



14 December 2023

DIGITALEUROPE's Response to the European Commission's Consultation on DORA's Delegated Acts on Criticality Designation Criteria and on Oversight Fees



Introduction

DIGITALEUROPE appreciates the opportunity to provide comments to the European Commission on the draft delegated acts under DORA mandate. We welcome the Commission's sensible approach, advancing the ESA guidance delivered in the Joint Report on 29 September. The draft delegated acts show a welcome focus on proportionality in many aspects raised by industry stakeholders under the ESA consultation in 2023. We would like to offer the following comments to further strengthen the principle of proportionality and to constructively support additional legal clarity and certainty.

1) Delegated act on criticality designation criteria

We welcome the Commission's approach to a *sequenced* application of indicators with a focus on ICT services that support critical or important functions. This approach is consistent with DORA Level 1 and will focus designation and resources on ICT services that are objectively critical to financial stability.

Article 1: Assessment approach

In an administrative decision-making process like the criticality assessment under DORA, fundamental fairness requires reasoned decision making with notice and explanation to the regulated entity and an opportunity to be heard. Article 1 of the Act should be modified to improve the designation process.

As drafted, Article 1 establishes a two-step assessment process for each of the four general criteria for criticality designation set forth in Article 31(2) of DORA. Under each criterion, Step 1 will involve a quantitative assessment of financial entities' reliance on services from an ICT third-party service provider, and Step 2 will involve a qualitative assessment of the impact or significance of relevant ICT services. If both steps are satisfied for all criteria, an ICT service provider will be designated as critical. This process constitutes a multi-factor approach to guard against both substantial systemic risk and excessive designation. But it exhibits some shortcomings because it does not mandate consistent examination of a particular ICT service across each criterion (as opposed to service providers), and there is no explicit requirement for the ESAs to explain

their decision making which is necessary for an ICT service provider to correct any misunderstanding through a statement under Article 31(5) of DORA. These procedural gaps allow for the possibility of arbitrary and inconsistent decision-making because different assessment criteria could be deemed satisfied based on different services offered by the same provider, not each of which supports a financial entity's critical or important functions. To ensure consistency and accuracy in the assessment and designation process – and to ensure that practical effect will be given to an ICT service provider's right to submit a statement in response to a designation decision under Article 31(5) of DORA – this Article should expressly require that assessments and designation decisions be documented in writing with reasoned explanations according to each ICT service assessed. To resolve these issues, we propose adding the below underlined text to Article 1:

Article 1
Assessment approach

1. When considering the criteria set out in Article 31(2) of Regulation (EU) 2022/2554 to designate an ICT third-party service provider that is critical for financial entities, the ESAs shall apply the following approach:

(a) as a first step, the ESAs shall assess whether the ICT third-party service provider fulfils all of the 'step 1' sub-criteria set out in Articles 2(1), 3(1), and 5(1);

(b) as a second step, for those ICT third-party service providers that fulfil all of the 'step 1' sub-criteria referred to in point (a), the ESAs shall carry out their assessment in the light of the 'step 2' sub-criteria referred to in Articles 2(5), 3(4), 4(1), and 5(5).

By way of derogation from the first sub paragraph, for the assessment of the criterion (c) of Article 31(2) of Regulation (EU) 2022/2554, the first step shall be covered by the assessment to be carried out for the criteria (a), (b) and (d) of Article 31(2) of Regulation (EU) 2022/2554. **In performing assessments, the ESAs shall apply each sub-criteria to each particular ICT service under consideration for making a designation decision and shall document their assessment of each such ICT service under each sub-criteria.**

2. In providing notice of its assessment and any decision to designate an ICT third-party service provider as critical pursuant to Article 31(5) of

Regulation (EU) 2022/2554 and to ensure that any ICT third-party service provider designated as critical may exercise its right under that same Article, the ESAs shall include in such notice a reasoned explanation of such assessment and designation, which shall include identification of the particular ICT services by specific application covered by the designation and, for each such specific service, an explanation why each sub-criteria referenced in paragraph 1 of this Article is fulfilled with reference to specific evidence supporting the designation decision.

3. After the end of the time period for the submission of a reasoned statement referred to in Article 31(5), first subparagraph, of Regulation (EU) 2022/2554, the ESAs, through the Joint Committee and upon recommendation from the Oversight Forum, shall designate an ICT third-party service provider as critical for financial entities if it fulfils all the 'step 1' sub-criteria referred to in paragraph 1, point (a), and following a positive outcome of the assessment carried out in relation to the 'step 2' sub-criteria referred to in paragraph 1, point (b).

