EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

Amazon Web Services

Contact person

Mr/Ms

First name

Surname

Email address

Telephone number

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

General comments

Amazon Web Services ("AWS") is grateful for the opportunity to respond to the European Central Bank's ("ECB") Guide on outsourcing cloud services to cloud service providers ("ECB Guide").

AWS's response provides our views and interpretation from the perspective of a Cloud Service Provider ("CSP"). As a CSP, AWS appreciates the consultation opportunity and supports the intention of the ECB Guide to enable financial institutions to improve their operational resiliency, particularly in alignment with Regulation (EU) 2022/2554 ("DORA").

AWS's proposals to the ECB Guide primarily focus on three key areas: (i) aligning the ECB Guide with DORA to reduce the risk of confusion and costs for financial entities; (ii) clarifications about how cloud services work and the multi-tenant environment; and (iii) ensuring that financial entities remain competitive and able to choose services that work best for their customers and goals ("Submissions").

AWS's Submissions reflect its ongoing commitment to engaging in regulatory discussions in support of introduction and interpretation of consistent and fair regulatory frameworks for the use of cloud services by the financial services sector.

AWS would appreciate any opportunity to further discuss the comments included our submissions with the ECB.

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 is intended to be read in conjunction with Regulation (EU) 2022/2554 ("DORA"), and should be aligned with DORA's requirements. DORA provides the regulatory framework, processes and standards for financial entities using ICT third-party service providers, including cloud service providers ("CSPs"). Introducing new requirements in the ECB Guide that extend beyond DORA undermines the consistent standards and guidelines, creating ambiguity for financial entities. As drafted, the ECB Guide focuses solely on cloud services, which is unaligned with the scope of DORA, and asserts without substantiation that cloud service usage is highly concentrated and inherently riskier than other ICT solutions. DORA and the other regulations cited in the ECB Guide are intended to be technology agnostic and focused on risks. The definitions used in the ECB Guide are unaligned with those in DORA, creating confusion for financial entities. 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 an "understanding of those specific rules", it should focus on all ICT services. Such an approach is consistent with that of the European Banking Authority via the 'EBA Guidelines on outsourcing arrangements' and DORA itself. With statements like "the use of cloud services also increases institutions' exposure to several risks", the ECB Guide presupposes that using CSPs increases a financial entity's risk, without substantiation. In response to the ECB's statements in relation to concentration risks, choosing a single service provider is not indicative of concentration risk and can reduce complexity, reduce attack vectors, and maximise training gains for such concentrated solutions. Cloud services are neither concentrated from a sector perspective nor a geographic or service perspective. There is substantial evidence that the cloud services sector is not concentrated. The vast majority of customers use multiple IT providers. Since 2006, many providers around the world have begun offering IT services on-demand over a network. Google Cloud (launched in 2008), Microsoft Azure (2010), Rackspace (2010), Dell (2011), IBM (2011), OVHcloud (2011), DigitalOcean (2012), Hewlett Packard Enterprise (2012), Oracle (2016), Cloudflare (2018), Flexential (2019), and others have entered and continue to expand. From 2016 to 2021, Gartner reports that Microsoft Azure and Google Cloud each grew their cloud infrastructure sales significantly. DigitalOcean has grown by more than 30% each fiscal year since going public. Oracle declared in July 2022 that its cloud business was entering a "hypergrowth phase," and its infrastructure sales subsequently grew more than 50% year over-year. IBM attained double-digit growth in hybrid cloud revenue in 2022. Databricks became one of the ten most valuable start-ups worldwide within eight years of its launch. Snowflake reported 70% year-over-year product revenue growth in fiscal year 2023. AWS also vigorously competes with on-premises IT components, which capture the large majority of IT spend. According to Gartner forecast, for 2023, that less than 15% of IT spending would be on the cloud. This is competition at its best: even setting aside the many non-cloud competitors, the industry is competitive. If the purported concentration risk pertains to concentration of services or geographic concentration risk, both can be mitigated through financial entities appropriately architecting their environments. From a service perspective, Directive (EU) 2020/1828 ("Data Act") already contains requirements regarding a customer's ability to switch workloads between service providers. Service providers are incentivized to support interoperability. If a service provider cannot reasonably interoperate with these third-party solutions, customers will either stay with their current provider or choose an alternative that supports interoperability. AWS provides services and features that aid customers migrating workloads both to and from AWS, including AWS Application Migration Service and AWS Database Migration Service. The locational diversity of AWS's infrastructure can greatly reduce geographic concentration risk. To avoid single points of failure, AWS minimizes interconnectedness within our global infrastructure, reducing geographic concentration risk, by doing the following: (i) regions are designed to be independent and are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions; (ii) Availability Zones within each Region are physically separated and independent from each other, built with highly redundant networking to withstand disruptions; and (iii) compared to global financial institutions' on-premises environments, the locational diversity of AWS's infrastructure greatly reduces geographic concentration risk. The likelihood of AWS failing – either via bankruptcy or other incident – such that it would not be able to provision services is incredibly remote. If the concentration risk relates to continuity of services in event of a disruption, AWS maintains a formal risk management program designed to support the continuity of critical business functions. Additionally, the use of on-premises infrastructure can be inherently riskier than cloud services. Cloud services can provide solutions for some problems faced by companies with on-premises infrastructure, including in addressing security risks at scale. While customers need to appropriately architect their frameworks, increased resilience is a feature of the cloud. The CSP's one-to-many model enables more centralized security and more investment in security policing than a company could provision itself. Proposed section 1.1. should be **AMENDED** to **DELETE** the last two sentences in the first bulleted paragraph beginning with: **"WHILE THE USE OF CLOUD SERVICES CAN ..."** The ECB Guide's definitions are unaligned with Article 3 of DORA, including the definitions of **"critical or important function"** and **"ICT asset."** These competing definitions will cause confusion and difficulties for entities attempting to comply. **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: (x) differing from DORA; and (y) 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.	AWS	Publish
