12 September 2023

DIGITALEUROPE's response to the public consultation of European Supervisory Authorities on the first Batch of DORA's Regulatory Technical Standards

This document offers DIGITALEUROPE's contributions to the European Supervisory Authorities' public consultation on the first batch of the Digital Operational resilience Act (DORA)'s Regulatory Technical Standards (RTSs). This includes, *inter alia*, a suggested approach on ICT operations security; how to classify major incidents under DORA; a recommendation to introduce a transition period to establish the templates for the register of information; and an analysis of relevant or non-relevant risk considerations with regard to ICT third-party providers.

We look forward to our feedback being taken on board in the finalisation of the draft RTSs, due to be submitted to the European Commission by 17 January 2024.

Response to consultation paper on RTS on ICT risk management framework (Art.15) and RTS on simplified ICT risk management framework (Art.16)

DIGITALEUROPE's Suggested Approach Regarding the Provisions on Governance

We consider that the reference to "ICT security policies" must be replaced for "ICT risk management framework" as defined in the in Article 6(4) of Regulation (EU) 2022/2554. Moreover, these articles referring topics not directly related to security policies, but ICT management, BCM, etc.

While Article 6 of the DORA Regulation indicates the "ICT risk control function" as an independent line of the ICT risk management function and of the internal audit function, Article 2(1) of the RTS deviates from this approach. The responsibilities assigned to the "control function" seem to be mixed with the responsibilities of the "management function". Particularly for liability:

> Paragraph b) - "managing and monitoring the financial entity's ICT risk", in which clearly, although the monitoring of the entity's ICT risk should be the responsibility of the "control function", its "management" should not be.
>
> Paragraph c) - The control function should not be responsible for defining information security objectives. Their responsibility should be limited to the supervision and/or control of the adequacy of the objectives and of the indicators that the ICT risk management function has defined to monitor these objectives.

Paragraph e) - “Monitoring” is a responsibility that should not be exclusive to the control function. The risk management function will manage ICT risk through monitoring tasks.

Paragraph f) - Understanding the action of "development" as the elaboration first hand of the objective, scope, generation of contents of the awareness programs. It is considered that this should be a task carried out by an expert function in "digital operational resilience" of risk management. Although it is true that the control function should "control" that the content is appropriate to the risk that the entity manages. Moreover, the development of ICT Security Awareness & Operational resilience programs is not commonly assigned to the “control function” role as this process do not require to be independent. We suggest keeping open "who" is accountable for doing this, in order to give entities higher flexibility in the implementation. Consider merging with article 19, that it is not prescriptive of organizational structure.

We suggest that the "monitoring", "follow-up", "management", "supervision", "control", "definition", "development" actions that are the responsibility of the "control function" be clearly determined so that guarantee the independence of such actions.

Section IV: Encryption and cryptography

DIGITALEUROPE’s Suggested Approach on Encryption and Cryptography

Article 6(2): Encryption and cryptographic controls

We are not comfortable with the proposed approach and suggest removing encryption ‘in use’ and the requirement to “process data in use in a separated protected environment” as its feasibility and the benefit of adding this complexity to the business data processes is unclear in the current environments of the financial entities, which already have other measures to protect their data. Proposed change in Article 6(2): In the first sentence, after the words “where relevant” deleted the words “in use,”. In the second sentence, after the works “not possible,” delete the words “financial entities shall process data in use in a separated and protected environment”.

Article 6 indicates the controls that must be considered in the entity's encryption policy. It is requested that said policy should be governed by an objective-based approach, giving the possibility of including any control that meets the established objectives, thus allowing some flexibility.

Article 6(2)(b) sets out the internal encryption rules that must be included in the entity's encryption policy. Clarification is requested as to whether the internal encryption rules are mandatory or if, on the contrary, said decision is delegated to the entity's judgment.

Section V: ICT operations security

DIGITALEUROPE’s Suggested Approach on ICT Operations Security

Article 10(1)(b):

- Article 10(1)(b) indicates that vulnerability and patch management procedures must ensure that automatic vulnerability scans and assessments are performed on ICT assets according to their classification and risk. We consider that, although it is being left to the entity to decide the frequency of this execution based on the risk of the asset

(with the exception of those that provide support to essential functions, for which a minimum weekly frequency is forced), this is not It happens with the mechanism for the discovery of vulnerabilities.

- It is required to specify whether the use of automatic vulnerability scanning tools is mandatory. Thus, our proposal is that the entity can use vulnerability discovery mechanisms that provide a similar level of security or through compensator controls.

Article 10(2)(c):

The suggested approach to vulnerability reporting set out in Article 10(2)(c) of the draft RTS is problematic because it could be read to require disclosure of zero-day vulnerabilities without actionable information to mitigate risks of a vulnerability. Such a disclosure risks counterproductively weakening security because it increases the risk of threat actors' learning of the vulnerability and then equipping with them details and targets for exploitation.

The requirement in paragraph 2(c) to "report" any vulnerabilities to the financial entity should be amended to reflect commonly-accept coordinated vulnerability disclosure principles. In particular, ICT service providers should be required to disclose vulnerabilities to customers only if:

- A specific action is required by the customer in response to the vulnerability (which, in the case of software-as-a-service or cloud services, will rarely be the case, as the underlying software is managed by the ICT service provider not by the customer). This would help to ensure that vulnerability information provided to financial entities is only provided when that information is actionable by the financial entity; and
- Mitigation measures or patches are available. This would help to ensure that vulnerability information does not begin to circulate before a solution to that vulnerability has been identified.

