EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
DIGITALEUROPE

Contact person

Mr/Ms
Ms

First name
Laura

Surname
Chaney

Email address
laura.chaney@digitaleurope.org

Telephone number

☐ Please tick here if you do not wish your personal data to be published.

General comments

DIGITALEUROPE welcomes the opportunity to provide feedback to the ECB's "Guide on outsourcing cloud services to cloud service providers". We strongly support the efforts of EU policy-makers and regulators to enhance the operational resilience of the EU's financial sector and believe DORA provides an opportunity to deliver on this objective by facilitating the adoption of best-in-class technology by financial entities operating in the EU. The ECB Guide, however, introduces uncertainty for both supervised entities and technology providers given many of the provisions effectively go beyond the requirements set out in the DORA legislative text or are not aligned with the DORA text. Indeed, the proposed Guide is incompatible on several aspects with the requirements set out in DORA, including those related to (i) tech neutrality, (ii) the principle or proportionality, and (iii) the risk-based approach set out in the Regulation. As a secondary effect, such uncertainty would i) be passed to the broad financial sector impacting financial entities' cloud outsourcing strategy and ii) create fragmented approaches at supervisory level.

While the clarification of supervisory expectations by the SSM will, in due course, support the work of financial entities as they look to implement their cloud strategies, the proposed Guide seems to give the SSM a policy-making role which is not in line with the regulatory architecture of the EU. These incremental expectations land at a time when industry is already faced with very short timelines for DORA. Further, given several Level 2 texts are still not final, the Guide risks creating confusion and bifurcating readiness activities. The Guide also risks intra-EU fragmentation of the harmonised regime for ICT services that DORA was intended to create. Further, while we appreciate the need to identify and address the evolving risk profiles that outsourcing generates as a result of the adoption of cloud services, it is always important to remain technology neutral. The Guide does not recognise the overall benefits of this technology in terms of enhanced resiliency and security as widely acknowledged by international regulators and international standard setting bodies, such as the FSB and the BIS. The Guide also puts cloud users and providers at a disadvantage to other financial entities and ICT third party providers as they have to address incremental expectations within an already compressed time frame. We have provided detailed comments to specific sections of the consultation and look forward to the opportunity to share our views at a time of your convenience.

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Please enter all your feedback in this list.
When entering feedback, please make sure that:
- **each comment deals with a single issue only;**
- **you indicate the relevant article/chapter/paragraph, where appropriate;**
- **you indicate whether your comment is a proposed amendment, clarification or deletion.**

