EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
Bitkom e.V.

Contact person

Mr/Ms
Ms

First name
Sarah

Surname
Palurovic

Email address
s.palurovic@bitkom.org

Telephone number
4915114824853

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

General comments

Bitkom and its members took the opportunity to provide feedback on the “Guide on outsourcing cloud services to cloud service providers” by the ECB. The new ECB Guide draft contributes to a partially unaligned and overcrowded regulatory landscape, undermining operational resilience in the EU financial sector. Initially, the introduction of DORA was intended to reduce the fragmentation of existing supervisory practices and harmonize the rules for operational resilience. If DORA is aimed at harmonization within the EU, the question arises why it is necessary to issue various guidelines from the ECB, EBA, ESMA, etc., on topics such as cloud outsourcing in addition to partially already existing requirements from national financial supervisory authorities and national laws.

The ECB Guide introduces uncertainty for both supervised entities and technology providers, as many of its provisions go beyond the requirements set out in the DORA legislative text or are partially not aligned with it. This uncertainty could be passed on to the broader financial sector, impacting financial entities’ cloud outsourcing strategies and creating fragmented approaches at the supervisory level. While the clarification of supervisory expectations by the Single Supervisory Mechanism (SSM) will eventually support financial entities in implementing their cloud strategies, the guide appears to give the SSM a policy-making role that is not in line with the EU's regulatory architecture. These incremental expectations come at a time when the industry faces very short timelines for DORA, and with several level 2 texts still not final, the guide risks creating confusion and bifurcating readiness activities. This also risks intra-EU fragmentation of the harmonized regime for ICT services that DORA was intended to create. The introduction of DORA was meant to reduce the fragmentation of previous supervisory practices and harmonize the rules for operational resilience. By issuing the new guidelines now, the ECB is creating additional uncertainty. While many companies are in the middle of their DORA implementation processes, further considerations and evaluations need to be made regarding companies' cloud outsourcing.

We recommend considering the publication of one harmonized guideline on cloud outsourcing together with the EBA and other bodies to enable supervised institutions to comply with and follow supervisory expectations.

Additionally, while we recognize the need to address the evolving risk profiles that cloud services adoption generates, it is essential to remain technology-neutral. The guide does not adequately recognize the overall benefits of this technology in terms of enhanced resiliency and security, as acknowledged by international regulators and standard-setting bodies like the FSB and the BIS.

In case of additional follow-up questions or the desire to exchange more extensively about proposed amendments, deletions or clarifications, we are gladly available for any inquiries and follow up discussions.

