA_QA_2226	02-07-2024
ESMA_QA_2219	13-06-2024
ESMA_QA_2160	18-04-2024
ESMA_QA_2159	18-04-2024
ESMA_QA_2158	15-04-2024
ESMA_QA_2107	12-02-2024
ESMA_QA_2103	11-02-2024
ESMA_QA_2100	05-02-2024
ESMA_QA_2099	05-02-2024
ESMA_QA_2091	02-02-2024
ESMA_QA_2079	23-01-2024
ESMA_QA_2057	20-12-2023

Title	Submission Date
ESMA_QA_2056	20-12-2023

ESMA_QA_2496

Submission Date
27/03/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT-related incident

Subject Matter
Incident report submission format

Question
What is the submission format for the incident reports (initial notification, intermediate and final) that CTPPs and Financial Entities need to submit to the CA?

ESMA_QA_2459

Submission Date
11/03/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Subject Matter
Fintech company: DORA AND ROI

Question
Hi Team,

Hope you are well!

We are a Spanish Fintech company called Toqio, our company lets you create, customize, and scale unique financial products in our platform.Please find more information below:

https://toqio.co/platform

Could you please confirm that we have to comply with DORA and also we have to send the ROI to the authorities?

Thank you in advance,

Kindest regards,

Ester

ESMA_QA_2457

Submission Date
07/03/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
Clarification on DORA Audits for Non-European ICT Service Providers

Question
The DORA law states that ICT third-party service providers must fully cooperate during onsite inspections and audits conducted by competent authorities, the Lead Overseer, the financial entity, or an appointed third party.

Will these audits be conducted the same way if the provider is located outside Europe,

ESMA_QA_2456

Submission Date
07/03/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Subject Matter
Clarification on DORA Compliance for Intra-Group providers

Question
Can you confirm our understanding of the DORA law: an intra-group entity providing services to a financial entity is subject to the same obligations as a non-critical third-party provider. This includes requirements related to contractual

arrangements, provisions for critical functions, exit strategies and termination conditions, information registry, reporting to competent authorities, and pre-contractual assessments. Additionally, if the services involve critical or important functions, further requirements apply, such as TLPT tests and audits by competent authorities.

ESMA_QA_2435

Submission Date
10/02/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Subject Matter
Register of Information at consolidated level

Question
A Group contains within it both insurance entities and banking entities; for the purposes of preparing the Register at a consolidated level, must it consider both types of Entity? To which Authority is the Register sent at a consolidated level?

ESMA_QA_2431

Submission Date
04/02/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Subject Matter
Non-EU ICT service providers without a LEI - conflicting validation rules

Question
When an ICT service provider reported under schedule 05.01 is a legal person outside of the EU, the absence of a EUID and LEI will result in a report validation error rendering the submission of the ROI impossible. Should such service provider

be left out of the register or should a dummy EUID be used (preferably issued by ESA to adequately consolidate missing positions)

ESMA_QA_2428

Submission Date
03/02/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Subject Matter
Register of Information at sub-consolidated Level

Question
For the purpose of preparing the Register of ICT Supplier Information (RoI) on a sub-consolidated basis, is it necessary to include within the different templates (ref. “B_XX.XX.XXX”) the information pertaining to both the Contractual Agreements that

the Entity signs and those that it uses?
Specifically then, the “financial entity maintaining the register of information” is to be considered corresponding to the "entity signing the contractual arrangement" and the "financial entity making use of the ICT service(s)"?

ESMA_QA_2399

Submission Date
14/01/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Finalised Comprehensive List of DORA questions

Question
Is there a finalised comprehensive list of all questions that the firms involved in the financial markets should answer? For each question is it clear to which type of firm it applies?

ESMA_QA_2396

Submission Date
10/01/2025

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Additional Legal Reference
Article 3 (21)

Subject Matter
Definition on ICT services

Question

Article 3 (21) of DORA defines that 'ICT services’ means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis.

It is not clear whether "digital and data services" should be interpreted as:
Version one: either digital or data services (so two different of sets of activities or
Version two: services which need to be both: digital service and parallel/in the same time data service.