Article 2(5) and Article 3(4): intensity of impact; reliance

As drafted, Step 2 Sub-criteria 1.3 and 2.3 of Articles 2(5) and 3(4), respectively are unclear as to whether they will be applied to an ICT service provider's services in general or the ICT services supporting critical or important functions of financial entities that will be assessed in the corresponding Step 1 under each of these Articles. This text creates the risk that the Step 2 assessment will be broader than their corresponding Step 1 indicators. As Step 2 follows Step 1, the assessments under these sub-criteria should be limited to the financial entities and ICT services supporting critical functions identified in Step 1.

In addition, the terms "intensity of impact" and "dependence" in Sub-criteria 1.3 and 1.4 in Article 2(5)(a), (b), respectively, are undefined and could be interpreted and applied in numerous and potentially inconsistent ways. We urge the Commission to clarify that impact intensity to be evaluated according to the disruption of a financial entity's critical or important functions and that dependence on a sub-contractor means not mere utilization but that the subcontractor's failure of performance would result in failure of an ICT services supporting the financial entity's critical or important functions.

To resolve these issues, we propose adding the below underlined text to Article 2 and Article 3:

Article 2(5):

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels

T.+32 (0) 2 609 53 10 / www.digitaleurope.org / [@DIGITALEUROPE](https://twitter.com/DIGITALEUROPE)

EU Transparency Register: 64270747023-20

(a) Sub-criterion 1.3: the intensity of the impact of discontinuing the ICT services provided by the ICT third-party service provider on the activities and operations of financial entities **identified in the ‘step 1’ sub criteria referred to in paragraph 1 of this Article** and the number of **those** financial entities affected;

(b) Sub-criterion 1.4: the dependence of the critical ICT third-party service provider on the same subcontractors providing ICT services supporting critical or important functions of financial entities, **as determined by whether the failure of performance of such subcontractors would result in the failure of ICT services supporting such critical or important functions.**

Article 3 (4):

4. Sub-criterion 2.3: G-SIIs or O-SIIs and other financial **entities included in the assessment in the ‘step 1’ sub criteria referred to in paragraph 1 of this Article**, including where **those** G-SIIs or O-SIIs provide financial infrastructure services to other financial entities, relying on an ICT service provided by the same ICT third-party service provider, are interdependent.

Article 6: Information sources to enable criticality assessment

As drafted, Article 6 provides that the ESAs, in performing criticality assessments, may use data provided by regulated financial entities in their “registers of information” and “additional available data they have at their disposal from all available sources.” This proposed provision raises related concerns regarding information authenticity, reliability, transparency, and confidentiality. In the event that ESAs assess criticality based on “additional available data,” they should be limited to using only verifiable and reliable information that satisfies authenticity standards appropriate for administrative agency decision-making. Further, the best way to ensure the reliability of information underlying an assessment is to disclose to the relevant ICT service provider the information on which the ESAs rely, so its veracity can be evaluated. In addition, because any non-public information that the ESAs might use in performing their assessments might contain commercially sensitive data or pose a security risk if publicized – whether from registers of information, statements from and ICT service provider under Article 31(5) of DORA, or other sources – the Act should clearly specify that such information must be safeguarded and is exempt from public disclosure.

To address these issues, we propose adding the below underlined text to Article 6:

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels

T. +32 (0) 2 609 53 10 / www.digitaleurope.org / [@DIGITALEUROPE](https://twitter.com/DIGITALEUROPE)

EU Transparency Register: 64270747023-20

*Article 6**Information sources to enable criticality assessment*

1. The ESAs shall use the data provided by the registers of information referred to in Article 28(3) of Regulation (EU) No 2022/2554, for the assessment of the sub criteria listed in Articles 2 to 5. The ESAs may also use additional available data they have at their **disposal from the exercise of their supervisory role** and from all **reliable** sources of information to perform the criticality assessment. **The ESAs shall reference the specific sources on why they rely in any notice of designation under Article 31(5) of Regulation (EU) No 2022/2554.**

...

3. Information provided to the ESAs in registers of information or in statements under Article 28(3) and 31(5) of Regulation (EU) No 2022/2554, respectively, or on which the ESAs rely for their assessment of the sub criteria listed in Articles 2 to 5 that is not otherwise public shall be treated as confidential, safeguarded as such, and exempt from disclosure, except to the relevant ICT third-party service provider.

2) Delegated act on oversight fees

Article 1: Estimation of the Expenditures of the Lead Overseers

Article 1 of the Act provides that the Lead Overseer and other ESAs shall annually estimate their overall costs for performing oversight duties and that such estimate shall be the basis for calculating the amount of oversight fees that will be charged to a critical ICT third-party service provider. Article 1 provides that the Lead Overseer shall take into account five categories of “direct and indirect costs.” The Act lacks explicit terms to minimize costs and limit them only to costs that are reasonably necessary for performance of oversight duties. Absence of cost-containment terms is problematic because, for example, it is unclear whether or how a Lead Overseer agency’s general overhead costs could be considered an “indirect cost” of oversight under DORA. Because regulated ICT service providers will have to bear the costs of oversight and yet have no control over how costs are incurred, the Act should include requirements and principles to contain oversight costs as much as possible and allow regulated entities to understand the basis for oversight fees.