Paragraph 2(c) should be amended as follows:

Proposed amendment: Article 10(2)(c) should be amended to insert after the words "report them to the financial entity" the words "only if appropriate solutions to the vulnerability, such as patches or mitigation measures, have been identified by the ICT third-party service provider and require actions by the financial entity for implementation". Additionally, Article 10(2)(c) should be amended to insert the word "and" before the word "determine" and insert the words "or notify the financial entity of how to implement such solutions, if action by the financial entity is necessary for implementation" after the words "implement appropriate solutions".

Article 10(2)(d) indicates the need to monitor the use of open-source libraries in a general manner, without reference to a risk approach. Complete traceability and control of all updates is technically very complex, with a very high number of changes that, in an entity of a certain size, are not manageable and would represent a worthless cost, which is why it is proposed to clarify that they must be to do depending on the risk of the bookstore.

Article 10(2)(e):

- Procedures already in place to notify relevant counterparts (including customers and third parties as appropriate) about significant vulnerabilities, however we suggest eliminating the requirement to make disclosure of vulnerabilities to the public in general.

- We consider that the procedure to "*establish procedures for responsible disclosure of vulnerabilities to clients and counterparts as well as to the public, as appropriate*" must

be focused on third parties' vulnerabilities related to their ICT services provided to the financial entities in order to report them to the entities under coordinated vulnerability disclosure policies when remediation or mitigation measures (e.g. patches) are available and implemented.

Impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets (without considering their classification and overall risk profile)

We consider this approach is not appropriate and automated weekly scans should be performed on a risk-based approach, focusing on the most critical assets.

Due to the size of the entity and the need to ensure that the tests do not affect the service, weekly execution of the scanners, without taking into account their criticality, is not viable. There are alternative methods for identifying significant vulnerabilities (which are those of immediate identification interest) through intelligence sources that can replace this procedure while maintaining the same level of information about vulnerable assets. Taking into account the risk vision, we believe that the entity should be allowed to define the specific strategy for the continuous management of significant vulnerabilities.

Section VI: Network security

DIGITALEUROPE's Suggested approach on network security

Article 13(1)(a) indicates that policies, procedures, protocols and tools should be developed, documented and implemented that consider the segregation and segmentation of ICT systems and networks according to the essentiality or importance of the function they support, its classification and its risk. However, it is not specified what type of segmentation.

Clarification is required regarding the expected expectations on the type of segregation and segmentation (segregation of subnets, segmentation by access levels, VPN, etc.) and potential evidence that could be requested during supervision.

Regarding section 13(1)(e), the encryption of connections over corporate networks must take into account the possibility of establishing mitigating measures in controlled network environments in addition to encryption.

Section VII: ICT project and change management

DIGITALEUROPE's Suggested approach on ICT project and change management

Article 16(3) indicates that test and development environments must be segregated from the production environment. However, the degree of segregation required is not specified.

Clarification of the level of segregation required in the environments is required (through access credentials, by permissions and roles, different databases, different servers, different networks, etc.).

Additionally, Article 9(4)e of Regulation (EU) 2022/2554 indicates that financial institutions must "apply documented policies, procedures and controls for the management of changes in ICT, (...) that are based on an approach risk assessment and form an integral part of the entity's overall change management process...".

Clarification is requested as to whether the concept "forming an integral part of the general change management process" refers to the existence of a global change management process that includes, in addition to ICT changes, non-ICT changes.

Chapter IV: ICT business continuity management

DIGITALEUROPE's Suggested approach on ICT business continuity management

Article 26 (2) (b)

Testing of ICT services under business continuity plan testing: The wording of Art. 26 (2) (b) does not clearly indicate the origin of the testing to be included. In the interest of legal certainty, we recommend a clarifying amendment to Art. 26 (2):

> "*(b) include the financial entity's testing of the ICT services provided by ICT third-party service providers, where applicable.*"

Article 26(2)(e)

We do not agree with the approach to testing of business continuity plans set out in Article 26 of the draft RTS. In particular, for service providers who offer a standardised service with common controls, it would be inefficient and unnecessary to insist upon "verification" of their business continuity capabilities by every financial entity who used their services. To avoid this duplication of effort, we recommend that the provision be revised to clarify that financial entities may, for the purpose of "verifying" a third-party provider's ability to respond to business continuity challenges, rely upon the ICT service provider's demonstrated adherence to an accepted international standard, such as ISO 22301.

Therefore, we suggest amending Article 26(2)(e) as follows:
Insert at the end of Article 26(e) the sentence "In the case of ICT third-party service providers, such verification may take the form of that ICT third-party service provider providing appropriate evidence of its adherence to a relevant European or international standard (such as ISO 22301:2019) or suitable independent certification".

Chapter V: Report on the ICT risk management framework review

Suggested approach on the format and content of the report on the ICT risk management framework review

Article 28:

We are not comfortable with the proposed approach for the reporting of the ICT risk management framework. We consider that this requirement requires a lot of effort, add bureaucracy and overlaps other regulatory reporting obligations such as SREP ICT Questionnaire, JST regular follow-up meetings, specific OSIs and the new cyber resilience stress test. In addition, this reporting process reduce the flexibility to update the financial entity ICT Framework revision that must be a continuous improvement process.