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 ECB Guide on outsourcing cloud services to cloud service providers (the "ECB Guide") is intended to be read in conjunction with Regulation (EU) 2022/2554 ("DORA"), it should be aligned with DORA. DORA provides the regulatory framework, processes and standards for cloud service providers. The introduction of new requirements in the ECB Guide that extend beyond DORA undermines having consistent standards and guidelines, and will create ambiguity for financial entities. As presently drafted, the ECB Guide focuses solely on cloud services, contrary to the scope of DORA, and asserts without substantiation that cloud service usage is both highly concentrated and inherently riskier than other ICT solutions. DORA and other regulations are intended to be technology agnostic and focused on risks. The ECB's hyper focus on cloud services, is contrary to this and singles out cloud services without clear justification. Further, the definitions used in the ECB Guide are unaligned with those in DORA, creating confusion for financial entities. The ECB Guide states that it provides an understanding of new legal acts, including DORA, but only focuses on cloud services rather than all ICT services. DORA is not only applicable to cloud services, but all "ICT services". Article 1 of DORA is focused on a high common level of overall digital operational resilience, not just the resilience of cloud services. "ICT services" is broader than cloud services. If the ECB Guide is intended to be the "ECB's understanding of those specific rules", it should focus on all ICT services rather than focusing solely on cloud so as to ensure all types of ICT services are subject to the same requirements regarding resilience and security. Such an approach is in keeping with that previously adopted by the European Banking Authority pursuant to the 'EBA Guidelines on outsourcing arrangements and DORA itself. By making statements such as "while the use of cloud services can bring numerous benefits to the banking industry … it also increases institutions' exposure to several risks", the ECB Guide subsection 1.1 presupposes that the use of CSPs both increases a financial entity's risk, and also that the cloud services market is highly concentrated without substantiation. Further, it assumes using a single provider leads to higher operational risk. In response to statements made by the ECB in relation to concentrated risks, choosing a single service provider is not indicative of concentration risk and may have benefits in terms of resilience and security for financial entities. Concentration can be beneficial to reduce complexity, reduce attack vectors, and maximise training gains for such concentrated solutions. Cloud services are neither concentrated from a market perspective nor a geographic or service perspective. If the purported concentration risk pertains to concentration of services or geographic concentration risk, both can be mitigated through financial entities appropriately architecting their own environments. The use of on-premises infrastructure is inherently riskier than cloud services. Financial entities are entitled to their choice of infrastructure (cloud service, on-premise or a combination) and to evaluate the operational resilience and any associated risks, and other factors. During this evaluation, financial entities may determine lower risks in cloud services, especially in light of a fast-evolving cybersecurity threat landscape. Cloud services, can provide solutions for some problems faced by companies with on-premises infrastructure such as, a wide range of security problems. While financial entity customers need to appropriately architect their frameworks', increased resilience is a feature of the cloud. The CSP's one-to-many model enables both more centralized security and significant more investment in security policing than a company could provision itself. Accordingly, proposed section 1.1. should be AMENDED to DELETE the last two sentences in the first bulleted paragraph: "WHILE THE USE OF CLOUD SERVICES CAN BRING NUMEROUS BENEFITS TO THE BANKING INDUSTRY (INCLUDING ACCESS TO INNOVATIVE TECHNOLOGIES, SCALABILITY AND FLEXIBILITY), IT ALSO INCREASES INSTITUTIONS' EXPOSURE TO SEVERAL RISKS. THE CLOUD SERVICES MARKET IS HIGHLY CONCENTRATED, WITH MANY CSPS RELYING ON PROPRIETARY TECHNOLOGIES, AND THOSE TECHNOLOGIES MUST BE UNDERSTOOD, ASSESSED AND MONITORED BY THE INSTITUTIONS IN QUESTION." The definitions for purposes of the guide are unaligned with Article 3 of DORA and require amendment. The definitions of "critical or important function" and "ICT asset", in particular, are inconsistent. While the ECB's Guide is stated to be non-binding, these competing definitions will cause confusion and difficulties for financial entities attempting to comply with both the Guidelines and DORA. EACH DEFINITION SHOULD BE REPLACED BY THE DORA DEFINITION.	The proposed amendments should be implemented to: (i) avoid confusion caused by aspects of the ECB Guide: (i) differing from DORA; and (ii) introducing additional requirements on financial entities and by extension CSPs; and (ii) avoid introducing undefined concepts, such as "concentration risk" that are not factually substantiated in the ECB Guide or reflective of how CSPs provide services to customers. The proposed amendments align the ECB Guide with DORA, which is the stated purpose of the ECB Guide.	Bitkom	Publish
2	1. Introduction 1.2 Scope and Effect	1.2	3	Clarification	As drafted, proposed subsection 1.2 is also unaligned with DORA's scope and should be amended to avoid confusion and conflicting requirements for financial entities. Although the ECB Guide states that it should be "read in conjunction with DORA" and that DORA has priority, it deviates from DORA in several respects. There is a misalignment between the stated intention of this subsection 1.2 and several other parts of the ECB Guide that establish new de-facto requirements in addition to those present in DORA, including: (i) the introduction of a multi-vendor requirement for 'critical or important systems' in section 2, sub-subsection 2.2.1 which is not required by Article 12 of DORA, despite the citation of Article 12. In addition, Article 6(9) of DORA makes clear that while entities may establish a multi-vendor strategy they are not required to; and (ii) the introduction of new termination rights at section 2, sub-section 2.4.1 not contemplated by DORA (Article 28(7)). The ECB Guide exclusively focuses on cloud services whereas DORA focuses on a broader range of ICT services. 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. As noted above in section 1.1, DORA and other regulations are intended to be technology agnostic and focused on risks. The ECB's singular focus in this sub-section, is contrary to DORA and other regulations. Please elaborate on the hierarchy of the documents and regulatory publishments. In many places, DORA sets out less stringent requirements than the ECB paper and the EBA guidelines on outsourcing do not address the topic of the cloud separately. It is therefore unclear what significance this paper now has. As drafted, the ECB Guide could be interpreted as the ECB creating additional regulation by instituting requirements in addition to those present in DORA and to clarify that the ECB is not taking on a regulatory function or instituting additional requirements than those present in DORA, proposed subsection 1.2 should be AMENDED to ADD the following text after the sentence beginning "The ECB Guide should be read in conjunction with the DORA regulatory framework: "THE ECB GUIDE IS NOT INTENDED TO INSTITUTE REQUIREMENTS ON CSPS OR FINANCIAL ENTITIES NOT ALREADY PRESENT IN THE DORA REGULATORY FRAMEWORK."	The proposed amendment should be incorporated into draft subsection 1.2 to clarify that the ECB Guide does not expand upon DORA through the imposition of additional new requirements. As the ECB Guide notes that it "does not lay down legally binding requirements" nor "replace the relevant legal requirements stemming from Union or national law", this amendment clarifies that the ECB Guide is not intended to introduce inconsistency or additional requirements in relation to DORA.	Bitkom	Publish
3	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	2.1.1	4	Clarification	ECB states that institutions should ensure that their CSPs have established equivalent risk management practises, procedures and controls. How shall institutions ensure this exactly? Please provide clarifying examples.	The requirement is unclear yet and needs concretization.	Bitkom	Publish
4	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Deletion	It is important for institutions to undertake a "pre-outsourcing analysis" prior to entering into new cloud outsourcing arrangements to assess relevant risks. As drafted, proposed sub subsection 2.1.2 of the ECB Guide: (i) assumes the presence of unsubstantiated risks; and (ii) introduces new additional requirements than those present in DORA. It is unclear how proposed sub-subsection 2.1.2 will assist financial entities in undertaking a pre-outsourcing analysis. Specifically, proposed sub-subsection 2.1.2 appears to require additional aspects of a pre-outsourcing analysis not present in Article 28(4) DORA and the Commission Delegated Regulation. Proposed sub-subsection 2.1.2 presupposes that concentration risks, a decline in service quality, price increases, and risks of a multi-tenant environment are present risks. The basis for this is unclear and none of these asserted risks are part of Article 28(4) DORA's mandated pre-outsourcing analysis. As noted in the response to section 1.1, financial entities are entitled to their choice of infrastructure and to evaluate risks, such as those related to vendor lock-ins. As "[v]endor lock-in" is an undefined term, we understand avoiding lock-in to mean that if a customer decides to move, it can do so without unreasonable difficulty. Whereas customers using on-premises IT solutions have been and continue to be largely "locked-in" to costly infrastructure legacy hardware, as well as software that only runs on specific hardware and costly licensing fees, the introduction of cloud computing has greatly increased customers' ability to move to another vendor. CSPs are required to provide customers with controls to retrieve (as well as modify or delete) their assets in accordance with the requirements under the Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 ("Data Act").	The proposed deletions in sub-subsection 2.1.2 should be incorporated as the purported risks are both factually unsubstantiated, introduces requirements that go beyond those introduced by Article 28(4) DORA, and do not reflect how cloud services are provided. The inclusion of these purported risks is unnecessary, fail to achieve the intent of the ECB Guide to be read in conjunction with DORA, and require additional requirements not outlined in Article 28(4) DORA.	Bitkom	Publish