ESMA_QA_2386

Submission Date
20/12/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Additional Legal Reference
article 2(1)(e) DORA

Subject Matter
Applicability of DORA to third country investment firms

Question

DORA also applies to the "financial entities" listed in Article 2 DORA. This includes investment firms as defined in Article 4 point (1) of Directive 2014/65/EU. Reference is made to Article 2 subsection 1 under e. in conjunction with Article 3 point (33) of DORA. Does this mean that DORA also applies to investment firms with their seats outside the EU which provide investment services in the EU?

ESMA_QA_2382

Submission Date
18/12/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Applicable accounting standard for calculation of turnover

Question
Our understanding is that a business can rely on the exemption under either Article 3(60) micro enterprise, (63) small enterprise or (64) medium-sized enterprise categories under DORA. We have however not been able to find clear information

on which accounting standard that should be used when calculating annual turnover under DORA. In addition, our analysis has not shown that the Commission Recommendation 2003/361/EC on small and medium-sized enterprises provides any guidance on the question of which accounting standard can be used.
In a recent informal call with the Swedish FSA, we were informed that, when calculating the turnover of an entity to determine whether it falls under the SME exemption under DORA, the entity should use the same accounting standards that were used to draw up the relevant audited accounts. Thus, if IFRS is applied by the national entities, the relevant entity shall use the same basis (IFRS) to calculate the relevant national turnover. Is this also ESMA's view?

ESMA_QA_2381

Submission Date
17/12/2024

Status: Question Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
art. 3 ust. 21

Question
Are service providers that are financial entities, in particular GPW, KDPW, IRGiT Banks, foreign entities that are financial institutions ICT service providers? The service does not concern the provision of ICT services, but e.g. maintaining a bank

account.

ESMA_QA_2379

Submission Date
17/12/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
Art. 1 ust. 1 DORA - systems supporting the business processes of financial entities

Question
Financial entities select ICT service providers based on risk assessment, taking into account the business continuity plan and a number of national and sectoral regulations regarding cybersecurity. In addition to standard contractual relationships

with entrepreneurs, there are also solutions that financial entities use:
a) on the basis of a license, e.g. open source. The license provisions are not negotiated, and the service is not individually parameterized for the investment company. The investment company has no influence on the shape of the service and the license provisions. The licenses contain provisions regarding automatic update of the tool, but do not contain provisions regarding, e.g. support or SLA, e.g. Adobe Acrobat Reader;
b) web applications, e.g. Lex/Legalis systems (review of legal acts), which employees access via a browser, the agreement does not involve installing the application on the employee's computer, but only providing a specified number of licenses for use by the company, or a web system for registering correspondence in the case of ordering a courier;
c) providers of employee benefits, e.g. medical care. They are not directly related to the company's business, employees use the application on private devices and log in with a private email address, while registration is necessary for the medical company to create an account for the employee;

Is it possible to apply the principle of proportionality, provided for in the DORA regulations, which will allow for proper identification of risks and the application of proportionate mitigants in the case of the above-mentioned services? In the opinion of the financial entity, the application of all the obligations indicated in the DORA regulations, in particular those concerning contractual provisions and reporting obligations, is disproportionate to the risk generated by the above solutions. The financial entity does not deny the need for each case of evaluation of the solution and review of its correct functioning, the number of entities in relation to which these obligations would have to be performed may affect the quality of the duties performed.

Are the services supporting a critical or important function all the services used as part of performing this function, including those that are quickly and relatively cheaply replaceable (e.g. Adobe Acrobat Reader, 7ZIP, e-mail encryption program)?

ESMA_QA_2378

Submission Date
17/12/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Article 3(28) and EU Subcontractors

Question
DORA Article 3(28) excludes natural persons from the definition of 3rd country subcontractors, does the same apply to EU Subcontractors?

ESMA Answer

17-12-2024

Original language

Article 3(28) clearly carves out natural persons from the definition of 3rd country subcontractors. This does however not infer that natural persons are not included in the scope of EU subcontractors.

The ITS on the Register of Information clearly indicates that (i) subcontractors may be individuals acting in business capacity (Article 3(6)) and (ii) in Part 2, tables on instructions, line B_05.01.0070). It is clarified that ICT third party service providers may be either legal persons or individuals acting on business capacity.