Given the length and exhaustiveness required for said report, it is proposed to simplify and seek synergies with other reports that are reported to the regulator / other auditors. Writing such a report would involve a large amount of resources.

Response to Consultation paper on RTS on criteria for the classification of ICT-related incidents (Article 18(3))

Overall Approach for classification of major incidents under DORA

- We are concerned that the approach outlined fails to closely sync with the DORA definition of *major ICT related incident*, by losing the link with critical and important functions. We would want to see this link restored throughout the classification process and criteria. Given '*criticality of services affected'* is one of the criteria outlined, we suggest considering the following two possible approaches:
    - Embed the critical/important functions link into each of the criteria (as seen with duration of downtime) OR
    - Make the critical services criteria, which is already a primary criterion, a Mandatory one for classification purposes.
- Additionally, we find the proposed classification matrix too complex and prescriptive, bearing in mind that during an incident financial entity will be focused on incident response and mitigation, and often unable to assess the full set of facts in the early stages. The CP itself acknowledges that "*FEs are best positioned to identify their clients, and hence no further elaboration of this term is proposed in the CP*." This logic should apply across all the criteria, with the conclusion that materiality thresholds should be qualitative binary thresholds, based on a financial entity's judgment. The inclusion of fixed thresholds with fixed amounts does not reflect an approach based upon proportionality.
- We also flag that it will often be difficult to segregate the data under each of the criteria on an EU-only basis. For many international firms with a global presence, it will not be feasible to distinguish the regional impact during an incident.
- We think the Thresholds defined in the RTS are ambiguous and need to be further defined for both primary and secondary criteria. We find a relation between primary criteria 1 and secondary 4, as well as for primary criteria 3 and secondary criteria 2.
- The criteria included for classification of major incidents are not necessary linked with the impact of the incidents.

Additionally, concerning the chart on page 38 - Application of three scenarios on a sample of payment incidents, we think it would be necessary to provide further details on the data and the source of data used to build the scenarios. The example tables in page 38 find that Scenario 3 better classifies incidents, but with a different set of data perhaps the preferred scenario would have been the first or the second one. In addition, in the table the concept of "high level of escalation" is used, but it hasn't been defined.

Specification and materiality thresholds of the criterion 'Clients, financial counterparts and transactions affected', as proposed in Articles 1 and 9 of the draft RTS

Article 1

As written, the specification and materiality thresholds set out in Article 1 and 9 of the draft RTS run the practical risk of triggering reporting requirements for less than major incidents because the term "affected" is without limit. As the proposed standard is currently drafted, *any* effect, regardless of severity, may be sufficient to count against the Article 9 thresholds.

For example, a lag in accessing a customer portal, or in processing a transaction, which has no material impact on any customer's experience (*i.e.*, a slight delay in execution but not a failure of execution) would still be captured by the current materiality threshold and therefore meet the Article 8(2)(a) threshold.
Lack of a clarifying limitation as to what it means to be "affected by" an incident is likely to lead to excessive reporting of relatively minor incidents. That is contrary to the objective of requiring reporting of only major incidents. Overreporting both distracts financial entity resources away from attending to more significant risks and makes it more difficult for supervisory authorities to identify material risks since they will be overburdened with irrelevant reports.
Moreover, when it comes to Article 1(3) the financial entities do not have access to the information that would allow them to assess the knock-on impact from an incident on a client or counterpart, including the implications for a financial entity's business objectives and wider market efficiency. We believe that in practice this criterion would either become meaningless and would be ignored, or it would result in significant amounts of overreporting as firms would have to make significant assumptions. We recommend that this criterion be removed and the focus remain on the impact of the incident on the financial entities' clients, counterparts or transactions.

Therefore, we propose the following changes to Article 1:
At the end of Article 1(1) insert the wording "and which suffer a material degradation in the service provided to them". At the end of Article 1(2) insert the wording "and which suffer a material degradation in the service provided to them under that contractual arrangement". In Article 1(3) after the words "financial counterpart will" insert the word "materially". At the end of Article 1(4) insert the wording "and which suffers a material degradation in the processing of the transaction.".

Article 9 (1)

Materiality thresholds of client numbers affected: We encourage an alignment of threshold numbers with NIS 1, raising the affected client number from 50.000 to 100.000 under (1)(c).

Specification and thresholds of the criteria 'Reputational impact', 'Duration and service downtime', 'Geographical spread' and 'Economic impact', as proposed in Articles 2, 3, 4, 7, 10, 11, 12 and 15 of the draft RTS

Articles 2 and 10 are too broad, since any "media attention" or "complaints from clients" would meet the thresholds – even if the operational/financial impact of the incident is negligible to the financial entity (FE). E.g., a single retail customer's complaint, a mention of an incident in a solitary blog, or on social media could meet this threshold. Therefore, DORA Art. 4 proportionality principle should apply here, thus giving FEs freedom to use discretion in assessing reputation impact.
With regards to Art. 2(c), FE is unlikely to meet regulatory requirements during an incident, hence ESAs should adopt the PSD2 approach targeting those regulatory omissions serious enough to merit the "imposition of supervisory measures or sanctions".