5	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Deletion	In the cloud, financial entities also maintain control over their data, including where it is hosted and processed. This is a feature of the cloud and is committed to by CSPs contractually to customers.	The proposed deletions in sub-subsection 2.1.2 should be incorporated as the purported risks are both factually unsubstantiated, introduces requirements that go beyond those introduced by Article 28(4) DORA, and do not reflect how cloud services are provided. The inclusion of these purported risks is unnecessary, fail to achieve the intent of the ECB Guide to be read in conjunction with DORA, and require additional requirements not outlined in Article 28(4) DORA.	Bitkom	Publish
6	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Deletion	The Guide presupposes that a price increase is a "common scenario" in a "concentrated market", both of which are not applicable to all CSPs. In addition to these issues, proposed sub-subsection 2.1.2 also further deviates from cited Article 28(4) DORA by requiring a financial entity to "ensure" that the CSP has itself "properly implemented the relevant checks." There is nothing within Article 28(4) DORA that requires a CSP to implement "relevant checks". Article 28(4) is explicit that the responsibilities listed are the financial entity's responsibilities. "Relevant checks" is undefined and it is unclear how these checks relate to the "pre-outsourcing analysis". As drafted, the ECB Guide does not reflect or acknowledge DORA and regulatory technical standards made pursuant to DORA that already mandate a series of steps when conducting CSP diligence.	The proposed deletions in sub-subsection 2.1.2 should be incorporated as the purported risks are both factually unsubstantiated, introduces requirements that go beyond those introduced by Article 28(4) DORA, and do not reflect how cloud services are provided. The inclusion of these purported risks is unnecessary, fail to achieve the intent of the ECB Guide to be read in conjunction with DORA, and require additional requirements not outlined in Article 28(4) DORA.	Bitkom	Publish
7	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Deletion	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 AMENDED to read: "IT IS GOOD PRACTICE FOR A PRE-OUTSOURCING ANALYSIS TO TAKE INTO ACCOUNT ALL THE RELEVANT REQUIREMENTS LAID DOWN IN REGULATION (EU) 2022/2554 AND COMMISSION DELEGATED REGULATION SUPPLEMENTING REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL WITH REGARD TO REGULATORY TECHNICAL STANDARDS SPECIFYING THE DETAILED CONTENT OF THE POLICY REGARDING CONTRACTUAL ARRANGEMENTS ON THE USE OF ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS PROVIDED BY ICT THIRD-PARTY SERVICE PROVIDERS."	The proposed deletions in sub-subsection 2.1.2 should be incorporated as the purported risks are both factually unsubstantiated, introduces requirements that go beyond those introduced by Article 28(4) DORA, and do not reflect how cloud services are provided. The inclusion of these purported risks is unnecessary, fail to achieve the intent of the ECB Guide to be read in conjunction with DORA, and require additional requirements not outlined in Article 28(4) DORA.	Bitkom	Publish
8	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy	2.1.3	5	Deletion	In the ECB's view, the provision of Art 28 (2) DORA requires institutions to have a specific cloud strategy that can be integrated into the general outsourcing strategy. The requirement to treat cloud service providers separately and stricter in overall ICT risk management goes far too far and does not result from DORA. DORA does not treat cloud services any differently than other ICT services. A change or deletion is suggested.	It does not follow from Art. 28 (2) DORA that cloud services must be subject to different or particularly strict requirements than other ICT service providers. In particular, such an approach fails to recognize that there may also be other ICT services (e.g. core banking systems) that are only provided by a limited number of service providers and that the dependency and concentration risk may therefore be at least as high as with cloud outsourcing.	Bitkom	Publish
9	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy	2.1.3	5	Amendment	It is important that financial entities have clear strategies for workloads. As drafted, sub-subsection 2.1.3 does not include all relevant elements of cited Article 6(3) DORA. Article 6(3) DORA notes that financial entities "shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools." It's important to amend sub subsection 2.1.3 to include "policies, procedures, ICT protocols, and tools" to provide relevant context, and accurately reflect how CSPs provide services to their customers and ensure the ECB Guide is fully aligned with DORA. In the context of Article 6(3) DORA is important because the financial entity should be using policies, procedures, ICT protocols, and tools" in addition to "strategies" to ensure consistency between an institution's cloud strategy and overall strategy. Accordingly, sub-subsection 2.1.3 should be AMENDED to ADD: "Further, Article 6(3) of DORA requires appropriate strategies, POLICIES, PROCEDURES, ICT PROTOCOLS AND TOOLS."	The proposed amendment to sub-subsection 2.1.3 should be included to include relevant context from Article 6(3) DORA as it more appropriately reflects how cloud services are provisioned and the responsibilities of the financial entities.	Bitkom	Publish