When we look at Article 29(2) of DORA, we can infer that the relevant subcontractors are anyway ICT third party service providers. Hence, other than in the case of the third-country subcontractors, the ITS on registers has clarified that EU ICT subcontractors may be individuals.

ESMA_QA_2356

Submission Date
03/12/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Additional Legal Reference
Articles 2(1)(k) and 2(3)(a), Regulation (EU) 2022/2554 (“DORA”)

Subject Matter
Application of DORA to AIFMs which have chosen to opt-in to the application of the AIFMD but whose asset under managment is below the thresholds as provided for by Article 3(2) of AIFMD

Question

Are sub-threshold alternative investment fund managers (AIFMs) as referred to in Article 3(2) of Directive 2011/61/EU (“AIFMD”), which have chosen to opt-in to the application of the AIFMD according to Article 3(4) of that Directive, captured within the scope of application of Regulation (EU) 2022/2554 (“DORA”) under Articles 2(1)(k) and 2(3)(a) of DORA, if the thresholds regarding assets under management (“AuM”) referred to under Article 3(2) of AIFMD are not exceeded by such AIFM?

ESMA Answer

03-12-2024

Original language

According to the European Commission Q&A DORA003, DORA applies to AIFMs as defined in Article 3(44) of Directive 2011/61/EU (AIFMD), with the exemption of sub-threshold AIFMs referred to in Article 3(2) of AIFMD, which are excluded from the scope of application of DORA.

However, in case such a sub-threshold AIFM decides to opt-in to the application of the entirety of AIFMD (Article 3(4) of Directive 2011/61/EU), all requirements that are applicable to managers of alternative investment funds defined in Article 4(1), point (b), of AIFMD will become applicable to the entity that opted in. As Article 18 of AIFMD applies (amended by Directive (EU) 2022/2556 it includes a reference to Regulation (EU) 2022/2554 (DORA)), DORA applies as well to these entities.

Consequently, DORA also applies to sub-threshold AIFM which have decided to opt in to Directive 2011/61/EU despite not exceeding the thresholds under Article 3(2) of Directive 2011/61/EU.

ESMA_QA_2328

Submission Date
06/11/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Question
We have service providers (Market Axess), who classify themselves as DORA-relevant because they offer regulated financial services (ARM and APA). However, they do not see themselves obligated to make contractual adjustments according to

Article 30. This is because "financial services" would not fall under the definition of "ICT service" as per Article 3(21) of DORA. Additionally, this requirement would only apply to non-regulated companies. Is this understanding correct?

ESMA_QA_2313

Submission Date
23/10/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Additional Legal Reference
ITS on Register of Information

Subject Matter
b_06.01.0020 - Licensed activity - Legal Protection Insurance

Question

Which licensed activity has to be selected for the licensed activity dropdown in the Register of Information if the entity is a legal protection insurance? According to the Annex of Solvency II it is the class 17, but class 17 is not available in the choices for the drop down field.

ESMA_QA_2311

Submission Date
22/10/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Scope of application of DORA for UCITS Management Companies

Question
Can you set out how UCITS Management Companies fall in scope for DORA and if there are any exemptions.

ESMA_QA_2310

Submission Date
22/10/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Application of DORA to non-EU AIFMs of AIFs with EU investors

Question
The scope of DORA includes (Article 2(1)(k) “managers of alternative investment funds”. Such an entity is defined in Article 3(44) as “… a manager of alternative investment funds as defined in Article 4(1), point (b), of Directive 2011/61/EU”. It is

noted that the definition does not extend to the need to be authorised or registered under Directive 2011/61/EU. As such this can be read as meaning that all managers (regardless of their jurisdiction) of alternative investment funds could potentially fall within scope of DORA.

ESMA_QA_2107 clarifies that a financial entity in the EU is subject DORA and that DORA does not directly apply to a non-EU entity providing services to an EU financial entity – although DORA may apply indirectly to the non-EU entity given that the “EU financial entity is expected to validate that the non-EU third-party provider does not prevent it to be compliant with DORA”.