Deadline:	15.07.2024

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
1	1. Introduction 1.1. Purpose	1.1	1	Amendment	The Guide states that cloud service usage is inherently riskier than other ICT solutions. 1.1 (first bullet) should be amended to read: '…THE USE OF CLOUD SERVICES CAN BRING NUMEROUS BENEFITS TO THE BANKING INDUSTRY, INCLUDING ACCESS TO INNOVATIVE TECHNOLOGIES, SCALABILITY, FLEXIBILITY, AND ENHANCED SECURITY AND OPERATIONAL RESILIENCE. HOWEVER, IT CAN ALSO INCREASE INSTITUTIONS' EXPOSURE TO SEVERAL RISKS, NOTWITHSTANDING THE COMMITMENT OF CSP TO COMPLY WITH THE HIGHEST STANDARDS'.	CSPs provide improved operational resilience and can effectively lower risks for financial entities by providing them best in class technology, as recognised by international regulators and standards setting bodies such as the Financial Stability Board (FSB). Financial firms with legacy on-premises infrastructure must employ a wide range of security solutions to improve security posture, but this is scattered across a financial entity's IT environment, increasing complexity and operational risks. Further, legacy systems are usually not able to cope with the fast-changing cyber-threat environment, increasing risks for the firm and the overall financial system by not utilising CSPs' services.	Chaney, Laura	Publish
2	1. Introduction 1.1. Purpose	1.1	1	Amendment	The third bullet should be amended as follows: DORA, which focus on 'ENSURING THAT ALL PARTICIPANTS IN THE FINANCIAL SYSTEM HAVE THE NECESSARY SAFEGUARDS IN PLACE TO MITIGATE ICT RISKS, INCLUDING ICT THIRD-PARTY RISKS'.	DORA has broader objectives than establishing qualitative rules protecting against ICT-related incidents.	Chaney, Laura	Publish
3	1. Introduction 1.1. Purpose	Definition	2	Amendment	The ECB Guide exclusively focuses on cloud services whereas DORA focuses on a broader range of ICT services. 'WHILE THE GUIDE FOCUSES ON THE USE OF CLOUD SERVICES, THE SSM THE SSM SUPERVISORY EXPECTATIONS ON CLOUD OUTSOURCING ARE ALIGNED WITH DORA SCOPE AND AIM. THE SAME LEVEL OF RESILIENCE AS PER DORA SHOULD BE ENSURED...'	This focus seems misplaced as Recital 20 DORA notes that CSPs are only "one category of digital infrastructure" and that DORA "applies to all critical ICT third-party service providers", not just CSPs. In this sense, DORA seeks to raise the bar of operational resilience across all types of financial entities' infrastructure by remaining tech neutral. The ECB Guide should make it explicit that the SSM will apply the same level of supervisory expectations related to IT systems, regardless of the type of infrastructure used by the financial entity.	Chaney, Laura	Publish
4	1. Introduction 1.1. Purpose	1.1	2	Amendment	The definition of the 'critical or important function' does not correspond to the definition of Art. 3(22) of DORA Regulation, which is the following: 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law'.	For consistency reasons, we believe the definition in the ECB Guide should be the same one provided in the DORA Regulation.	Chaney, Laura	Publish
5	1. Introduction 1.1. Purpose	Definition	2	Amendment	The ECB Guide uses terms that have already been defined in other documents such as DORA or the EBA Guidelines on outsourcing arrangements (or the BRRD). The 'Definitions of terms for the purpose of this Guide' table should be deleted in its entirety and replaced with a cross-reference to the relevant pieces of legislation that the ECB has in mind.	To try and keep as much consistency of meaning across those different pieces of legislation, the ECB Guide should refer to existing definitions instead of creating its own.	Chaney, Laura	Publish
6	1. Introduction 1.2 Scope and Effect	First paragraph	3	Clarification	The ECB Guide states that 'THE SUPERVISORY REGIME UNDER DORA THAT WILL ENTER INTO FORCE ON 17 JANUARY 2025 HAS BEEN TAKEN INTO CONSIDERATION TO THE EXTENT POSSIBLE' (own emphasis). This sentence should be clarified as it is unclear at present why it would not be possible to take into account the mandatory (including for the ECB) supervisory regime established by DORA.	Given the amount of co-existing and partially overlapping regulations, guides and guidelines in the financial sector, it is key that financial entities and CSPs have as much clarity and simplicity as possible on what rules apply to their activities, and that the order of precedence between these rules be respected.	Chaney, Laura	Publish