10	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Clarification	It is importance to have robust business continuity plans. Proposed sub-subsection 2.2.1 is likely to cause confusion and increased costs for financial entities rather than aid in developing appropriate mechanisms for cloud services. As drafted, proposed sub-subsection 2.2.1 is unaligned with DORA as it explicitly mandates the introduction of a multi-provider requirement for critical or important systems. The ECB cites Article 12 DORA and goes on to state that "back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned." The wording in Article 12 does not support this. While Article 12(3) states that, when using their own systems, financial entities should ensure backup data is "physically and logically segregated" from source ICT systems [in relation to entities own systems], this does not mandate a multi-provider strategy. Article 6(9) DORA is clear that a multi-vendor strategy is not mandatory, so it does not follow that the ECB would interpret such strategy as being mandatory. This sub-section 2.2.1 clearly exceeds the requirements of DORA. Accordingly, the following amendments to sub-subsection 2.2.1 should be incorporated. The sentence "IN ORDER TO AVOID JEOPARDISING THE SECURITY OF NETWORK AND INFORMATION SYSTEMS, THE ECB CONSIDERS THAT BACK-UPS OF CRITICAL OR IMPORTANT SYSTEMS SHOULD NOT BE STORED IN THE CLOUD WHICH HOSTS THE SERVICES CONCERNED" should be AMENDED to read "IN ORDER TO AVOID JEOPARDISING THE SECURITY OF NETWORK AND INFORMATION SYSTEMS, THE ECB CONSIDERS THAT BEST PRACTICE IS FOR BACK-UPS OF CRITICAL OR IMPORTANT SYSTEMS SHOULD BE PHYSICALLY AND LOGICALLY SEGREGATED."	The proposed amendments to draft sub-subsection 2.2.1 should be incorporated as it will align the text with DORA and avoid new regulatory requirements increasing costs for financial entities and potentially introducing new sources of risk and complexity.	Bitkom	Publish
11	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Clarification	As previously stated, financial entities are entitled to choose their infrastructure. This sub-section contradicts this by mandating a multi-provider requirement for critical or important systems. This requirement is likely to: (i) lessen operational resilience by introducing new sources of risk; and (ii) cause significant confusion and costs for financial entities. A mandatory multi-vendor strategy is likely to add additional attack and risk vectors as financial entities will need to maintain separate environments across multiple CSPs or on-premises. Increasing attack and risk vectors has the opposite intended aim of increasing operational resilience. Requiring that backup systems be stored on another CSP or on-premise would be significantly expensive, especially given the breadth of the definition of critical or important systems under DORA, and especially where a CSP can offer the ability to store data both physically and logically separated. Proposed sub-subsection 2.2.1 also misunderstands Article 12(6) DORA. Article 12(6) mentions "extreme scenarios" but does not contemplate a scenario of lack of cooperation from a CSP. This is an extrapolation of the underlying DORA text. The sub-section "OR AN EXIT WITHOUT COOPERATION FROM THE CSP(S) IN QUESTION" should be DELETED. Should the section not be amended, clarification is needed with regards to the term "not be stored in the cloud which hosts the services concerned" since it could mean a range of including on prem backup, backup to other CSP, backup to same CSP but different location.	The proposed amendments to draft sub-subsection 2.2.1 should be incorporated as it will align the text with DORA and avoid new regulatory requirements increasing costs for financial entities and potentially introducing new sources of risk and complexity.	Bitkom	Publish
12	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Clarification	It is important for financial entities to maintain appropriate cloud resilience measures. While appreciating that these measures are not mandatory, sub-subsection 2.2.2 may cause confusion and increased costs for financial entities as it: (i) deviates from the requirements outlined in Article 6(8) DORA; (ii) may increase costs for 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. The final version of the ECB Guide should provide clarification on these points. One example is "These scenarios should be tested regularly in accordance with the institution's strategy and in line with its business continuity policy and requirements." Please clarify "regularly" (for example by "yearly"). Article 6(8) states "the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives." It is unclear how the proposed architecting requirements the ECB outlines in 2.2.2 accomplish this or are aligned with DORA. As drafted, these requirements are 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.	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 that lack a common definition.	Bitkom	Publish
13	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Clarification	Draft sub-subsection 2.2.2 is likely to cause confusion because it uses terms like "availability zone" and "hybrid cloud architecture", which are undefined within DORA and also defined differently by various CSPs. It is unclear what "two or more distinct substructures" means. Without alignment on these threshold definitions, the ECB Guide will cause confusion for financial entities.	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 that lack a common definition.	Bitkom	Publish
14	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Clarification	An "abrupt discontinuation of a CSP's outsourced cloud services" without recovery in a timeline beyond a financial entity's business continuity plans is not always a plausible scenario for a CSP.	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 that lack a common definition.	Bitkom	Publish