We propose the following changes to Article 2:

Amend Art. 2 sentence 1 to read: "For the purposes of determining the substantial reputational impact of the incident, taking into account the proportionality principle, FEs shall, within reason, take into account the level of visibility that the incident has gained in the market."
Amend Art. 2(a) to read "the incident has attracted attention from general news or sector- or industry- specific media entities". Amend Article 2(b) to insert the words "about the incident" after the word "complaints" and insert the words "at least 1% of" after "from".

Amend Art. 2(c) to replace the words “meet regulatory requirements” with the words “comply with regulatory requirements, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available”.
Amend Art. 2(d) to replace the words “an impact” with the words “a material impact”.

In Art. 3 (1) sentence 2 the notion “the moment the incident occurs" is unclear. From operational perspective, the suggested alternatives “detected” or “recorded in[…] logs or other data sources” can be just as unclear as the primary approach under sentence 1. Instead, it should focus on incident declaration and include the word “declared” before the word “detected”.

In Art. 3(2), “partial” unavailability is not a well-defined concept in an ICT services context and creates uncertainty and may present a very low threshold, leading to overreporting.
We also recommend indicating an end of the incident once an “acceptable” level of service provision is restored. We propose to amend Art. 3(2) to read: “Financial entities shall measure the service downtime of an incident from the moment the service is fully unavailable to clients and/or financial counterparts, or partially unavailable such that the full or partial unavailability prevents or materially degrades the clients’ and/or financial counterparts’ ability to receive the relevant service, to the moment when regular activities have been restored to the level of service.”

With regard to Art. 4, at the time of an incident FEs do not have access to external information that would allow them to assess the impact on clients’ and/or counterparts’ operations in different territories, e.g. an incident in one EU member state (MS) could impact a client located there, but that client may then sell into another MS or have clients outside of the MS. The original FE would have no way to assess this, especially not at the time of the incident. Similarly, FEs do not have access to external information to determine if a third-party provider that may be common is impacted by an incident in different territories. Thus, the current wording of Art. 4 will lead to FEs reporting any incident at any third-party provider, regardless of the materiality of the incident or the likelihood of it servicing FEs in other EU MSs.

We propose focusing on assessing whether the incident has impacted FEs’ activities in other EU MSs as conducted by their branches or other legal entities within those MSs. We recommend that Art. 4(a) and Art. 4(3) should therefore be deleted.

Under Art. 11(b): The use of a 2-hour threshold in service downtime for services supporting critical functions is concerning. There are many services supporting critical functions where the failure would not have a material end-impact. The 2-hour timeframe is also at odds with the standard 24 hours present in other parts of DORA and NIS2. To restore the link with critical/important functions and ensure broader regulatory alignment, we recommend a single timeframe threshold of 24 hours, and recommend deleting Art. 11(b).

The materiality threshold within Art. 12 has lost the reference to “material impact to its entities in two or more jurisdictions” as set out within recital 36. This should be reinserted.

The materiality threshold in Art. 15(1), namely 100,000 euros, is too low and will lead to overreporting. For further clarity, we suggest relabelling this criteria to “firm financial impact”.

Specification and threshold of the criterion 'Data losses', as proposed in Article 5 and 13

The phrases "significant impact" and "critical data" used in Article 13 should be defined to facilitate consistent application of the standards set out in these articles. This criterion should be harmonized with other incident notification regulations.

Therefore, we suggest the following changes to Article 13:
Insert at the end of Article 13 the following sentences: 'Significant impact' means an event materially disrupting the execution of a critical or important function in the provision of services for a client, counterparty, or transaction. 'Critical data' means non-public data necessary for the execution of a critical or important function in the provision of services for a client, counterparty, or transaction."

Specification and threshold of the criterion 'Critical services affected', as proposed in Articles 6 and 14

We agree with the ESAs in raising the existing PSD2 materiality threshold on critical services affected on the basis of internal escalation. The assumption is though that this escalation must be formal escalation through established governance or incident management processes, rather than informal exchange of information between staff. We propose inserting the word "formally" within Article 14 to affirm this assumption. (i.e. "Any impact on critical services in accordance with Article 6, which has been formally escalated.").
There will continue to be significant variation across firms with this criterion, but failure to clarify could unintentionally result in reduced internal reporting which would ultimately backfire.
We have also assumed escalation relates only to the management within the EU, given the scope of DORA.
In addition, clarification is required of what would be considered "service or activities that required authorization" on article 6.
Furthermore, alignment is required with "ECB Cyber Incident reporting" where escalation to top-management is delimited to "outside of any regular/routine reporting", and only when implying decision taking.

Assessing the Feasibility and Impact of Classifying Recurring Incidents under Article 16 of DORA: A Call for Feedback and Insights

We have major concerns with the provisions for Recurring Incidents. With regards to the wording of Article 16:

- The ability to determine that two or more incidents have the same *root cause* will be extremely challenging and burdensome for financial entities since this is unlikely to be known at the time of the incident. This is likely to result in financial entities erring on the side of caution and overreporting incidents as recurring to avoid any regulatory breach. Similarly, the suggestion that *similarity of nature* would suffice is far too broad a term and would likewise result in significant overreporting.
- The RTS should use this opportunity to rebolster the link with critical and important functions, as the definition of major incident set out within the DORA Level 1 text, by specifically requiring the impact of recurring incidents to be limited to the impact upon critical or important functions.
- Additionally, the most practical solution would be to raise the threshold to compensate for the inevitable overreporting. We recommend *four* occurrences should be required for an incident to be defined as recurring under Article 16. Also, a time period must be

applied to the analysis of recurring incidents. Otherwise, the look back period is potentially indefinite.