7	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	Last sentence	4	Amendment	We agree that financial entities should establish appropriate governance frameworks aligned with DORA, however, 2.1.1 states that the use of cloud services makes 'a clear and unambiguous allocation of responsibilities more challenging'. Subsequently, it also introduces de-facto new requirements for CSPs to have 'equivalent risk management' practices, processes and controls, which are not included in DORA. We propose that in paragraph 3, the word 'EQUIVALENT' should be DELETED AND REPLACED with the word 'RELEVANT'.	Given the multi-tenant environment operated by CSPs, these cannot have "equivalent" risk measures to every single financial entity to whom they provide services as it's practically impossible for a CSP to ensure equivalent compliance with each individual financial entities' risk management practices, processes and controls. Replacing the current wording with "relevant policies and procedures" as present in the Commission Delegated Regulation Art. 9(1) appropriately apportions the burden between CSP and a financial entity.	Chaney, Laura	Publish
9	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	All			Pre-outsourcing analysis is an important aspect of a financial entity's move to the cloud. However, the Guide presupposes the presence of several unsubstantiated risks, including concentration risks, a decline in service quality, price increases, and risks of a multi-tenant environment are present risks rather than unsubstantiated assertions; and also introduces de-facto requirements not present in DORA. Additionally, the Guide fails to account for 'lock-ins' with respect to in-sourced software development and on-premise infrastructure maintained by financial entities. To align proposed sub-subsection 2.1.2 with DORA, the following AMENDMENTS should be incorporated. The sentences 'ASSESS THE CSP'S ABILITY TO PROVIDE THE INFORMATION REQUIRED FOR THESE CHECKS; and 'ENSURE THAT THE CSP HAS ITSELF PROPERLY IMPLEMENTED THE RELEVANT CHECKS' should be DELETED. Additionally, the ENTIRE PARAGRAPH after 'IT IS GOOD PRACTICE FOR A PRE-OUTSOURCING ANALYSIS TO CONSIDER THE FOLLOWING RISKS' should also be DELETED.	The proposed deletions in sub-subsection 2.1.2 should be incorporated as the purported risks are both factually unsubstantiated, not mandated in Art. 28(4) DORA.	Chaney, Laura	Publish
11	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2	6	Amendment	Back-ups of critical functions are an important element of a financial entity business continuity plans, as noted by DORA. However, sub-subsection 2.2.1 of the Guide mandates financial entities to employ multi-provider requirement for critical or important functions. This is not in line with DORA and would potentially lead to increased risks and costs. The text should be amended to read: 'IN ORDER TO AVOID JEOPARDISING THE SECURITY OF NETWORK AND INFORMATION SYSTEMS, THE ECB CONSIDERS THAT BACK-UPS OF CRITICAL OR IMPORTANT SYSTEMS SHOULD BE STORED IN LOGICALLY AND PHYSICALLY SEGREGATED SYSTEMS'.	Art. 12(3) states that backup systems should be 'physically and logically segregated' from source ICT systems [in relation to entities own systems], this does not mandate a multi-provider strategy. Art. 6(9) DORA states that a multi-vendor strategy is not mandatory, so it does not follow that the ECB would interpret such strategy as being mandatory.	Chaney, Laura	Publish
12	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	3	6	Deletion	DORA Art. 12 (6) addresses recovery procedures and methods, while ECB Guide goes further adding unclarity and complexities related to perform exit 'under stress' or exit 'without cooperation from the CSP'. We propose to delete the paragraph 'For the purposes of Art. 12(6) of DORA, the ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question'.	ECB guidance is not aligned with DORA (Art.12) and seems to suggest unrealistic time objectives for exit plan. This misalignment is also observed in paragraph 2.2.2 (orderly transition under the exit plan and ability to bring data and applications back on-premises). See also amendment proposal below (paragraph 2.2.2).	Chaney, Laura	Publish
13	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Whole section	7	Clarification	Sub-subsection 2.2.2 should be clarified to align the ECB Guide with DORA, reduce the potential increased costs and undue burden on financial entities using cloud, and avoid the use of varied industry terms.	As currently draft, 2.2.2 (i) deviates from the requirements outlined in Art. 6(8) DORA; (ii) may increase costs on financial entities through the imposition of costly architecture requirements not included in DORA; and (iii) uses terminology that is undefined within the ECB Guide and not used uniformly amongst CSPs. Further, the Guide is likely to cause undue burden and cost on financial entities that use CSPs rather than address ICT risk. These architecture requirements are not present for other ICT services. For example, the ECB does not suggest that financial entities are required to maintain multiple data centres in different locations if they have solely on-premises infrastructure.	Chaney, Laura	Publish
14	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	First paragraph, fifth bullet point	7	Amendment	Note 7 for the 'FOR CRITICAL FUNCTIONS' term in the fifth bullet point of the first paragraph should refer to DORA, instead of the EBA Guidelines.	DORA being the only legally binding requirement, it is its definitions that should prevail over any other.	Chaney, Laura	Publish
15	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Last bullet	7	Amendment	The last bullet of 2.2.2 should be amended as follows: The institution must retain the ability to bring data and applications back on-premises OR TRANSFER DATA AND APPLICATIONS TO AN ALTERNATIVE PROVIDER. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP.	Art. 28(8) DORA does not limit exit strategies and plans to bringing data and applications back on-premises. Instead, Article 28(8) refers to both" transfer[ing] them to alternative providers or reincorporat[ing] them in-house". The ECB should not exclude options explicitly permitted under DORA and we recommend that this text is clarified.	Chaney, Laura	Publish