15	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	2.2.3	7	Clarification	Business continuity and disaster recovery in the context of operational resilience is important. However, as presently drafted, it is unclear how proposed sub-subsection 2.2.3 will aid entities in this goal. The current drafting may increase operational costs on financial entities and is not aligned with DORA. Sub-subsection 2.2.3 interprets Article 11(6) DORA, which is lex specialis under NIS 2, and Article 21(2)(c) of NIS 2 to require a financial entity to not rely on disaster recovery certifications and to undertake spot checks at short notice. Neither Article 11(6) DORA nor Article 21(2)(c) of NIS 2, however, mandate this type of testing. Reliance upon disaster recovery certifications or third-party certifications is a scalable and widely acceptable proxy for financial entities as part of comprehensive ICT risk management.	The proposed amendments to sub-subsection 2.2.3 should be incorporated to better achieve the stated aim of enabling financial entities to have comprehensive ICT risk management. The present stated requirements are not present in DORA and NIS 2, may increase costs for financial entities, and could inhibit appropriate ICT risk management by jeopardising the multi-tenant environment. At the very least, the institution should be able to rely on certificates from independent third parties, unless the outsourcing is critical/important.	Bitkom	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	2.2.3	7	Clarification	Additionally, Article 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 valuable for financial entities in testing disaster recovery. Such certifications are carried out independent of CSPs to internationally recognised standards. Compelling financial entities to engage in individual testing would be costly and less effective than relying on third-party certifications, which can enable the testing of multiple scenarios in ways a single firm may not be able to achieve. Permitting a financial entity to undertake a one-to-one test of disaster recovery scenarios could jeopardize the multi-tenant environment unnecessarily when third-party certifications providing appropriate assurance are readily available. Furthermore, the suggestion that financial entities should undertake their own one-to-one disaster recovery tests actually reduces operational resilience. In the cloud environment, financial entities do not have dedicated data centres. Permitting a financial entity to undertake a one-to-one test of disaster recovery scenarios could jeopardize the multi-tenant environment unnecessarily when third-party certifications providing appropriate assurance are readily available. As proposed sub-subsection 2.2.3 is not aligned with DORA and introduces new requirements, 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".	The proposed amendments to sub-subsection 2.2.3 should be incorporated to better achieve the stated aim of enabling financial entities to have comprehensive ICT risk management. The present stated requirements are not present in DORA and NIS 2, may increase costs for financial entities, and could inhibit appropriate ICT risk management by jeopardising the multi-tenant environment. At the very least, the institution should be able to rely on certificates from independent third parties, unless the outsourcing is critical/important.	Bitkom	Publish
17	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	It is unclear how proposed sub-subsection 2.2.4 will assist financial entities with assessment of concentration and provider lock-in risks. As drafted, sub-subsection 2.2.4: (i) presupposes that concentration risk exists in the cloud services market; (ii) misunderstands how financial entities can architect environments to avoid concentration risks; and (iii) differs from DORA in its specific requirements on how to address these risks. As noted in the response to proposed subsection 1.1, it is not agreed that concentration risk exists in the cloud services market. Moreover, proposed sub-subsection 2.2.4 does not recognize how financial entities can architect requirements to avoid concentration risks, and also deviates from DORA.	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
18	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	As discussed in the response to 2.1.2, vendor lock-in is less of a possibility using cloud services than some traditional ICT services. The introduction of cloud computing has enabled customers' ability to switch to other vendors with less cost. With cloud services, customers have full control, ownership, and portability of their data. They can choose one or more services that meet their particular needs, and mix and match those with hardware and software from other providers, including on-premises providers, to create their overall IT solution. Avoiding lock-in does not mean there will not be trade-offs or switching costs, including time, flexibility, functionality and financial costs.	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
19	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	Proposed sub-subsection 2.2.4 is unaligned with DORA. Recital 67 DORA stated that DORA intends to promote a balanced risk on concentration risk and "it is not considered appropriate to set out rules on strict caps and limits to ICT third-party exposures." Additionally, Article 1(h) of the Commission Delegated Regulation does not contain the requirements to assess the three "main aspects" of concentration risks. Proposed sub-subsection 2.2.4 deviates from both of these and does not achieve the aim of helping financial entities assess alleged concentration risks. Rather, this sub-section has the potential to increase complexity and costs for financial entities, while also introducing new sources of risk by defining concentration risk so broadly that it compels financial entities to adopt a multi-vendor strategy.	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
20	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	CSPs often provide substantial information to financial entities in relation to internal architectures, which can include, exit plans. However, the ECB Guide pre-supposes that the financial entities lack this knowledge and that this causes higher concentration risks.	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
21	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	Sub-section 2.2.4 links scalability of cloud and new functions with concentrated risks. CSPs customers are typically looking for providers to meet the objectives of a defined IT need — whether on-premises, in the cloud, or a combination. It is rare that customers are only seeking use of "the cloud". Additionally, customers assess their IT needs on a workload-by-workload basis. Customers, therefore, consider services from multiple IT providers, including on-premises/private cloud solutions, independent software vendors ("ISVs"), and other cloud services providers (both larger and smaller cloud services providers). This means that customers demand and can use multiple IT providers or switch between different IT providers of their choice to ensure that their IT needs are met. The link between scalability of functions and concentrated risk is unsubstantiated.	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
22	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	To address these issues, sub-subsection 2.2.4 should be AMENDED to remove: (i) the sentence: "CONCENTRATION RISKS ARE GENERALLY EXACERBATED BY A LACK OF KNOWLEDGE ABOUT OTHER CSPS' PROPRIETARY TECHNOLOGY, WHICH CREATES DIFFICULTIES AND INCREASES THE COST OF SWITCHING OR EXITING CONTRACTS ("LOCK-IN RISK")"; (ii) the sentence: "WHEN ASSESSING CONCENTRATION RISKS, THREE MAIN ASPECTS MAY BE CONSIDERED: CONCENTRATION IN A SPECIFIC PROVIDER, CONCENTRATION IN A SPECIFIC GEOGRAPHICAL LOCATION AND CONCENTRATION IN A SPECIFIC FUNCTIONALITY/SERVICE (ALSO TAKING INTO ACCOUNT THE FACT THAT OTHER OUTSOURCING PROVIDERS USED BY THE SUPERVISED ENTITY WILL ALSO BE RELIANT ON THE CSP'S CLOUD SERVICES)."."; and (iii) the clause "BUT ALSO BY TAKING INTO ACCOUNT THE SCALABILITY OF THE CLOUD (WHICH ALLOWS IT TO BE GRADUALLY EXTENDED TO ENCOMPASS NEW FUNCTIONS, WITH POTENTIAL EFFECTS ON CONCENTRATION RISKS)."."	The proposed amendments to draft sub-subsection 2.2.4 should be incorporated to better align it with DORA and remove the presumptions regarding concentration risk that are unsubstantiated.	Bitkom	Publish
23	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Clarification	ECB requires that a risk assessment should be done "on a regular basis". Please elaborate on how often the risk assessment should be done in case of non-critical and in case of critical functions outsourced to CSP.	The requirement is unclear yet and needs concretization.	Bitkom	Publish
24	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	2.3.1	9	Amendment	It is unclear how proposed sub-subsection 2.3.1 aids financial entities in developing adequate security measures as it: (i) contains requirements not present in DORA; (ii) links the use of multi-vendor technologies with increased data security, when the effect is often the opposite i.e., increased attack vectors; and (iii) uses undefined terminology that may cause confusion. DORA does not require financial entities to use a multi-vendor strategy. Article 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. This sub-section contradicts financial entities right of choice and sub-subsection 2.3.1 inappropriately links a multi-vendor strategy with increased data resiliency. For customers who have mission-critical, extreme-availability workloads, a multi-region approach is more effective than operating across multiple providers. Customers get the best performance, security and cost when they choose to work primarily with one provider. Customers who use a multi-vendor strategy actually face increased complexity when it comes to operating their applications and infrastructure, including in regards to security. They often have to use solutions from multiple providers to provision, manage, and govern IT resources, to monitor the health of their applications; and to collect and analyse data stored in multiple locations. Rather than enhance data security, a multi-vendor approach actually can compromise data security.	The proposed amendments to sub-subsection 2.3.1 should be incorporated as they better align the text with DORA and will lead to less confusion for financial entities.	Bitkom	Publish
25	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and	2.3.1	9	Amendment	The 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.	The proposed amendments to sub-subsection 2.3.1 should be incorporated as they better align the text with DORA and will lead to less confusion for financial entities.	Bitkom	Publish
26	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and	2.3.1	9	Amendment	Accordingly, sub-subsection 2.3.1 should be AMENDED to READ: "IN ADDITION TO ENCRYPTION TECHNOLOGY, INSTITUTIONS MAY ALSO (I) USE MULTI-CLOUD TECHNOLOGIES, OR (II) ADOPT OTHER DATA LOSS PREVENTION MEASURES."	The proposed amendments to sub-subsection 2.3.1 should be incorporated as they better align the text with DORA and will lead to less confusion for financial entities.	Bitkom	Publish
27	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	2.3.1	9	Clarification	"The security and accuracy of data in transit and data at rest are key requirements when relying on cloud infrastructure" Why is this restricted to cloud infrastructure?	Needed to better understand the motivation of the statement	Bitkom	Publish