2	1. Introduction 1.2 Scope and Effect	1.2	3	Amendment	As drafted, proposed subsection 1.2 is 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", 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' at 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 the response to section 1.1, DORA and other regulations cited are intended to be technology agnostic and focused on risks. The ECB's singular focus in this sub-section, is contrary to this agnostic approach. 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.	AWS	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	Amendment	AWS agrees that financial entities should establish appropriate governance frameworks aligned with DORA requirements. It is unclear, however, that proposed sub-section 2.1.1 will help financial entities achieve the requirements under DORA. As presently drafted, proposed sub-section section 2.1.1: (i) misinterprets the clear roles and responsibilities for CSPs and customers in the provision of cloud services; and (ii) does not acknowledge regulatory requirements set out in both Article 28(1) DORA and the related *Commission Delegated Regulation supplementing Regulation (EU) 2022/2554 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 "Commission Delegated Regulation"). We disagree that cloud services make a "clear and unambiguous allocation of responsibilities more challenging." The CSP operates, manages and controls the components of the host operating system (e.g., the physical security of the facilities in which the services operate). The customer assumes responsibility for and management of the guest operating environment (including backup creation for parallel structure, identity and access management, updates, encryption, etc.) and other associated application software as well as the configuration of the CSP-provided security group firewall, as explained in AWS's shared responsibility model (https://aws.amazon.com/compliance/shared-responsibility-model/). Proposed sub-subsection 2.1.1 should be **AMENDED** to **DELETE** the words **"MAKING A CLEAR AND UNAMBIGUOUS ALLOCATION OF RESPONSIBILITIES MORE CHALLENGING"** as this is not reflective of how CSPs provide services to customers. It is also not clear what point of comparison is being used when suggesting allocating responsibilities is more challenging. As drafted, proposed sub-subsection 2.1.1 cites Article 28(1) DORA in support of the following interpretations: (i) institutions should apply the same level of diligence regarding risk management as those who keep services in-house or on-premises; and (ii) that financial entities should ensure that their CSPs have "equivalent risk management" practices, processes and controls. The present drafting will cause confusion as Article 28(1) DORA mandates neither of these. Article 28 DORA does not distinguish between CSPs and on-premises infrastructure and instead refers to managing ICT third-party risk generally. Furthermore, the requirement that institutions should ensure CSPs have "equivalent risk management practices" substantially deviates from Commission Delegated Regulation Article 9(1). Commission Delegated Regulation Article 9(1) states institutions need to ensure ICT third-party service providers are used in compliance with a financial entity's "relevant policies and procedures". This is an important distinction. It is not that a CSP must have the same risk management practices as its customers, which will differ from customer to customer. It is the case that customers must ensure they may use CSP services in compliance with their own practices. The ECB's statement is not workable in practice and does not account for the "one-to-many" nature of CSPs. It is impossible for a CSP to ensure equivalent compliance with each individual financial entities' risk management practices, processes and controls, which will differ from customer to customer and be impacted by those customers practical needs and risk tolerances. We note that, as at the time of this consultation a separate consultation is in progress regarding the NIS 2 Directive Implementing Regulation which includes express risk management requirements for 'cloud computing service providers', further confusing this issue. Given the stages of these consultations, it is unclear how (if at all) the ECB will take these requirements into account. Additionally, the ECB Guide states that the same supervisory expectations apply when a non-CSP service provider relies on a CSP. This statement would require that even in the event that a CSP has no relationship with a financial entity, it has to follow the procedures of every single end financial entity customer of its direct customers. Using "relevant policies and procedures" as present in the Commission Delegated Regulation Article 9(1) appropriately apportions the burden between CSP and financial entity. To align proposed sub-subsection 2.1.1 with DORA, it should **AMENDED** as follows: The sentence beginning paragraph 3 ,"**THE ECB UNDERSTANDS ARTICLE 28(1)(A) OF DORA AS MEANING THAT INSTITUTIONS WHICH OUTSOURCE ICT SHOULD APPLY THE SAME LEVEL OF DILIGENCE REGARDING RISK MANAGEMENT, PROCESSES, AND CONTROLS (INCLUDING ICT SECURITY) AS THOSE WHICH DECIDE TO KEEP THE RELEVANT SERVICES IN-HOUSE)" should be DELETED or, at least, AMENDED to read: "THE ECB UNDERSTANDS ARTICLE 28(1)(A) OF DORA AS MEANING THAT INSTITUTIONS WHO USE ICT SERVICES MUST ENSURE THAT THE USE OF SUCH SERVICES DOES NOT PREVENT THEM FROM REMAINING COMPLIANT WITH DORA AND OTHER APPLICABLE FINANCIAL SERVICES LAWS.**". In the same paragraph 3, the word "**EQUIVALENT**" should be **DELETED** AND **REPLACED** with the word "**RELEVANT**"	Sub-subsection 2.1.1. should be amended to acknowledge: (i) the responsibilities between CSPs and customers in cloud services; and (ii) the obligations under Article 28(1) DORA and the Commission Delegated Regulation Article 9(1). As presently drafted, sub-subsection 2.1.1 is unaligned with DORA and presents an interpretation that mandates additional requirements not present in the text and subsequent Commission Delegated Regulation. Incorporating the proposed amendments would avoid the appearance of imposing new and more stringent requirements upon customers in contravention of the ECB Guide's stated purpose.	AWS	Publish
4	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Deletion	AWS understands the importance of institutions undertaking 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 our response to section 1.1, financial entities are entitled to their choice of infrastructure and to evaluate risks, including those related to vendor lock-in. As "[v]endor lock-in" is an undefined term, we understand avoiding vendor 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. AWS provides its 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 the Data Act. The Data Act, in particular, has requirements that customers must have contractual terms regarding switching between service providers. As noted in our response to Sub-section 1.1, AWS provides many services and features that can aid customers migrating workloads both to and from AWS, including services such that customers will not even need AWS' assistance to retrieve their assets, nor even to migrate off of AWS. AWS has developed its services in this manner so that customers can retain control over and flexibility in their use of the services and their assets. The presumption that financial entities are "locked-in" when using cloud services is factually unsubstantiated and contradicted by existing EU regulation. 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. Additionally, the Guide presupposes that a price increase is a "common scenario" in a "concentrated market", both of which are not applicable to AWS or to all CSPs. As stated in our detailed comments to section 1.1 and above, financial entities are entitled to a choice in risk appetite, and in AWS's view concentration risks for CSPs do not exist either in respect to market, geographic, or service concentration risks. Additionally, the benefits of cloud computing include reduced costs. As of September 2023, AWS has reduced prices over 120 times since AWS was first launched in 2006. Additionally, IT providers, including new CSPs, often tout their pricing in direct comparison to other CSPs, which encourages further price competition. Furthermore, CSPs also compete with each other and with on-premises providers by offering free tiers, which allow free usage up to a certain threshold for many services. AWS first offered a free tier in 2010, making it easier for companies using on-premises services to experiment with cloud services. The AWS free tier has expanded since, and today provides free usage allotments for more than 100 AWS services. Microsoft Azure, Google Cloud, and Oracle each offer their own free tier as well. None of this indicates that "significant increase in price" is a "common scenario". As discussed above in relation to comments for subsection 1.1, the cloud services market is not concentrated. Since 2006, many providers globally have begun offering IT services on-demand over a network. 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. 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..."** should also be **AMENDED** to: **"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 are 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.	AWS	Publish