16	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	Whole section	8	Amendment	Reliance upon disaster recovery certifications or third-party certifications is a scalable and widely acknowledged to be an appropriate and practical proxy for financial entities as part of comprehensive ICT risk management. As drafted sub-subsection 2.2.3 is not aligned with DORA and introduces de-facto new requirements. Hence, sub-subsection 2.2.3 should be amended to DELETE the FOUR SENTENCES in paragraph 1 'ON THE BASIS OF THESE PROVISIONS, THE ECB UNDERSTANDS THAT AN INSTITUTION SHOULD TEST ITS CSP'S DISASTER RECOVERY PLANS AND SHOULD NOT RELY EXCLUSIVELY ON RELEVANT DISASTER RECOVERY CERTIFICATIONS. WHEN CONDUCTING DISASTER RECOVERY TESTS WITH THE CSP, THE INSTITUTION SHOULD PERFORM SPOT CHECKS AND/OR TESTS AT SHORT NOTICE IN ORDER TO ASSESS ITS READINESS FOR AN ACTUAL DISASTER EVENT. THE TESTING PLAN SHOULD COVER A VARIETY OF DISASTER RECOVERY SCENARIOS (INCLUDING COMPONENT FAILURE, FULL SITE LOSS, LOSS OF A REGION AND PARTIAL FAILURES). THESE SCENARIOS SHOULD BE TESTED REGULARLY IN ACCORDANCE WITH THE INSTITUTION'S STRATEGY AND IN LINE WITH ITS BUSINESS CONTINUITY POLICY AND REQUIREMENTS'.	Art. 40 DORA notes that a Lead Overseer may rely upon relevant third party certifications. If such certifications are an acceptable mechanism for the Lead Overseer to evaluate a CSP, it reasons that those certifications would also be valid for financial entities in testing disaster recovery. Public cloud services are multi-tenant environments. In this context, disaster recovery (DR) testing must be conducted in a way that safeguards all the CSP's customers. This is only possible with careful planning and robust guardrails. An expectation that each institution directly and individually test the CSP's DR plans exposes all the CSP's customers to an undue operational risk (this includes other institutions and financial entities). This is especially the case if the expectation is for institutions to conduct tests at short notice.	Chaney, Laura	Publish
17	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	Whole section		Deletion	As drafted, paragraph 2.2.4 of the Guide fails to acknowledge how financial entities can architect their cloud environments to avoid concentration risks; and differs from DORA in its specific requirements on how to address these risks. Sub-subsection 2.2.4 should be amended to remove: (i) in the first paragraph, the sentence beginning '[C]ONCENTRATION RISKS ARE GENERALLY EXARCERBATED'; (II) in the second paragraph, the sentence beginning with '[W]HEN ASSESSING CONCENTRATION RISKS,'; and (iii) at the end of the second paragraph, the clause 'but also by taking into account…with potential effects on concentration risks'.	Proposed sub-subsection 2.2.4 is unaligned with DORA. Recital 67 DORA stated that DORA intends to promote a balanced approach to concentration risk and 'it is not considered appropriate to set out rules on strict caps and limits to ICT third-party exposures'.	Chaney, Laura	Publish
18	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes	First paragraph	9	Deletion	Delete reference to NIS 2 (as well as on pages 6 and 7).	Recital 16 DORA states that 'this Regulation constitutes *lex specialis* with regard to Directive (EU) 2022/2555 [NIS 2]'. DORA takes precedence on NIS 2 for financial entities under the scope of DORA and their ICT third-party providers, so these references to NIS 2 only generate confusion	Chaney, Laura	Publish
19	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	Second paragraph		Amendment	The second paragraph of 2.2.4 should be amended as follows: When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services (such as increased provider lock-in, less predictable costs, increased difficulty of auditing, concentration of provided functions and lack of transparency regarding the use of sub-providers), alongside aspects of data LOCATION~~RESIDENCY~~.	We believe the reference to 'data residency' in Section 2.2.4 refers to an expectation that the institution considers the location of the institution's data. However, given how the term is commonly used, the reference to 'data residency' could be read as an expectation that institution's data be located in a specific location. This would be inconsistent with Recital 82 DORA which says 'This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union'. To avoid this confusion, we recommend using the term 'data location'.	Chaney, Laura	Publish
20	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes	1		Clarification			Chaney, Laura	Publish