28	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	2.3.2	10	Clarification	"… assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP." Is it necessary to also assess CSP owned entities located in another country then the contract with the FE is located?	Needed to avoid to avoid countless interpretations.	Bitkom	Publish
29	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	10	Clarification	As drafted, sub-subsection 2.3.4 states that an institution's IAM policy should be extended to cover cloud assets and executed when entering a cloud outsourcing arrangement. This wording should be clarified, as the present drafting makes it ambiguous whether CSPs have to help financial entities execute their IAM policies. Pursuant to Article 9(4) DORA, it is solely a financial entity responsibility to implement policies that limit the physical or logical access to information assets and ICT assets. To avoid confusion, sub-subsection 2.3.4 should be AMENDED to read: "AN INSTITUTION'S IAM POLICY SHOULD BE EXTENDED TO COVER CLOUD ASSETS"	Should be amended to align the clause with DORA and to avoid confusion.	Bitkom	Publish
30	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.	11	Deletion	As drafted, it is unclear how sub-subsection 2.3.4.1 aligns with DORA or will help financial entities address the identified deficiencies in their operational resilience framework. Specifically, it is unclear how agreeing individual clauses with CSPs will constitute "good practice" when configuring the cloud environment. DORA does not require financial entities to have individual clauses when they use cloud services. It is costly for financial entities to negotiate bespoke terms and engages legal and business resources. Sub-subsection 2.3.4.1 discriminates against those financial entities using cloud services as such a requirement is not present for other ICT services. Cloud services are provided via a one-to-many model. The configuration of the services is entirely in the hands of the customer such that individual clauses relating to configuration are not required and would hamper the customer's ability to use such services, changing configurations as best suits their needs, undermining the value of cloud services. In this respect it's important to distinguish cloud services from traditional ICT services. While DORA does require certain contractual clauses, the negotiation of individual clauses is not required and unnecessary given the control financial entities maintain over their environments in the cloud. DORA already imposes mandatory contractual provisions, as such the ECB's guidance is unnecessary. This additional "good practice" set out by the ECB undermines the legal requirement to have in place mandatory obligations with ICT-service providers pursuant to DORA by suggesting customers agree to bespoke arrangements to comply. Sub-subsection 2.3.4.1 should be DELETED to avoid increasing costs on financial entities when using cloud services and introducing requirements not present in DORA.	Should be deleted as individual clauses are not mandatory per DORA and mandating individual clauses will not increase financial entity resiliency.	Bitkom	Publish
31	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.2	11	Clarification	"Users – especially those with privileged access to the system …" Users on the FE - and/or Users of the CSP? Please clarify.	Needed to understand who exactly is meant by "users"	Bitkom	Publish
32	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4	12	Clarification	"Significant risks and challenges can arise if an institution decides to terminate a contractual agreement with a CSP without having previously established a comprehensive exit plan on the basis of a principle-based exit strategy." Please specify the term "principle-based exit strategy"		Bitkom	Publish
33	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1.	12	Amendment	As presently drafted, proposed sub-subsection 2.4.1 is likely to cause confusion and increased costs for financial entities. Proposed sub-subsection 2.4.1 includes new termination, exit planning, and subcontractor requirements that are not present in DORA and associated regulations. DORA contains specific requirements for how ICT services may be terminated within Article 28(7). Proposed sub-subsection 2.4.1 introduces new termination rights not contemplated by Article 28(7) DORA. The list of "[o]ther changes that could lead to such a reason for termination" are not present in Article 28(7) DORA. Article 28(7) DORA includes a list of mandatory requirements, none of which include those mentioned in this paragraph. This additional list is also unnecessary as these scenarios can be covered by standard termination for convenience sections that enable financial entities to terminate their agreements with CSPs. Paragraph 3 "THE CONTRACT BETWEEN THE INSTITUTION AND THE CSP SHOULD OBLIGE THE CSP TO SUPPORT A SMOOTH AND EFFECTIVE TRANSITION IN ACCORDANCE WITH THE SCHEDULE IN THE AGREED EXIT PLAN" should be amended to read "THE CONTRACT BETWEEN THE INSTTUTION AND THE CSP SHOULD INCLUDE THE REQUIREMENTS REQUIRED BY ARTICLE 30(3)(F) OF DORA."	The proposed amendment to draft sub-subsection 2.4.1 should be incorporated to align the text with the cited DORA articles.	Bitkom	Publish