5	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	AWS understands the importance of financial entities having 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." In our view, 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. AWS operates under a shared responsibility model where financial entities manage certain security and resiliency components. Including relevant 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.	AWS	Publish
6	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	Amendment	AWS agrees with the importance of 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. For AWS each "Region" consists of multiple independent and physically separate Availability Zones within a geographic area. Strict logical separation between the software services in each Region is maintained. This ensures that an infrastructure or services failure in one Region will not result in a correlated failure in another Region. This kind of structure can provide an unprecedented ability for financial entities to back up critical data in multiple locations in efficient ways, which can mitigate a variety of risks, including geopolitical risks. 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. As previously stated, financial entities are entitled to choose their infrastructure. Sub-section 2.2.1 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. 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 sub-section **"OR AN EXIT WITHOUT COOPERATION FROM THE CSP(S) IN QUESTION"** should be **DELETED**.	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.	AWS	Publish
7	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Clarification	AWS understands the importance of financial entities maintaining 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. For example, the term region is used. As outlined above in sub-section 2.2.1, AWS Regions are separate geographic areas. AWS Regions consist of multiple, physically separated and isolated Availability Zones that are connected with low latency, high throughput, highly redundant networking. This term is not used uniformly by CSPs. The final version of the ECB Guide should provide clarification on these points. 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. Additionally, 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. Finally, it should also be noted that 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 a plausible scenario for AWS. AWS builds to guard against outages and incidents so when disruptions do occur, their impact on the continuity of services is as minimal as possible. AWS has multiple constructs that provide different levels of independent, redundant components.	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.	AWS	Publish