21	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes	Whole section	10	Amendment	DORA does not require financial entities to use a multi- vendor strategy. Art. 6(9) DORA explicitly notes that the use of a multi-vendor strategy is optional rather than mandated. Affirmatively linking a multi-vendor strategy with increased security appears to contradict DORA as it implies this approach is mandatory. It is also unsubstantiated. When not properly managed a multi- vendor strategy can increase security risks. proposed sub-subsection 2.3.1 uses the phrase 'micro-segmentation technologies' without defining the term, which is likely to cause confusion for financial entities and providers. If proposed sub-subsection 2.3.1 is intended to be aligned with DORA, the term should be revised to either use a commonly understood term within the industry or a term that is defined or understood within DORA. Hence, 2.3.1 in the Guide should be AMENDED to DELETE: 'IN ADDITION TO ENCRYPTION TECHNOLOGY, INSTITUTIONS MAY ALSO (I) USE MULTI-CLOUD TECHNOLOGIES THAT ENHANCE THEIR DATA SECURITY, (II) APPLY MICRO-SEGMENTATION TECHNOLOGIES OR (III) ADOPT OTHER DATA LOSS PREVENTION MEASURES'.	The proposed text in the Guide should be amended so it does not introduce requirements that are not contemplated in DORA.	Chaney, Laura	Publish
22	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	First paragraph	10	Deletion	We would challenge and delete the 'advice' mentioned in the first paragraph ('Institutions are advised, therefore, to draw up a list of acceptable countries where their data can be stored and processed, depending on the data in question. That Assessment should ideally take account of legal and political risks surrounding outsourcing (e.g. the risk of litigation or sanctions'.)	This requirement (or 'advice'), which infers that some countries are unacceptable locations for hosting and processing data, is not aligned with DORA's Recitals 82 and 83 ('Critical ICT third-party service providers should be able to provide ICT services from anywhere in the world, not necessarily or not only from premises located in the Union'. - Recital 83 and 'This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union" -Recital 82.)	Chaney, Laura	Publish
24	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	Second paragraph		Amendment	The second paragraph of 2.3.4 should be amended as follows: An institution's IAM policy should be extended to cover cloud assets and IMPLEMENTED ~~EXECUTED~~ when entering into a cloud outsourcing arrangement. This policy should cover both technical and business users	We believe the reference to 'executed' in Section 2.3.4 refers to an expectation that the institution's IAM policy should be *implemented* when entering into a cloud outsourcing arrangement. However, given how the term is commonly used, the reference to 'executed' could be read as an expectation that institution and the CSP *sign* the institution's IAM policy or otherwise incorporate it in the contract. An institution's IAM policy is internal to the institution and for security reasons should not be shared with the CSP. Nor is it appropriate for an institution's IAM policy to be included in the contract with the CSP because it exclusively contains responsibilities for the institution that are entirely within the institution's control when using a cloud service.	Chaney, Laura	Publish
26	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.1		Deletion	As drafted, 2.3.4.1 introduces requirements that are not included in DORA, but also will not increase the resiliency of financial entities. Sub-subsection 2.3.4.1 should be DELETED. The section should be deleted, or, as a minimum, 2.3.4.1 should be clarified as follows: The ECB considers it good practice for institutions to CONSIDER~~AGREE~~ individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT ~~CONFIGURING THE CLOUD ENVIRONMENT~~. If this is not feasible, the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties. Any deviations can then be analysed and addressed using risk mitigation measures.	DORA does not require financial entities to have individual clauses when they use cloud services. Further, it is unclear what the Guide considers 'best practices' when configuring cloud environments. While DORA does require contractual clauses, the negotiation of individual clauses is not required and unnecessary given the control financial entities maintain over their environments in the cloud. Public cloud services are one-to-many, standardised services. They operate in the same way for every customer. We agree that it is important for institutions and CSPs to understand their different areas of responsibility and that should be addressed in the contract. That said, it is not appropriate to expect institutions to include individual clauses in the contract with the CSP on a configuration-by-configuration basis. Firstly, cloud services are typically contracted for under a framework contract or master services agreement. This applies to all workloads/use cases that the institution chooses to configure and deploy and the institution can choose to deploy new workloads or reconfigure existing workloads at any time. In this context, it is not practical or appropriate to expect the institution to include individual clauses in their contract with the CSP each time they *configure* the cloud environment. Instead, the institution should focus on whether the contract and their use of the services aligns with their defined requirements during the pre-deployment phase. Secondly, configuration is a customer responsibility in the public cloud context. The CSP's obligations don't change based on how the customer chooses to configure their cloud environment. The CSP's obligation remains to ensure the features and functionality operate as described. As this obligation is universal (and not dependent on specific configuration), an expectation that institutions agree individual clauses with the CSP when configuring the cloud environment is redundant and confusing.	Chaney, Laura	Publish