Does the same principle apply to non-EU AIFMs that manage AIFs (regardless of where those AIFs are established) which have investors based in the EU i.e. DORA will not directly apply to such non-EU AIFMs, but may apply indirectly if such investors are financial entities in the EU who are directly subject to DORA?

ESMA_QA_2301

Submission Date
08/10/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Additional Legal Reference
Reg. DORA - Art. 3

Subject Matter
ICT Service definition

Question

Related to the definition provided by the Regulation, what are the criteria that can be used to identify the continuity component (i.e "on ongoing basis) mentioned?

ESMA_QA_2248

Submission Date
12/08/2024

Status: Forwarded to EC/Public Consultation/Other

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Additional Legal Reference
Article 3 of the DORA Regulation points (60), (63) and (64)

Subject Matter
Size Thresholds for Self-Managed AIFs and UCITS

Question

We have been discussing a number of queries submitted by the local industry regarding practical difficulties when applying the definitions of micro, small and medium-sized enterprises as per Article 3 points (60), (63) and (64) of the DORA Regulation to self-managed AIFs and UCITS. We would like to obtain further clarification on the correct and proportionate interpretation of “annual turnover”, “total assets” and “employees” in the context of self-managed AIFs and UCITS.

ESMA_QA_2241

Submission Date
23/07/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT-related incident

Subject Matter
Consultas relacionadas con el reporte de incidentes

Question
Buenos días, me gustaría hacer dos consultas relacionadas con el reporte de incidentes:

En primer lugar, tras la publicación del segundo lote de RTS de DORA. En relación al RTS Final Report Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threats. Nos gustaría realizar dos consultas:
- Por una parte, se incluye, en el artículo 6 de los plazos de notificación para el reporte intermedio, las entidades financieras presentarán sin demora indebida un informe intermedio actualizado, en cualquier caso, cuando se hayan restablecido las actividades regulares. Por lo tanto, ¿se trata de un reporte obligatorio actualizar el informe intermedio bajo esa casuística?

- Por otro lado, en la RTS no se identifica a la autoridad competente a la que se debe de realizar los distintos reportes. En nuestro caso, España, tenemos como CSIRT de referencia INCIBE y también como autoridad competente BANCO DE ESPAÑA, ¿podríais comentarnos a quién es específico se deberían de realizar esos reportes, por favor?

En segundo lugar, aunque no se disponga de una relación estrecha con DORA, ha resultado también necesario Se elabora un informe semestral para la Autoridad Bancaria Europea (EBA) relacionado con los incidentes de ciberseguridad sufridos, con el propósito de llevar a cabo estudios estadísticos en el sector. ¿Podrías ayudarnos a confirmar si esta información es cierta y donde podríamos encontrar la referencia por favor?

ESMA_QA_2240

Submission Date
23/07/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT-related incident

Subject Matter
Consultas relacionadas con el reporte de incidentes

Question
Buenos días, me gustaría hacer dos consultas relacionadas con el reporte de incidentes:

En primer lugar, tras la publicación del segundo lote de RTS de DORA. En relación al RTS Final Report Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threats. Nos gustaría realizar dos consultas:
- Por una parte, se incluye, en el artículo 6 de los plazos de notificación para el reporte intermedio, las entidades financieras presentarán sin demora indebida un informe intermedio actualizado, en cualquier caso, cuando se hayan restablecido las actividades regulares. Por lo tanto, ¿se trata de un reporte obligatorio actualizar el informe intermedio bajo esa casuística?

- Por otro lado, en la RTS no se identifica a la autoridad competente a la que se debe de realizar los distintos reportes. En nuestro caso, España, tenemos como CSIRT de referencia INCIBE y también como autoridad competente BANCO DE ESPAÑA, ¿podríais comentarnos a quién es específico se deberían de realizar esos reportes, por favor?

En segundo lugar, aunque no se disponga de una relación estrecha con DORA, ha resultado también necesario Se elabora un informe semestral para la Autoridad Bancaria Europea (EBA) relacionado con los incidentes de ciberseguridad sufridos, con el propósito de llevar a cabo estudios estadísticos en el sector. ¿Podrías ayudarnos a confirmar si esta información es cierta y donde podríamos encontrar la referencia por favor?