At a minimum, we propose that Article 16(2) be amended by replacing the word “twice: with the words “four times in a 12-month period” and adding the words “critical or important functions” at the end of the sentence.

Approach for classification of significant cyber threats as proposed in Articles 17

We support the alignment with DORA, and by extension the Cybersecurity Act 2019, in determining a *cyber threat*.

We are concerned though by the highly speculative nature of Article 17(1) on what constitutes a *significant cyber threat*. We do not view the current proposal as workable, particularly whether there is a high probability of materialisation/impact within another financial entity, client, counterpart or third party. Financial entities would not typically have this information available to them, and as a rule would not be in a position to determine whether the conditions set out within Article 8 could materialise in entities other than itself.

Further, rather than having all three components as subjective judgments, we would suggest a more balanced approach, with at least the first criteria purely objective. For example, “a) the cyber threat targeted a critical or important function; and b) if the cyber threat materialised it could fulfil the conditions set out in Article 8”.

Additionally, we highlight that Article 19(3) of DORA obligates financial entities, where applicable, to inform clients of ‘significant cyber threats. The extremely broad definition proposed in Article 17 of the RTS creates huge challenges when complying with this obligation:

- Firstly, firms are duty bound to keep their intelligence confidential by virtue of MoU’s and NDA’s. Whilst exclusion clauses exist to share information with regulators, they do not exist to share information with corporate third parties. Therefore, in attempting to comply with Article 19(3), firms would be in breach of contractual obligations to their intelligence providers & other entities.
- Secondly, providing this information to clients would go against the spirit of the cyber intelligence sharing community:
    - It would put a firm in breach of TLP rules.
    - It could damage trust, with clients inundated with speculative threats that do not materialise, resulting in intelligence sharing becoming less forthcoming.

Key outcomes of DORA, for example increasing information sharing and strengthening resilience, would not be achieved by this provision.

Approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19

We flag that sharing non-anonymised data between member states may pose confidentiality / security risks. Mitigation measures will be needed to address the risk of data loss or breach.

Response to Consultation paper on ITS to establish the templates for the register of information (Art.28(9))

Operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity

Most of third-party ICT providers that are not EU based do not have LEIs. Alternative approaches (as are now accepted in SSM reports) must be allowed.

Evaluating the Inclusion of Material Subcontractors in the Register of Information: Article 4(1)b of ICT Regulation

Financial entities will have difficulties to provide information on subcontractors beyond Rank 3. We suggest reducing responsibility of financial entities only for vendors of Rank 1,2 and 3. Rank beyond 3 should be optional.

Furthermore, the current wording of Article 4(1)(b) is insufficiently clear on what basis financial entities should assess whether a given subcontractor is “material”. These risks creating inconsistency in financial entities’ approaches to assessing materiality, as well as a risk that some entities will incorrectly focus their assessments. We recommend that the wording be amended to clarify that assessing “materiality” should be linked to the operational risk a given subcontractor poses – considering which subcontractors are operationally critical to the financial entity’s underlying functions.

Therefore, we suggest the following changes to Article 4(1)(b):

Insert at the end of Article 4(1)(b) the sentence “For the purpose of this article, a sub-contractor is material if a deficient performance by such subcontractor would cause a disruption to critical or important functions of the financial entity supported by the ICT third-party service provider”.

Implementation of Register of Information

The Register template is a brand-new independent register with few leverages on the EBA Outsourcing Guidelines and will require the following: capture and codification of data fields, implementing RACI both at consolidated and sub-consolidated level, updates and changes in the vendor management tools.

We also recommend introducing a transition period as we have for EBA Guidelines (2 years).

Operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information

Is this requirement only for contracts terminated from January 2025? Or it applies to all contracts terminated since 2020? If the latter, there will be information availability and quality issues.

We question the necessity to keep information for five years. It will produce a large amount of information about services/vendors no longer being used.

Assignments of responsibilities in Article 6

We have concerns on how the sub-consolidated level applies to bank's branches.

Operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at entity level

Dealing with different versions of the register of information and different tables for sub-consolidated and consolidated levels will require relevant efforts to implement the two views.

Assessing the Relevance of Columns RT.02.01.0041 and RT.02.01.0042 in the RT.02.01 Template for Contractual Arrangements

We do not understand why this data are relevant in terms of digital operational resilience. We suggest removing them.

Evaluating Template RT.05.02: Is it Comprehensive Enough for Capturing the Full ICT Value Chain for Financial Entities?

We suggest the template that covers the entire supply chain be required only for critical services.

Data quality of this template is heavily dependent on the third-party provider willingness to provide the requested information.

Articles 2, 5 and template RT.05.02 - Clarification/limitation needed of supply chains in the register:

It is extremely disproportionate to require financial entities to include all subcontractors in the ICT service supply chain in the register, regardless of the materiality of the subcontracted ICT services.