27	2.4 Exit strategy and termination rights 2.4.1 Termination rights	First two paragraphs		Deletion	The first two paragraphs of Section 2.4.1 should be deleted.	Art. 28(7) of DORA is clear about the circumstances in which financial entities should be able to terminate. The ECB's expectations regarding grounds of termination overlap with and in many cases go beyond the four requirements in Art. 28(7). For example: 'Ongoing inadequate performance' overlaps with and sets a lower and less precise threshold than Art. 28(7)(a), (b) and (c); 'Serious breaches of the contractual terms, or of the applicable law or regulations' completely overlaps completely with Art. 28(7)(a) but uses different words; 'An excessive increase in expenses under the contractual arrangements that are attributable to the CSP' does not clearly map to any part of Art. 28(7). This will add significant confusion to contracting for cloud services without a clear foundation within or consistency with DORA. It also appears to single-out and prejudice cloud services despite similar considerations applying to all ICT services and outsourcing. The ECB's proposal to include a list of scenarios that could trigger a grounds of termination is also confusing. Termination rights should be based on whether the grounds of termination in Art. 28(7) of DORA are in fact present. This is inherently a subjective analysis based on the relevant circumstances. It cannot be based on a standard list of events that may or may not in reality trigger grounds for termination.	Chaney, Laura	Publish
28	2.4 Exit strategy and termination rights 2.4.1 Termination rights	Penultimate paragraph		Amendment	The penultimate paragraph should be deleted, or, as a minimum amended as follows: On the basis of the requirement concerning key contractual provisions contained in Art. 30(2)(a) of DORA, institutions should ensure that WHERE RELEVANT all ~~SUPPLIERS OF SUBCONTRACTED SERVICES SUPPORTING THE CSP~~ SUBCONTRACTORS THAT EFFECTIVELY UNDERPIN THE PROVISION OF THESE ICT SERVICES (I.E. ALL THE SUBCONTRACTORS PROVIDING ICT SERVICES WHOSE DISRUPTION WOULD IMPAIR THE SECURITY OR THE CONTINUITY OF THE SERVICE PROVISION) comply WITH EQUIVALENT ~~THE SAME~~ contractual obligations that apply between the institution and the CSP, (including obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and back-ups) if termination rights are exercised.	The conditions under Art. 30(2)(a) of DORA are the subject of regulatory technical standard to be prepared by the ESAs pursuant to Art. 30(5). The ECB should not propose overlapping expectations before the final version of the RTS is available. In particular, we note that the ECB's consultation closes on 15 July 2024. This is two days before the DORA deadline for the ESAs to submit the RTS to the Commission. Given the circumstances, no stakeholders responding to the ECB's consultation will have been able to assess them against the final RTS. We are concerned that this does not provide a meaningful period of consultation. Beyond the procedural concerns, the ECB's proposal raises a number of substantive concerns in light of the draft RTS. Firstly, the ECB proposal uses the phrase 'suppliers of subcontracted services supporting the CSP'. This phrase is not used in DORA or the draft RTS. Therefore, it is not possible to clearly map it to definitions in the legislative acts, some of which are still to be determined in the RTS. Secondly, the draft RTS contains requirements about flowing down contract terms to subcontractors that overlap with this proposal (see Art. 3 and 4 of the draft RTS). The ECB's proposal that subcontractors be subject to the 'same contractual obligations' is more consistent with a traditional outsourcing service model and is not compatible with cloud services. •It is feasible in a **traditional outsourcing service model** for the primary contract to be replicated in the subcontract or for the primary contract to dictate details of the subcontract. This is because, in the traditional context: - The primary provider typically transfers an entire ICT service (all the services under the primary contract) or a discrete part of the service (all the services in one or more delivery schedules of the primary contract) to the subcontractor. - The service is one-to-one (i.e. subcontractors are engaged to support specific customers on an individual basis). So there's only one set of primary contract terms that need to be passed-through to subcontractors. •This is not how subcontracting works in the **public cloud service model:** - The CSP may subcontract components of the service (e.g. technical support). These components are building blocks of the overall service, but they don't always have a one-to-one relationship with the service provided by the CSP. Therefore, it is not possible to simply replicate terms in the primary contract in the subcontractor. Instead, the primary contract should set these expectations as between the financial entity and the provider and require the provider to ensure that they are addressed in the subcontract without dictating how. - The service is one-to-many. A single subcontractor engaged by a CSP is relevant to potentially all the CSP's customers. Although the CSP will have a separate contract with each financial entity (this could be hundreds of financial entities), it will only have one contract with the subcontractor. It is not possible for that contract to replicate the terms of all the individual financial entity contracts.	Chaney, Laura	Publish