8	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	Amendment	AWS appreciates the importance of business continuity and disaster recovery in the context of operational resilience. As presently drafted, however, 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. For AWS, for example, the disaster recovery tests are a technical program where failure scenarios are simulated on a centre's critical infrastructure, which includes electrical, mechanical, controls and ancillary systems inclusive of life safety. It is also possible to conduct failure simulations, as well as simulate power failure of an availability zone. Given the one-to-many model, AWS is able to test a plethora of situations that would be difficult or expensive for a financial entity to test on its own. AWS operates thousands of controls that meet the highest standards of operational resilience in the industry. To understand these controls and how we operate them, financial entities can access widely recognised security standards and compliance certifications issued by third parties. For example, our System and Organization Control (SOC) 2 Type II report, reflecting examination by our independent third-party auditor, provides an overview of the AWS Resiliency Program. In addition, AWS aligns with the ISO 27001, the ISO 27017 guidance on information security in the cloud and ISO 27018 code of practice on protection of personal data in the cloud and other standards. 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. For AWS, such certifications are carried out independent of AWS and other 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. For example, for AWS this could lead to requests for AWS to shut down data centres or Availability Zones to test individual financial entities' disaster recovery plans. 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.	AWS	Publish
9	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 risks relating to a single point of failure; 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, AWS disagrees 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. 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. 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. As outlined above at sub-section 2.2.3 and evidenced throughout its responses to the ECB Guide, as a CSP, AWS provides substantial information to financial entities in relation to AWS architecture. Additionally, AWS engages directly with financial entities and their use of the services, including, in some cases, and upon request of the customer with their exit plans. However, the ECB Guide pre-supposes that the financial entities lack this knowledge and that this causes higher concentration risks. Sub-section 2.2.4 links scalability of cloud and new functions with concentrated risks. From AWS's perspective, 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. 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.	AWS	Publish
10	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, it is our view that 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. Finally, 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. 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.	AWS	Publish