We suggest the amendments below to Art. 2 and 5 and the TP 05.02 guidance on "material" subcontracting:

- In Article 2(2) amend the definition of 'subcontractor' by adding the words "chain' whereby those subcontracted ICT service comprise all or a material part of the ICT services provided by the direct ICT third-party service provider" after the works "'ICT service supply chain'".
- In article 5(d) insert the word "material" before the word "subcontractors"
- In "5. Instructions to fill in template RT.05.02 — ICT service supply chains", under point(iii) insert the word "material" before "the word "subcontractors"

In the table within the "fill-in Instruction" of Column Code "RT.05.02.0060" insert the word "material" before the word "subcontractor" and before the word "contractor".

Proposed taxonomy for ICT services in Annex IV

We must deal with other existing taxonomies such as the EBA outsourcing register (as requested by SSM) and OCIR. We would prefer to use a single harmonized taxonomy.

Assessing the Adequacy of Reporting Instructions in Annex V for Total Asset Value and Financial Indicators of Different Financial Entities

As in Question 7, we do not see why this information is relevant under DORA objectives and suggest removing it.

Assessing the structure of the Register of Information

The only concern is the difficulty to deal with tables 10 and 14 (entity and consolidated/sub-consolidated level)

Evaluating the Adequacy of Information Requested in Register of Information Templates: Balancing the Needs of Diverse Financial Entities and Regulatory Goals

We suggest reducing the most detailed requirements to critical services only.

Response to Consultation paper to specify the policy on ICT services performed by ICT third-party providers (Article 28(10))

Assessing the clearness of Articles 1 and 2 on the application of proportionality and the level of application

Article 1 - risk consideration for the location of the parent company:

In order to appropriately consider the risk factors triggered by geo-political developments, it is not necessary to single out the location of the parent company as the determining risk factor. Where the ESAs target the “exposure to foreign jurisdictions” as an underlying risk consideration, this is not determined exclusively by a provider's parent company. Any presence in a jurisdiction potentially creates exposure to that jurisdiction. For example: An EU headquartered service provider - whose parent company is in the EU - but that has group operations outside the EU is also exposed to foreign law. A more proportionate approach would be to consider geo-political risks generally without a specific focus on the parent company.

Assessing the clearness of Article 3 regarding the governance arrangements

The reference in **Article 3(2)** to a “timely” implementation of contractual changes is insufficiently clear, particularly as any changes would likely require re-negotiation of contracts with relevant third-party ICT service providers. Re-negotiating multi-year service contracts in a rushed manner—potentially on an annual basis—is impractical for both financial entities and service providers, is not consistent with best practice contract management, and would not materially improve operational resilience.

The provision should be amended to clarify that any updates to financial entities’ portfolio of vendor contracts may be made in the ordinary contracting lifecycle – for example, when those contracts expire or come due for renewal. As a backstop, we propose that amendments should be implemented within three years at the latest.

Proposed amendment: insert at the end of Article 3(2) the words “within three years or when those contractual arrangements otherwise fall due for amendment during the ordinary contracting lifecycle, whichever comes earlier”.

Each financial entity is best positioned to determine which ICT services support its critical or important functions. However, to promote consistency and thoroughness, we recommend stating that in **Article 3(3)** the methodology for determining which ICT services support critical or important functions should be based on relevant European or international standards.

Proposed amendment: In Article 3(3), insert after the word “methodology” the words “based on relevant European or international standards”.

Article 3(5) could be read as requiring ICT service providers to “ensure” financial entities’ compliance with the financial entity’s regulatory obligations. This is not appropriate: the financial entity—not its third-party ICT service providers—controls and must be ultimately responsible for ensuring compliance with its legal obligations, consistent with DORA Article 28(1)(a) and Recital 64.
If the intention of this paragraph is for financial entities to assess that ICT service providers are capable of meeting the security standards required by DORA, the wording is currently insufficiently clear.

Proposed amendment: In Article 3(5), replace the words “ensure that the financial entity…” with the words “comply with that ICT third party service provider’s contractual and regulatory obligations in relation to its provision of services to the financial entity”.

As currently drafted, **Article 3(8)** is disproportionate as it would lead to duplication of effort. It would require a large number of different financial entities to conduct regular independent audits of third-party ICT services—such as cloud services—that implement the same standardized functionality and controls for each financial entity.
We encourage the ESAs to recognize that independent certifications or, if needed to supplement these certifications, pooled auditing can achieve the same purposes as a dedicated audit without requiring duplicative resource commitment by financial entities and ICT service providers – as is already recognized by European standards such as the European Banking Authority’s Guidelines on Outsourcing to Cloud Service Providers, and by DORA Article 26(4) – and that the frequency and extent of audits should be commensurate with the level of risk.
Proposed amendment: In Article 3(8) replace the words following “independent review”, with the words “which may where appropriate be achieved by the ICT third party service provider demonstrating that it has obtained independent certification based on relevant European or international standards, demonstrating that it has subjected itself to independent review, or, if necessary to supplement these independent certifications or reviews, pooled auditing against a set of standardized controls. Reviews of such ICT services shall be included in the financial entity’s audit plan, and the frequency and scope of such reviews shall be proportionate to the risks posed by the ICT services and the quality of the independent review described in this paragraph.”

To provide clarity as to the scope of appropriate access, especially for multi-tenant cloud services offerings, **Article 3(9)(d)** should expressly acknowledge that such access should be limited to data and premises necessary for assessing contractual compliance. It would be disproportionate (and could create confidentiality risks) to require service providers to grant unrestricted access to data and premises in unspecified circumstances.