ESMA_QA_2226

Submission Date
02/07/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
Scope of the definition of ICT services

Question
As the manager of an Alternative Investment Fund (AIF), we provide specialized investment opportunities to professional investors such as pension funds, insurers, and banks within the EU. Consequently, both our firm and our investors fall within

the scope of DORA.

Our investors can access their portfolios through an online portal operated by a third-party service provider (an ICT third-party service provider). We intend to establish a DORA addendum with this ICT third-party service provider to address this specific ICT service.

Several of our investors have inquired about DORA compliance in relation to their contractual relationship with us. While we are committed to ensuring the portal itself is compliant, we believe our core service – providing investment opportunities – does not constitute an ICT service under DORA. The online portal is merely a supplementary tool for accessing reports, not a fundamental part of our contractual obligations. This view is further supported by the fact that our agreements with investors only stipulate that we provide them with reports, without specifying the method of delivery.

Given these considerations, do you agree with our assessment that our services to investors do not fall under the definition of an ICT service as per DORA and that we, in respect of our investors, cannot be considered an ICT third-party service provider?

ESMA_QA_2219

Submission Date
13/06/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Additional Legal Reference
Final Report on Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework

Subject Matter
Questions on Microenterprises and RMF

Question

QUESTION 1: Internal Audit Frequency for Microenterprises and financial entities subject to the simplified risk management framework
Recital 43 of DORA states that microenterprises and financial entities (FEs) referred to in Article 16(1) of DORA are not required to conduct regular internal audits of their ICT risk management framework (RMF). Does it conflict with Article 28, paragraph 5 of Commission Delegated Regulation (EU) 2024/1774 (RTS) that mandates an internal audit on the ICT RMF in line with the FE's audit plan?

QUESTION 2: ICT Testing Requirements for Microenterprises and Financial Entities – Cyber-attack scenarios
Article 11.6 of DORA excludes microenterprises from the requirement to include cyber-attack scenarios in their ICT business continuity and recovery plan testing. Does it conflict with Article 39, paragraph 1 of the Commission Delegated Regulation (EU) 2024/1774 (RTS), which mandates the inclusion of cyber-attack scenarios in the testing plans for financial entities referred to in Article 16(1) of DORA?

QUESTION 3: Recital 43 of DORA specifies that microenterprises and financial entities referred to in Article 16(1) of DORA are not required to regularly conduct risk analyses on legacy ICT systems. Does it conflict with Article 34, paragraph 1, point (e) of the Commission Delegated Regulation (EU) 2024/1774 (RTS) which mandates that financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 must manage the risks related to outdated or unsupported and legacy ICT assets?

ESMA Answer

11-12-2024

Original language

ANSWER 1: Recital 43 does not conflict with Article 28, paragraph 5 of the RTS. The text of Recital 43 in DORA suggests that microenterprises and FEs referred to in Article 16(1) of DORA are not obligated to conduct internal audits of their ICT RMF on a regular basis. This means there is no mandate for these entities to perform the said internal audit with a specific periodicity. However, it does not exclude the necessity of conducting internal audits as deemed necessary by the FE's audit plan. The responsibility for determining the appropriate frequency and triggers for audits lies with the FE.

ANSWER 2: There is no contradiction between Article 11.6 of DORA and Article 39, paragraph 1 of the RTS. Article 11.6 of DORA explicitly excludes microenterprises from the requirement to include cyber-attack scenarios in their ICT business continuity and recovery plan testing. This exclusion applies solely to microenterprises and not to financial entities referred to in Article 16(1) of DORA. DORA clearly distinguishes between microenterprises and financial entities referred to in Article 16(1) of DORA, ensuring that the latter are still required to include cyber-attack scenarios in their testing plans as per Article 39, paragraph 1 of the RTS.

ANSWER 3: There is no contradiction between Recital 43 of DORA and Article 34, paragraph 1, point (e) of the RTS. Recital 43 specifies that microenterprises and financial entities referred to in Article 16(1) of DORA are not required to regularly conduct risk analyses on legacy ICT systems. This means there is no mandate for these entities to perform risk analyses with a specific periodicity. However, it does not imply that the risks associated with legacy systems should not be managed at all. Article 34 does not specify a required frequency for these risk analyses.