34	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1.	12	Amendment	The proposed sub-subsection 2.4.1 obligates CSPs to support a financial entity's exit plan. This obligation is not present in Article 30(3)(f) DORA, which only includes reference to "exit strategies" and not a specific "exit plan". It may be not be operationally possible for a CSP to support all aspects of a financial entity's exit plan, particularly where a financial entity requires expertise that the CSP may not have available. Personnel from one CSP, for example, would not be best positioned to re-configure a financial entity's data to transition to another CSP. Further, contractual requirements regarding a CSPs obligation to support financial entities exit strategy is also prescribed under Article 25(2)(b) of the Data Act and additional requirements risk further uncertainty for providers and users of cloud services.	The proposed amendment to draft sub-subsection 2.4.1 should be incorporated to align the text with the cited DORA articles.	Bitkom	Publish
35	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1.	12	Amendment	Proposed sub-subsection 2.4.1 obligates CSPs to support a financial entity's exit plan. This obligation is not present in Article 30(3)(f) DORA, which only includes reference to "exit strategies" and not a specific "exit plan". It may be not be operationally possible for a CSP to support all aspects of a financial entity's exit plan, particularly where a financial entity requires expertise that the CSP may not have available. Personnel from one CSP, for example, would not be best positioned to re-configure a financial entity's data to transition to another CSP. As these requirements are not present in Article 28(7) DORA and are unnecessary, proposed sub-subsection 2.4.1 should be AMENDED to DELETE the list in paragraph 2 after "OTHER CHANGES." Paragraph 5 "ON THE BASIS OF THE REQUIREMENT CONCERNING KEY CONTRACTUAL PROVISIONS CONTAINED IN ARTICLE 30(2)(A) OF DORA, INSTITUTIONS SHOULD ENSURE THAT ALL SUPPLIERS OF SUBCONTRACTED SERVICES SUPPORTING THE CSP COMPLY WITH 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" should be DELETED as it contains requirements that are not present in DORA. If a reference is deemed required, the Guide should point to the requirements in the forthcoming RTS made pursuant to Article 30(5) which will detail the elements financial entities need to determine and assess when subcontracting ICT services supporting critical or important functions. Aligning this with DORA will lessen potential confusion for financial entities as they attempt to comply.	The proposed amendment to draft sub-subsection 2.4.1 should be incorporated to align the text with the cited DORA articles.	Bitkom	Publish
36	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	14	Amendment	"As a result of the particular way in which cloud services are set up, the CSP has the technical ability to terminate any service/access for any customer at any point in time in such a way that the service cannot be resumed by another party. Regardless of any contractual agreement, such a termination could be caused by external events such as conflicting legislation. In the exit strategies that are required under Article 28(8) of DORA, institutions should include a business continuity policy catering for such a situation in order to ensure that the institution is able to withstand that scenario and has access to the data required to operate the service in question." In practice, business continuity in such a case is almost impossible to achieve (without performing constant on-prem data backups which would be highly cost-intensive).		Bitkom	Publish
37	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	15	Amendment	As drafted, it is unclear how proposed section 2.5's concerns are related to DORA or reflective of how CSPs provide services and information to customers. While DORA emphasizes that the ability to monitor ICT providers is important, the claim that CSPs do not provide sufficient detail about their processes and controls is unfounded. It is also unclear why proposed Article 2.5 seems to indicate the reliance upon these statements and third-party certifications is insufficient. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. These are not "homegrown" documents and ensure the security and, as a result, the resilience of CSPs is maintained. Article 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 a useful tool for financial entities looking to understand a CSPs infrastructure processes and internal control systems. Accordingly, proposed section 2.5 should be AMENDED to DELETE all the text: "IN MANY CASES, CSPS DO NOT PROVIDE SUFFICIENT DETAIL ABOUT THEIR INFRASTRUCTURE PROCESSES AND THEIR INTERNAL CONTROL SYSTEMS, WITH THE RESULT THAT INSTITUTIONS OFTEN LACK DETAILED FIRST-HAND KNOWLEDGE OF THE CSP'S PREMISES, INFORMATION SYSTEMS, PROPRIETARY TECHNOLOGY, SUB-PROVIDERS AND CONTINGENCY PLANS, AS THE MAJORITY OF ENTITIES RELY SOLELY ON THE CSP'S STATEMENTS AND THIRD-PARTY CERTIFICATIONS."	Proposed section 2.5 should be amended as the statements within are unaligned with DORA and not reflective of how CSPs provide services and information to customers.	Bitkom	Publish
38	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1	15	Amendment	As presently drafted, it is unclear how proposed sub-subsection 2.5.1 is aligned with Article 6(10) DORA. While Article 6(10) DORA notes that financial entities may "outsource the asks of verifying compliance with ICT risk management requirements", proposed sub-subsection 2.5.1 contradicts this and states that this is insufficient. This will cause confusion for financial entities as they undertake DORA implementation.	The proposed amendment to sub-subsection 2.5.1 should be incorporated as the present drafting is factually unsubstantiated, reflects a lack of understanding of how cloud services are provided, and introduces additional concerns not present in cited Article 6(10).	Bitkom	Publish