We recommend that the paragraph be amended to align the scope of access with the purpose of Art 30(3)(e) – i.e., to monitor the service provider’s performance of its contractual obligations.

Proposed amendment: Consistent with the existing EBA Guidelines on Outsourcing, insert at the end of Article 3(9)(d) the words “provided by the ICT service provider to the financial entity, so as to enable the financial entity to monitor compliance with the contractual arrangement”.

Assessing the clearness of Article 4

Proposed article 4 requires financial entities to “differentiate” between providers located in an EU member state and providers located elsewhere without any link to risk. That is, the article requires providers to distinguish between EU and non-EU providers even if using a non-EU provider does not present any additional risk.

This goes significantly beyond the data localization obligations already contained in DORA, which cover the risk the draft regulatory technical standard is seeking to address – in particular, Article 30(2)(b) requires ICT service providers to be transparent about the locations their services are provided from.

As drafted, this provision is inconsistent with the purpose of DORA, which aims to mitigate operational risks. It is also inconsistent with existing European guidance such as EIOPA Guideline 12 on Outsourcing to Cloud Service Providers, which provides that entities should “adopt a risk-based approach to data storage and data processing locations” rather than distinguishing the two without any justification, and the European Banking Authority’s Guidelines on Outsourcing Arrangements, paragraph 83 of which recommends a “risk-based approach to data storage and data processing locations”.

We recommend removing the proposed Article 4 as it presents an unnecessary extension of the existing obligation imposed by Article 30(2)(b) of DORA. At a minimum, it should be amended to reflect the intention of DORA and existing European guidance. This would help to clarify that ICT third-party risk strategies should focus on identifying and mitigating genuine operational risks to critical or important services.

Proposed amendment: In Article 4, after the words “shall differentiate”, insert the words “to the extent such differentiation is necessary to address a risk of disruption to that critical or important function”.

Assessing the clearness of Article 5

It is unclear from the current drafting of Article 5(1)(e) what would constitute a “new or material” change to a contractual arrangement. An overbroad application of this article would lead to unnecessary administrative burden for minor or routine changes, without providing any meaningful improvement in operational resilience. We therefore recommend that Article 5 be amended to clarify that the phrase “new or material” is intended to focus on changes that have a material impact on operational risk.

Proposed amendment: In Article 5(1)(e) replace the words “new or material changes to relevant third-party contractual arrangements” with the words “new third-party contractual arrangements or material changes to existing relevant third-party contractual arrangements that materially increase the risk of disruption to a critical or important function”.

Assessing the clearness of Articles 6 and 7

Article 6 imposes inappropriate burdens on covered entities. The range of information required to be compiled to prepare this risk assessment is broad and is likely to significantly

slow commercial agreements and the adoption of new technologies, hence it is important to consider at which point in the contracting and ICT deployment life cycle it would be most appropriate to conduct this risk assessment.
Pre-contracting risk assessments necessarily occur before the financial entity has full appreciation of how the relevant ICT product will be integrated into their ICT environment. In addition, contracting arrangements usually extend over many years during which time both the vendor's product and the financial service entity's use of that product evolves – the risks that these evolutions entail cannot be fully enumerated or mitigated pre-contracting.
Due to these challenges, it would be more effective to focus risk assessments on individual *deployments* of an ICT tool or of particular *vendors*, rather than on each individual contract.

We propose to amend the first sentence of Art. 6(2) to begin as follows:
"The policy referred to in paragraph 1 shall require that:

(a) before entering into a contractual arrangement with an ICT third-party service provider, a vendor risk assessment shall be conducted of that third-party service provider, with such assessment to be applicable to the primary contractual arrangement with that ICT third-party service provider, as distinguished from subsequent arrangements that are subject to the primary contractual arrangement. The vendor risk assessment shall be updated once every three years or when such contractual arrangement otherwise falls due for amendment during the ordinary contracting lifecycle, whichever comes earlier; and
(b) before any deployment of an ICT third-party service provider's services to support critical or important functions, a risk assessment shall be conducted of the specific deployment of that service.

These assessments shall be conducted at financial entity level and…"

We recommend that the due diligence criteria set out in Art. 7 be amended so that they are more clearly focused on operational risks. Under Art. 7(1)(a), it is unclear what objective and measurable criteria a financial entity would apply to conduct meaningful diligence in respect of the range of factors listed there, which may lead entities to rely on subjective preferences. The paragraph provides little explanation of what an "appropriate" organisational structure is to provide ICT services, nor of how a provider's "business reputation" is relevant for the purpose of providing ICT services. Therefore, we propose in Art. 7(1)(a) to remove the words "the business reputation", "abilities," and "appropriate organisational structure, including", and "and professional".
Art. 7(1)(b) does not specify the scope of subcontractor services. It could be read as requiring a generalized inquiry as to reliance on subcontractors, rather than a focus on the relevant use of subcontractors *for the proposed contractual arrangement*. It should be made clear that due diligence in respect of subcontractors is required to assess the vendor's use of subcontractors *for services supporting critical or important functions under the proposed contract,* rather than the vendor's use of subcontractors generally. At the end of Art. 7(1)(b) insert the words "supporting the financial entity's critical or important functions such that a failure of such subcontractors presents a substantial risk of disruption to the specified critical or important functions".