To address these issues, we propose adding the below underlined text to Article 1:

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels

T. +32 (0) 2 609 53 10 / www.digitaleurope.org / [@DIGITALEUROPE](https://twitter.com/DIGITALEUROPE)

EU Transparency Register: 64270747023-20

*Article 1**Estimation of the expenditures of the Lead Overseers when performing their oversight duties*

1. In each year, the Lead Overseer and the other European Supervisory Authorities shall estimate the overall annual costs that are **reasonably necessary and** expected to be incurred for the performance of their oversight duties. The amount of the **reasonably necessary** overall annual costs estimated shall be the basis for determining the overall amount of oversight fees charged.

2. When estimating the annual **reasonably necessary** overall costs, the Lead Overseer shall take into account the following direct and indirect costs:

(a) costs related to the designation of ICT third-party service providers as critical;

(b) costs related to the appointment of the Lead Overseer;

(c) costs related to the actual oversight of critical ICT third-party service providers, including the following:

(i) costs related to the participation of competent authorities in that oversight, **limited to activity that is essential for performance of an oversight duty;**

(ii) costs incurred as a result of work carried out by the joint examination team;

(iii) costs of advice provided by independent experts, **provided that such costs do not exceed reasonable market rates for services from such experts;**

(d) costs related to the follow-up of the recommendations issued by the Lead Overseers in accordance with Article 35(1), point (d), of Regulation (EU) 2022/2554;

(e) costs related to the governance of the oversight framework.

3. For each year's estimate of reasonably necessary overall annual costs, the Lead Overseer and the European Supervisory Authorities shall prepare and provide to critical ICT third-party service providers a calculation of the estimated costs according to each category of allowable costs included paragraph 2 of this Article, including differentiation between direct and indirect costs, the specific activities of competent authorities for which costs will be incurred, and any independent experts' identities, rates, and specific topics of advice included in the estimate.

Article 2: Applicable Turnover and Calculation of Oversight Fees

The EC's proposal to limit the scope for fees, applying a reference to the list of ICT services in the ITS on the register of information (Article 1 (1)), is welcome. Assuming the list of ICT services in the ITS is aligned with DORA's focus on the resilience of the financial sector, it would be appropriate to scope turnover to revenue generated by the CTPP in providing services on that list.

The ESAs flagged procedural difficulty in the determination of the applicable turnover in their advice. However, this should not lead to a recommendation of an inequitable approach by overly extending a fall-back option, as we see it under Art. 2 (3) of the draft delegated act. Art. 43(1) DORA foresees that fees shall cover the Lead Overseer's necessary expenditure in relation to the conduct of the oversight and in relation to matters falling under the remit of direct oversight activities. In this sense, **it would be disproportionate to determine applicable turnover based on the revenue generated by all the services provided by a CTPP regardless of their relevance to DORA, financial entities or the functions (critical or important, or not) being supported.**

We appreciate the Commission's intention to avoid basing the calculation of the fees on the global turnover of the CTPP as per Art. 2 (1). To ensure the practical efficacy of this framework and maintain consistent focus on ICT services supporting financial entities' critical or important functions, **we recommend clarifying in Art. 2 (1) that relevant register of information data will be provided to regulated service providers and that the relevant revenue is for services supporting critical or important functions.**

Moreover, the draft delegated act proposes the application of only a phased broadening of the in-scope turnover as a fall-back under Art. 2 (3). However, **there should be more flexibility in the fallback options where the figures the CTPP can provide entirely include the in-scope turnover in the earlier option.**

Under current Art. 2 (3), if the CTPP does not have audited figures that align exactly with the scope of paragraph 1 or the first option in paragraph 3, then their only option is to provide worldwide revenue. **This is disproportionate where the CTPP is able to provide audited figures that entirely include the in-scope revenue for the previous, more narrow option even if the figures are not limited to that narrower scope.**

Since DORA will designate the EU subsidiary of the CTPP as the legal entity subject to direct oversight, we propose that the basis for the calculation is the audited annual figures of this legal entity. In order to ensure further proportional, considering the revenue of the EU legal entity will include the revenue related to customers of the CTPP that are out of the scope of DORA, we would suggest

the oversight fees paid by a CTPP should not exceed 5% of the total oversight fees collected by the Overseers. This is in line with the approach set out in the Commission Delegated Regulation (EU) No 272/2012 of 7 February 2012 supplementing Regulation (EC) No 1060/2009 of the European Parliament and of the Council with regard to fees charged by the European Securities and Markets Authority to credit rating agencies.