ESMA_QA_2160

Submission Date
18/04/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Register of information

Subject Matter
DORA compliance contractual template to be provided by the ESA’s for FE’s / ICT providers

Question
Contractual agreements need to be updated to ensure that they are DORA compliant, yet Financial Entities (FE’s) do not know when standard contractual

clauses will be provided by the relevant public authorities following the Article 30.4. of Regulation(EU) 2022/2554 We understand that if standard contractual clauses are not provided by the relevant public authorities' in due time, then the legal departments of FE’s and ICT providers will potentially need to develop their own contractual clauses and templates, which will not only create a huge amount of work, duplicated by the different parties, and potentially mis-interpretation of the regulation, but will lead to protracted contractual negotiations between the FE’s and the ICT providers over which template should be used to cover the services provided, i.e. the template designed by the FE, or, the template designed by the ICT provider, and which will undoubtedly lead to a situation whereby the FE’s and ICT providers are required to manage multiple different contractual arrangements (which in turn will generate a tremendous additional supervisory efforts regarding the different provisions implemented).
Could you please kindly confirm the expected date when the relevant public authorities will release a first draft of the DORA compliant standard contractual clauses and template to be used by the FE’s and ICT providers?
Notwithstanding the fact that the abovementioned article refers to standard clauses for certain specific services, the financial sector has claimed the publication of standard contractual clauses under DORA. This will not only ease negotiations between FE´s and ICT providers but will also enforce the contractual security framework, as less misinterpretations of DORA will take place.
Additionally, critical ITC providers are still to be designated by the ESAs and, therefore, negotiations between FE´s and ICT providers have not started yet in most of the cases. Therefore, we strongly request that consideration be given to the possibility of establishing a transitional period to adapt the contracts to the framework established by DORA.

ESMA_QA_2159

Submission Date
18/04/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Historic Question Reference
Clarification Request on Preliminary Assessment of ICT Concentration Risk submitted via DORA's consultation papers.

Additional Legal Reference
Art.1(i) of the 'Draft RTS to specify the elements that a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions', as mandated by Article 30(5) of Regulation (EU) 2022/2554

Subject Matter

Intragroup ICT service providers consideration regarding the preliminary assessment of ICT concentration risk.

Question

When conducting the preliminary assessment of potential ICT concentration risk associated with an ICT service provider, as stipulated in Regulation 2022/2054 and its corresponding draft RTS on subcontracting ICT services supporting critical or important functions, what treatment should be applied to ICT intra-group service providers? In other words, are financial entities (FEs) required to consider this concentration risk for ICT intra-group service providers? Alternatively, would the exemption outlined in Regulation 2022/2054 article 31.8(iii) apply, thereby meaning that this risk should not be considered for intra-group service providers?

REGIS-TR SA seeks further clarification on this matter, given that the DORA Regulation establishes that

- 'While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment'.

Similarly, article 28.4(c) states that

- 'Before entering into a contractual arrangement on the use of ICT services, financial entities shall: (c) identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29'.

Furthermore, the aforementioned article 29 covers the considerations and risks to take into account in relation to ICT service providers supporting critical or important functions, when performing the preliminary assessment of ICT concentration risk.

Additionally, the draft RTS on 'the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions' also explains that

- ‘ICT intragroup subcontractors, including the ones fully or collectively owned by financial entities within the same institutional protection scheme, providing ICT services supporting critical or important functions should be considered as ICT third-party services providers. Intragroup ICT subcontracting should not be treated differently from subcontracting outside of the group. The risks posed by those ICT intragroup subcontractors may be different but the requirements applicable to them are the same in accordance with Regulation (EU) 2022/2054. When the use of ICT subcontractors is permitted, then those also include ICT intragroup subcontractors’, thereby making no distinction between intra-group and external service providers.