Regarding the provisions in Art. 7(1)(e) concerning ethical, social, and environmental responsibilities, these policy aims are generally laudable, but they exceed the scope of DORA itself and the legislative mandate for development of RTS. As set forth in DORA Recitals 12 and 29, the purpose of the law is to mitigate systemic risk and establish enhanced minimum baselines for financial entities' management of ICT risk. Art. 30 of DORA, which generally requires the adoption of corporate policies and corresponding contractual terms for ICT risk management, does not mention any of the issues in proposed Art. 7(e). To ensure that the RTS conforms, as a matter of principle, to the scope of DORA and the stated objectives and intent of the legislation, we therefore urge the ESAs to remove proposed Article 7(e). Regulation of these issues and other issues beyond the scope of

DORA would be more appropriately left to regulation through legislation specifically developed to address these matters.

Under Art. 7(3) it is not appropriate for the financial entity's policy to require an "audit" at the selection phase. The draft RTS should also be updated to make clear that financial entities should only be required to consider the elements listed in 3(c)(i)-(v) "as appropriate and where available", and we propose to include this wording before outlining points (i)-(v).

Assessing the clearness of Article 8

We are concerned about what types of conflicts of interest the regulator intends to target here and how these should be understood in the case of intra-group providers.

Assessing the clearness of Article 9

Article 9 (1) Contractual clauses for the use of ICT services supporting critical or important functions:

We recommend the following amendment to paragraph 1, in line with our proposed deletion under Art. 3 (9), avoiding a detrimental duplication with DORA Art. 30 in the technical standards. Proposed amendment: In Article 9(1) after the words "set out by Article 30(2)", insert the words "and (3)".

Article 9 (2) - Contractual clauses for the use of ICT services supporting critical or important functions:

The RTS should not limit or exclude the options available to financial entities for audits / testing under DORA Level 1. We recommend the following amendment: at the end of paragraph 2(b) insert the words "*or in the case of pooled threat-led penetration testing a third party contractually engaged by the ICT third-party services provider in accordance with Article 26(4) of Regulation (EU) 2022/2554; or"*

Article 9 (4) - Contractual clauses for the use of ICT services supporting critical or important functions:

The RTS should not create documentary requirements for contracting that exceed the requirements established in DORA Level 1. The procedural requirements under DORA Art 30(1) already cover contract documentation. We propose an amendment for the RTS to better align with its procedural concepts established, which account for the realities of modern contracting.

Proposed amendment: Amend Article 9(4) to replace the words "and signed by" with the words "accessible and executed by". Amend Article 9(4) to insert the words "in accordance with the terms of their contractual arrangement" after the words "by all parties".

Assessing the clearness of Article 10

Article 10(1):

This provision could be enhanced and clarified by further addressing the types of indicators appropriate for monitoring a service provider's compliance and performance. First, the proposed standard does not specifically refer to the use of objectively measurable indicators for monitoring compliance / contractual performance. Use of non-objectively measurable indicators could lead to uncertainty or disagreement about whether service levels have been met. This proposal contrasts with, for example, Article 30(3)(a) of DORA

which explicitly refers to “precise quantitative” performance targets. The technical standard should therefore be amended to clarify that, in line with Article 30(3), a policy should only include objectively measurable indicators to monitor compliance.
Second, the phrase “measures to monitor compliance” is potentially ambiguous. In particular, it is unclear whether this provision would function to mandate audit powers beyond those set forth in DORA and accompany regulatory technical standards more generally. Accordingnly, this standard should be revised to clarify that it is subject to and does not expand audit rights already referred to in the technical standard and DORA more generally.
Third, the reference to “penalties” for service level failures should be amended as contractual “penalties” are not enforceable in many jurisdictions – including member states such as Ireland and key international markets such as the United Kingdom and United States – and it is inefficient to require financial services providers to implement clauses into their contracts that have no legal effect. We recommend instead using the wording from Article 30(3)(a) of DORA – namely “appropriate corrective actions”.
Proposed amendment: In Article 10(1) replace the words “specify the measures” with “specify precise quantitative measures” and the replace the words “including measures” with “including precise quantitative measures”. In Article 10(1) at the end of the first sentence insert the additional wording “relevant to the ICT third party service provider’s services, such as through service levels. Such measures to monitor compliance will not require audit rights in excess of those required elsewhere under Regulation (EU) 2022/2554) or its accompanying regulatory technical standards”. In Article 10(1) replace the word “penalties” with the word “appropriate remedial measures or remuneration”.

Article 10(2)(e):

If the duty to financial entity to perform independent review and compliance audits relates to reviews and audits of the ICT third party services provider, it seems to contradict Article 7 (3) (b) where audits are the preferred option but can be replaced by adequate other sources of confirmation. We suggest adding this option to Article 10 (2) (e).

Assessing the clearness of Article 11

We would like to underline that it is very difficult to carry out actual tests of termination and exit of ICT services providers. We think banks would only be able to undertake partial tests, for example, on the capacity to download the required information timely and in a valid format, so that any other provider can use the information, or as a <tabletop> simulation of the exit plan.

FOR MORE INFORMATION, PLEASE CONTACT:

Vincenzo Renda

Associate Director for Digital Transformation Policy

vincenzo.renda@digitaleurope.org/ +32 490 11 42 15

Laura Chaney

Officer for Digital Transformation Policy

laura.chaney@digitaleurope.org/ +32 493 09 87 42

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 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

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, 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 Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, 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, ZIPSEE
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