Article 5.2.(c): ‘...a registered credit rating agency as referred to in paragraph 1 shall pay as an annual supervisory fee a part of the relevant amount which corresponds to the ratio of the credit rating agency’s applicable turnover to the total applicable turnover of all registered credit rating agencies required to pay an annual supervisory fee...’

To address this, we propose adding the below underlined text to Article 2:

Article 2

Applicable turnover of critical ICT third-party service-providers for the calculation of the oversight fees

1. For the purposes of Article 3, the turnover of a critical ICT third-party service provider shall be its revenues generated in the Union from the provision of the ICT services **supporting financial entities’ critical or important functions** listed in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554 and provided to the financial institutions listed in Article 2(1) of Regulation (EU) 2022/2554. **Each year, the Lead Overseer shall provide to each critical ICT third-party service provider subject to its oversight the relevant excerpts of the registers of information submitted by financial entities identifying the contractual arrangements and ICT services supporting financial entities’ critical or important functions provided by the critical ICT third-party service provider.**

...

3. Where the critical ICT third-party service provider does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to **or entirely include** revenues generated from the provision of services to financial institutions listed in Article 2(1) of Regulation (EU) 2022/2554, the Lead Overseer shall consider the turnover generated in the Union from the provision of the ICT services listed in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554 irrespective of the type of clients of the critical ICT third-party service provider.

Where the critical ICT third-party service provider does not provide the Lead Overseer with audited figures by the date referred to in paragraph 2 that are limited to or entirely include revenues generated in the Union from the provision of ICT services referred to in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554, the Lead Overseer shall consider the worldwide turnover generated from the provision of those ICT services.

A designated critical ICT third-party service provider shall pay as an annual oversight fee a part of the relevant amount which corresponds to the ratio of the critical ICT third-party provider applicable turnover to the total applicable turnover of all designated critical ICT third-party provider required to pay an annual oversight fee which should not exceed 5% of the total oversight fees collected by the Overseers.

Article 6: Lead Overseer-CTPP Communications

Due to its business sensitive nature, audited financial data provided by the CTPP to the Lead Overseer must be treated as confidential data and for this reason it should not to be disclosed to any third parties.

The information necessary for oversight fee calculation that will be exchanged between the Lead Overseer and CTPP will contain highly sensitive commercial data. Accordingly, it should be treated and safeguarded as confidential, exempt from public disclosure, and used only for the limited purpose of oversight fee calculation.

To ensure these protections, we propose adding the below underlined text to Article 6:

Article 6

Communication between the Lead Overseer and critical ICT third-party service providers

For the purposes of this Regulation, all communication between the European Supervisory Authorities and critical ICT third-party service providers shall take place by electronic means. **All information, other than information related to the estimate of reasonably necessary overall annual costs under Article 1, exchanged between European Supervisory Authorities and critical ICT third-party providers pursuant to this Regulation shall be treated and safeguarded as confidential, exempt from disclosure, and used only for the limited purpose of applying this Regulation.**

FOR MORE INFORMATION, PLEASE
CONTACT:

- **Laura Chaney**
Manager for Digital Transformation Policy
laura.chaney@digitaleurope.org / +32 4 93 09 87 42

- **Vincenzo Renda**
Director for Digital Transformation Policy
vincenzo.renda@digitaleurope.org / +32 490 11 42 15

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org /  @DIGITALEUROPE
EU Transparency Register: 64270747023-20

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 106 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels

T. +32 (0) 2 609 53 10 / www.digitaleurope.org /  @DIGITALEUROPE

EU Transparency Register: 64270747023-20

DIGITALEUROPE

Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, LSEG, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Vantiva, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ

Belgium: AGORIA

Croatia: Croatian Chamber of Economy

Cyprus: CITEA

Czech Republic: AAVIT

Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv

Estonia: ITL

Finland: TIF

France: AFNUM, SECIMAVI, numeum

Germany: bitkom, ZVEI

Greece: SEPE

Hungary: IVSZ

Ireland: Technology Ireland

Italy: Anitec-Assinform

Lithuania: Infobalt

Luxembourg: APSI

Moldova: ATIC

Netherlands: NLdigital, FIAR

Norway: Abelia

Poland: KIGEIT, PIIT, Digital Poland Association

Portugal: AGEFE

Romania: ANIS

Slovakia: ITAS

Slovenia: ICT Association of Slovenia at CCIS

Spain: Adigital, AMETIC

Sweden: TechSverige, Teknikföretagen

Switzerland: SWICO

Turkey: Digital Turkey Platform, ECID

Ukraine: IT Ukraine

United Kingdom: techUK

DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels

T. +32 (0) 2 609 53 10 / www.digitaleurope.org / [@DIGITALEUROPE](https://twitter.com/DIGITALEUROPE)

EU Transparency Register: 64270747023-20