11	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	Amendment	It is unclear how proposed sub-subsection 2.3.2 helps financial entities address the risks stemming from the location and processing of data. Proposed sub-subsection 2.3.2 may cause confusion and be overly burdensome to financial entities using cloud services as it: (i) includes requirements not present in DORA; (ii) is unclear what type of "data" is subject to its limitations; and (iii) appears to link data resiliency and data processing in an inappropriate manner. Sub-subsection 2.3.2 deviates from DORA at the outset because DORA does not require financial institutions to draw up a list of acceptable countries for data processing. Draft sub-subsection 2.3.2 does not clarify what type of data can only be stored and processed in "acceptable countries". Not all data is subject to data protection laws or is highly sensitive. The General Data Protection Regulation ("GDPR") for instance, only applies to personal data rather than all data. Draft sub-subsection 2.3.2 states that supervised entities should base their "acceptable countries" on a list of non-EU countries based on GDPR. It is unclear how countries that are considered adequate for data protection relate to data resiliency, including addressing the legal and political risks of outsourcing. To avoid confusion, sub-subsection 2.3.2 should be **AMENDED** to **DELETE** footnote 10 **"THE EUROPEAN COMMISSION HAS DRAWN UP A LIST OF NON-EU COUNTRIES WHERE DATA PROTECTION IS CONSIDERED ADEQUATE ON THE BASIS OF ARTICLE 45 OF THE GENERAL DATA PROTECTION REGULATION (GDPR). THE ECB ADVISES SUPERVISED ENTITIES TO USE THAT LIST."**	The proposed amendments to sub-subsection 2.3.2 should be incorporated to align with DORA and the EBA Guidelines, clarify expectations for financial entities, and remove the reference to GDPR countries as it does not achieve the aim of assisting countries with addressing the risks stemming from the location and processing of data.	AWS	Publish
12	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	Amendment	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**."	Sub-subsection 2.3.4 should be amended to align the clause with DORA and to avoid confusion.	AWS	Publish
13	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. With AWS, 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. AWS helps make this possible by not requiring up-front payments or long-term contracts. AWS also provides tools and the ability to financial entities to configure applications and services as preferred and to enable them to comply with relevant law. Based on the way cloud services are provisioned, individual clauses are unnecessary. Customers benefit from increased flexibility in choosing which services to use and when to use them, all of which can be accomplished on AWS. 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.	Sub-subsection 2.3.4.1 should be deleted as individual clauses are not mandatory per DORA and mandating individual clauses will not increase financial entity resiliency.	AWS	Publish
14	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. Additionally, 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. Proposed sub-subsection 2.4.1 also requires financial entities to maintain that "all suppliers of subcontracted services supporting the CSP" should have the "same contractual obligations that apply between the institution and the CSP." It does not distinguish between the importance of the subcontractor and is not required by DORA. It also does not reflect the reality that such provisions are unnecessary except for material subcontractors. 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 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 INSTITUTION AND THE CSP SHOULD INCLUDE THE REQUIREMENTS REQUIRED BY ARTICLE 30(3)(F) OF DORA**." 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.	AWS	Publish

15	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. AWS strives to provide information to all customers regarding infrastructure processes and internal control systems. AWS, for example, publicly discloses information about its Global Infrastructure (https://aws.amazon.com/about-aws/global-infrastructure/), as well as specific examples, for example how Amazon Simple Storage Service's (commonly called S3) API works: (https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html) and provides detailed information regarding various controls and third-party certifications. Financial institutions also get access to AWS' third party certifications proving their compliance with international security standards. AWS operates thousands of controls that meet the highest standards of operational resilience in the industry. To understand these controls and how we operate them, financial entities can access security standards and compliance certifications issued by third parties. For example, our System and Organization Control (SOC) 2 Type II report, reflecting examination by our independent third-party auditor, provides an overview of the AWS Resiliency Program. In addition, AWS aligns with the ISO 27001, the ISO 27017 guidance on information security in the cloud and ISO 27018 code of practice on protection of personal data in the cloud and other standards. 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.	AWS	Publish
16	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. Proposed sub-subsection 2.5.1 also suggests that a CSP is capable of manipulating independent monitoring tools without factual substantiation for that claim. AWS agrees that financial entities should be able to monitor the cloud environment and equips its customers with information and tools to do so. AWS shares important information with its customers. For instance, AWS has developed the AWS Health Dashboard, a public-facing website, to provide up-to-the-minute information on the overall availability of all its services across all AWS regions. AWS has also developed tools and resources which customers can leverage to enable them to stay informed of availability and security events that can affect their individual accounts and their use of the services, e.g., AWS Health and Amazon GuardDuty. Through customers' use of such incident management and response tools, customers customize what service event information they receive as relevant to their use of the services and their security configurations. As the information and the services that are provided to financial entities are provided on a one-to-many model, it is not feasible for AWS to "manipulate" these tools. First, different customers will have different needs and responses to the public information provided. It does not follow that AWS would manipulate these tools in favour of one customer or another. Second, AWS provides services, like CloudTrail, which would make it known if AWS somehow "manipulated" monitoring tools in a financial entity's environment. 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).	AWS	Publish
17	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.3	16	Amendment	AWS understands and agrees with the importance of memorialising rights and obligations in a cloud services model. 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 ESA 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 requires the use of standard contractual clauses when outsourcing cloud computing services. This requirement appears to contradict proposed sub-subsection 2.3.4.1 of the ECB Guide, which requires "individual clauses" with a cloud services provider be negotiated. Article 30(4) DORA also recognises that different standard contractual clauses may not be relevant for all ICT services and recommends financial entities consider their use, not mandate that use. Finally, 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. 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." 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.	AWS	Publish