39	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1	15	Amendment	Proposed sub-subsection 2.5.1 also suggests that a CSP is capable of manipulating independent monitoring tools without factual substantiation for that claim. Financial entities should be able to monitor the cloud environment and equips its customers with information and tools to do so. As proposed sub-subsection 2.5.1 includes a requirement not present in DORA and unsubstantiated allegations regarding manipulation of monitoring tools, it should be AMENDED to: "In such a scenario, the monitoring tools provided COULD be complemented by independent tools."	The proposed amendment to sub-subsection 2.5.1 should be incorporated as the present drafting is factually unsubstantiated, reflects a lack of understanding of how cloud services are provided, and introduces additional concerns not present in cited Article 6(10).	Bitkom	Publish
40	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.3	16	Amendment	It is importance to memorialise rights and obligations in a cloud services model. However, it is unclear how proposed sub-subsection 2.5.3 will help clearly allocate responsibilities between CSPs and financial entities in addition to those contractual provisions already required pursuant to DORA and EBA Guidelines. Proposed sub-subsection 2.5.3 could cause confusion as it: (i) requires the use of standard contractual clauses when outsourcing cloud computing services; and (ii) presupposes that a CSP could "unilaterally" change agreements.Proposed sub-subsection 2.5.3 states that a provider should sign a "separate digital or physical copy to prevent any risk of unilateral changes." This proposal: (i) reflects a lack of understanding of how CSPs provide agreements to customers on a one-to-many model; (ii) is factually unsubstantiated; (iii) likely to cause increased costs and complexity for financial entities; and (iv) is not required by DORA. In a one-to-many model with cloud services, the services operate the same way for every customer. There are no specialised services for financial entity customers. Changes and improvements to services occur frequently for all customers and service level agreements for these services need to remain uniform for all customers to benefit from changes. Operationally, it is not possible for cloud providers to change the services for a set of customers but wait to implement those changes based on static agreements signed with others. Instead, financial entities can use tools to be made aware of changes to these agreements through RSS feeds cloud providers maintain or third-party website change notification services as these agreements are public. Mandating specific requirements for financial entities would leave them unable to benefit from changes to services and would not deliver on the regulatory objectives set out in the Guide. The ECB Guide may have the unintended consequence that third-party providers are forced to create an industry or country-specific cloud, which would reduce the potential efficiency gains, scalability, and associated innovation that comes with increased use of cloud services, adding complexity and creating new security risks. As read, it appears that this sub-subsection 2.5.3 indicates CSPs could make unilateral changes fraudulently or without agreed notification. As noted above, this is unsubstantiated and not reflective of how changes are made or notice is provided. 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.	The amendments to proposed sub-subsection 2.5.3 should be incorporated to better align the provision with the DORA text, reduce the possibility for increased confusion and costs for financial entities, and remove unsubstantiated assertions that CSPs can commit fraud.	Bitkom	Publish
41	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.3	16	Amendment	As drafted, proposed sub-subsection 2.5.3 could also lead to unnecessary increased costs for financial entities as they would need to sign digital or physical copies for customer agreements, furnished online on a one-to-many model. This requirement discriminates against those financial entities with cloud workloads, as those using other digital ICT services. Financial entity customers, for instance, are not required to maintain physical or digital copies of every time their workforce consents to a "unilateral" phone software update. This requirement is not present in Article 30 DORA. While Article 30 mentions that this document should be a in a durable and accessible format, it has nothing about whether this must be "signed". To align Proposed sub-subsection 2.5.3 with DORA, it should be AMENDED to read: "Taking this into account, the ECB recommends that financial entities SHALL CONSIDER THE use OF standard contractual clauses when outsourcing cloud computing services."	The amendments to proposed sub-subsection 2.5.3 should be incorporated to better align the provision with the DORA text, reduce the possibility for increased confusion and costs for financial entities, and remove unsubstantiated assertions that CSPs can commit fraud.	Bitkom	Publish
42	Box 2: Contractual clauses	2.5.3	16	Amendment	ECB recommends that financial entities use standard contractual clausel (SCC) when outsourcing cloud computing services. It would be very helpful to understand which SCC are meant exactly here, esp. as no such SCC are published yet. Examples specifically for the financial industry would be also heplful.	This requirement is virtually impossible to implement in practice because the CSPs (even at large institutions) generally specify the contracts and not the institution. In practice, the institutions' negotiating power is extremely limited.	Bitkom	Publish