Due to these reasons, we are uncertain about whether the exemption outlined in Regulation 2022/2054 article 31.8(iii) would apply; or if exposure to a ICT intragroup service providers should also be considered during the preliminary assessment of ICT concentration risk.

ESMA_QA_2158

Submission Date
15/04/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT-related incident

Additional Legal Reference
Draft RTS Article 6 section 1 lit. b)JC 2023 70

Subject Matter
Understandig of timelimits of intermediate repots for major related ICT-incidents

Question

Is our standing of Article 6 of the RTS correct, that an institution should submit more than one intermediate report for a major ICT-incident, if that incident continues over the 72 hours threshold for the initial intermediate report?
Art. 6 states that an institution has to submit a report in case that after 72 hours the incident is not resolved or when the incident is resolved. Our understanding is that the "or" means that an institute has to submit more than one report in case that the incident is resolved after more than 72 hours.

ESMA Answer

15-04-2024

Original language

Article 19(4) of Regulation (EU) 2022/2554 (DORA) provides that financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit an intermediate report after the initial notification, as soon as the status of the original incident has changed significantly or the handling of the incident has changed based on new information available, followed, as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority.

Article 5(1)(b) of the Commission Delegated Regulation XX (RTS on content and timelines on incident reporting) specifies that financial entities shall submit an intermediate report ‘at the latest within 72 hours from the submission of the initial notification, even where the status or the handling of the incident have not changed as referred to in Article 19(4), point (b), of Regulation (EU) 2022/2554. Financial entities shall submit an updated intermediate report without undue delay, and in any case when the regular activities have been recovered’.

It follows from the above that financial entities shall submit an intermediate report under the conditions set out in Article 19(4) of DORA and at the very latest within 72 hours from the submission of the initial notification as set out in the Delegated Regulation.

Where financial entities have not recovered regular activities within 72 hours from the submission of the initial notification, they shall submit an intermediate within the 72-hour timeframe and at least another intermediate when the regular activities have been recovered.

Where financial entities have recovered regular activities, they can submit a single intermediate report, provided that the requirements of Article 19(4) of DORA are met.

ESMA_QA_2107

Submission Date
12/02/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Subject Matter
Application of DORA for outsourced critical services that are not ICT

Question
My questions relate to the scenario where a UK financial services firm, or an offshore financial services firm (e.g. in Guernsey), provides services to an EU financial services firm.

For example, in the scenario where an EU financial services firm outsourced its fund management to a UK asset management firm to manage a fund. Would the EU firm be expected to have sought reassurance from the UK fund manager that the UK firm is also compliant with DORA?
Thanks in advance for your help.

ESMA Answer

12-02-2024

Original language

A financial entity in the EU is subject to DORA and must ensure it operates DORA-compliant, which includes their third-party relationships.

Therefore, it follows that if an EU financial entity makes use of a non-EU third-party provider for a function or activity, independently of whether this function is considered as critical or important or not by the financial entity and this service provider in turn makes use of ICT services to support its function or activity, the responsibility to ensure the operational resilience of the function or activity that has been entrusted to the non-EU third-party provider remains with the financial entity.

The EU financial entity is expected to validate that the non-EU third-party provider does not prevent it to be compliant with DORA.

ESMA_QA_2103

Submission Date
11/02/2024

Status: Answer Published

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Subject Matter
EUC, EULA and Shadow IT

Question
For complying with the regulatory provisions envisaged by the DORA Regulation, Financial Entities should consider End User Computing (EUC) tools, End User License Agreements (EULA), and the conditions of Shadow IT.

Would it be possible to obtain the regulatory references for these areas?

ESMA Answer

11-02-2024

Original language

According to the broad definition of ICT asset under Article 3(7) of DORA, EUC tools are considered ICT assets since they are software or hardware used in the network and information systems of the financial entity. The same apply for the software governed by the EULA and the ICT systems developed and managed by users outside the ICT function (shadow IT). Therefore, all management, security, and risk assessment provisions of DORA related to ICT assets should apply to EUC tools, software governed by EULAs and Shadow IT. This includes identifying, documenting, and managing these assets to mitigate any associated risks.