29	2.4 Exit strategy and termination rights 2.4.1 Termination rights	Whole section	12-14	Deletion	As drafted, 2.4 introduces requirements that are not included in DORA, are unrealistic and too rigid while not increasing the resiliency of financial entities. Sub-subsection 2.4 should be DELETED in its entirety.	DORA does not require such detailed and, at times, impractical termination or exit plans but rather gives the parties the flexibility to agree termination rights, exit plans and supply chain monitoring tailored to and appropriate for each of their individual, specific contractual arrangement. The ECB Guide is adding burdens (drawing exit plans *before* systems go live, flowing down of "the same contractual obligations" and termination rights to subcontractors, granular technical exit plans) that are not mandated by DORA and that could create additional risks to the security, integrity and confidentiality of systems and data (e.g., independent verification of the feasibility of each exit plan).	Chaney, Laura	Publish
30	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.3			Sub-subsection 2.5.3 should be amended to better align with the DORA text, reduce the possibility for increased misinterpretations and costs for financial entities, and remove unsubstantiated assertions that CSPs can commit fraud ('manipulation'). Specifically, it should be AMENDED to read: 'Taking this into account, the ECB recommends that financial entities use standard contractual clauses when outsourcing cloud computing services, WHERE APPLICABLE AND RELEVANT TO THE FINANCIAL ENTITY'S USE OF CLOUD COMPUTING SERVICES'. Proposed sub-subsection 2.5.3 should also be AMENDED to DELETE the sentence beginning 'IF CONTRACTUAL PROVISIONS ARE STORED ONLINE, THE PROVIDER SHOULD BE REQUIRED TO SIGN A SEPARATE DIGITAL OR PHYSICAL COPY TO PREVENT ANY RISK OF UNILATERAL CHANGES' as it represents an unsubstantiated assertion, does not reflect the one-to-many cloud model, and is not required in DORA.	Sub-subsection 2.5.3 indicates CSPs could make unilateral changes fraudulently or without notification. This is unsubstantiated and not reflective of how changes are made or notice is provided.	Chaney, Laura	Publish
31	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	Whole section (2.5.3)		Deletion	Section 2.5.3 should be deleted	The ECB's proposed recommendation that financial entities use standard contractual clauses seems premature when no such standard contractual clauses yet exist. Also, it is unclear how financial entities are meant to apply the four recommendations about specific clauses when it is the public authorities - and not the financial entities - that will define the content of the standard contractual clauses referenced in Art. 30(4) of DORA. As a public authority, the ECB is well-positioned to contribute to any standard contractual clauses referred to in Art. 30(4). Rather than directing best practices at financial entities, it would be more effective to direct them to the public authorities drafting those clauses. In this context, the only appropriate obligation or expectation on financial entities is one to consider relevant standard contractual clauses as-and-when they become available. We urge the ECB not to pre-empt this by positively recommending the use of as-yet undefined clauses. If the ECB's intent is to propose best practices for contracts other than those referenced in Art. 30(4), then it is not clear how these expectations relate to (or avoid conflicting with) Articles 30(2) and (3), which clearly set out the requirements for contracts under DORA. Therefore, at a minimum, we encourage the ECB to provide more clarity regarding the development of SCCs that would be applicable to such a scenario.	Chaney, Laura	Publish
32	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	Last sentence	16	Deletion	The last sentence of this section which states 'INSTITUTIONS SHOULD USE CONTRACTUAL CLAUSES TO ENSURE APPROPRIATE INCIDENT AND MONITORING REPORTS, ENABLING ONGOING ASSESSMENT OF OUTSOURCES FUNCTIONS' should be deleted.	This is not required by DORA.	Chaney, Laura	Publish