In addition, According to Article 11, Paragraph (2), point (c) of the Commission Delegated Regulation (CDR) (EU) 2024/1774 (RTS on RMF), a financial entity should identify the security measures to ensure that only authorised software is installed in ICT systems and endpoint devices. This means that all ICT systems implemented need to be authorised; the financial entity should implement all necessary technical and organizational measures to this effect.

Also, Article 16, Paragraph (9) of the RTS on RMF emphasizes that procedures related to ICT systems' acquisition, development, and maintenance must also apply to ICT systems developed or managed by users outside the official ICT function, using a risk-based approach. Under DORA, all ICT assets must be identified,

documented, and managed to ensure they meet the entity's ICT risk management requirements. This means financial entities must ensure that their ICT risk management and control processes cover the ICT systems developed and managed by users outside the ICT function and EUC practices, ensuring all software and hardware is implemented in an authorised way and is securely integrated and operated within the organization's ICT infrastructure The risks that such a practice can pose should be also appropriately identified and managed, as per the Article 6 and Article 8 Paragraph (2) of DORA respectively.

Regarding the EULA, if an EULA is a contractual agreement between a third-party service provider, as defined by Article 3(19) of DORA and the financial entity, and the software governed by this EULA is installed on an ICT asset of the financial entity or used to support business functions of the financial entity, then all provisions of Regulation (EU) 2022/2554 regarding ICT risk management, including third-party risk management, apply. This scenario includes the use of authorised software governed by the EULA even if the terms of the EULA are accepted by the employee of the financial entity on behalf of the financial entity.

We understand there could be cases where the EULAs is not subject to specific third-party risk management provisions as above. Nevertheless, they would be anyway subject to the ICT risk management requirements, because the software provided under these agreements is often customised and maintained internally by the financial entity or involves minimal interaction with external service providers. The emphasis is on managing ICT risks directly related to the software's use and all the relevant DORA provisions should apply.

ESMA_QA_2100

Submission Date
05/02/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Digital operational resilience testing

Subject Matter
Cross-border Market Jurisdiction

Question
Would an EU-based Firm providing ICT Services wholly to non-EU-based Firms be deemed in or out of scope for DORA?

ESMA_QA_2099

Submission Date
05/02/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Additional Legal Reference
Article 3 (21)

Subject Matter
The activities of credit bureaus (credit reporting agencies)

Question

The activities of credit bureaus (credit reporting agencies) are not directly referenced within the scope of DORA. These services may not traditionally seen as "ICT Services", but they could be interpreted as "data services provided through ICT systems". Are these intended to be within scope for ICT services?

ESMA_QA_2091

Submission Date
02/02/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT risk management

Additional Legal Reference
„4. Data reporting service providers shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports.”

Subject Matter
impelemtation of Article 10 (4)

Question

Can you elaborate the requirement above? What an effective check should contain and how should be implemented practically?

ESMA_QA_2079

Submission Date
23/01/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
DORA, Article 3 - definition of microenterprise and small enterprise

Question
We are investment company that doesn´t meet DORA requirements to qualify as microenterprise neither as small enterprise since we have more than 10 employees (total of 14) but our annual turnover and/or annual balance sheet total that does not

exceed EUR 2 million. What are our obligations under DORA regulation?

ESMA_QA_2057

Submission Date
20/12/2023

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Additional Legal Reference
On Draft Implementing 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 (EU)

Subject Matter

Software companies

Question

How can DORA Article 28 be applied on software companies when the financial entity purchases off-the-shelf software licenses? If the off-the-shelf software supports critical or important function, should the DORA Article 28 (8) be applied?

ESMA_QA_2056

Submission Date
20/12/2023

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
ICT third-party risk management

Additional Legal Reference
On Draft Implementing 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 (EU)

Subject Matter

Software distributors

Question

When an off-the-shelf software license (e.g. operating systems, database) is purchased through a distributor, is the distributor qualifying as “ICT third-party service provider” in case if the distributor itself is not providing any additional services in addition to the distribution, and its contractual tasks are completed with the successful intermediation of the license agreement? Is the software company qualifying as a direct “ICT third-party service provider” based on the end-user license agreement (EULA) accepted by the financial entity?

No hay parametros en la URL.