EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Feedback statement on responses to the public consultation on the ECB draft Guide on outsourcing cloud services to cloud service providers

1 Introduction and summary of industry responses

1.1 Context

The European Central Bank (ECB) is publishing its Guide on outsourcing cloud services to cloud service providers as a further step in its supervisory strategy of setting out its supervisory expectations and promoting good practices on the outsourcing of cloud services.

The Guide sets out to specify supervisory expectations in this field, taking into account the Digital Operational and Resilience Act (DORA)[1] and the Capital Requirements Directive[2] for effective governance of risk stemming from outsourcing, while also looking to build robust frameworks for IT security and cyber resilience.

More precisely, the Guide describes a set of good practices that supervised entities can use as a basis for tackling cloud outsourcing risk. The aim is to help banks become more capable in this regard by building on good practices observed within the industry.

On 3 June 2024 the ECB launched a public consultation on the draft Guide, inviting feedback on the proposed guidelines. The following topics were addressed: (1) scope and enforceability of the Guide; (2) governance of cloud services; (3) availability and resilience of cloud services; (3) information and communications technology (ICT) and data security, confidentiality and integrity; (4) the exit strategy from cloud service providers (CSPs); and (5) oversight, monitoring and internal auditing of cloud services.

The public consultation lasted six weeks and ended on 15 July 2024. During that period interested parties had the opportunity to submit their comments. The ECB also informed the European Parliament of the public consultation.

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

2 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

1.2 Overview of the responses

The ECB received a total of 696 written comments from financial institutions and associations, both private and public, along with other stakeholders. The comments addressed all chapters and sections of the draft Guide.

Notably, various commenters requested further clarifications, including on the terminology used in the draft Guide, its scope and legal status, resilience measures related to the use of cloud services, the risk management framework for cloud services, and the exit strategy vis-à-vis CSPs.

Amendments to the draft Guide have been made, where appropriate, following careful consideration and expert assessment of the comments received.

1.3 Structure of this feedback statement

This feedback statement presents the ECB's assessment of the comments received during the public consultation and aims to provide answers to all matters raised by the industry. With a view to greater clarity and ease of use, and to help ensure the transparency of the public consultation process, this document also provides the names of the respondents when setting out the respective comments, enquiries and proposed amendments.

2 Responses to the public consultation on the draft ECB Guide on outsourcing cloud services to cloud service providers and ECB feedback

Comments on the draft Guide are addressed by chapter and section, following the structure and order of the document.

2.1 Table 1 – Comments on Chapter 1: Introduction

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
8	Relationship between the Guide and DORA and concentration risks	AWS 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	The ECB believes that the reasons for issuing an ECB guide specifically addressing cloud outsourcing are sufficiently substantiated in Section 1.1 of the Guide. This does not diminish or compromise the applicability of DORA to all ICT third-party providers (TPPs). The ECB provides in the Guide its understanding of the relevant DORA provisions and recommends good practices, so the Guide does not introduce new requirements beyond Union law and its implementing regulations. The Guide expresses a technology-agnostic view. Apart from highlighting risks that are particularly important in cloud environments, it also acknowledges the benefits of cloud technologies. When analysing the outsourcing registers of supervised entities in the SSM, we do indeed see the threat of increased concentration among only a few major providers of supervised entities, especially when considering sub-outsourcing.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
9	DORA requirements in relation to the Guide	AWS 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 ECB considers the wording "the ECB Guide does not lay down legally binding requirements" (p. 3) to be sufficiently precise in clarifying the nature of the document.	No
25	Scope of DORA	Nordea Abp	With this Guide, the ECB	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	beyond outsourcing	DORA main regulation EU 2022/2554, together with its regulatory technical standards, especially ITS on the Register of Information, RTS for ICT services supporting critical or important functions and RTS for subcontracting, are already detailed and specific on how financial entities should manage its end-to-end supplier value chains, including cloud. This guide should refer to DORA main regulation and the more detailed RTS:s at all times and accurately, especially as DORA widens the scope of outsourcing requirements on a wider circle of ICT TPPs. Important when considering the scope that DORA is not limited to the purpose of outsourcing whereas this guide is.	aims to make its supervisory approach towards cloud outsourcing transparent, without providing additional requirements to those of DORA governance and requirements. Furthermore, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”:	
26	Definitions used in the Guide	Nordea Abp The definitions, especially the ones also defined in DORA, such as critical or important functions and ICT assets, should be aligned in this guide and with DORA, this is currently not the case	The definition of “ICT asset” has been aligned with DORA.	Yes
27	Definition of outsourcing	Nordea Abp The term ”outsourcing” should only be used when referring to services that fall under the definition in the EBA Guidelines on Outsourcing. Not in general when referring to services that are being provided by 3rd party. Cloud services are not always outsourcing according to that definition.	The ECB has clarified the term “outsourcing” in Section 1.2 “Scope and effect” and included the definition in the table.	Yes
28	Use of proprietary technologies	Nordea Abp Please review the applicability of the passage "with many CSPs relying on proprietary technologies" as it mostly applies to Cloud services higher in the stack such as PaaS and SaaS. For IaaS the differences in technologies used by different CSPs applies to much lesser degree and this should be taken into consideration.	The ECB has reformulated this passage to read as follows: “The cloud services market is highly concentrated, with many CSPs relying on proprietary technologies, especially for SaaS and PaaS procurement models, cloud service expose supervised entities to several risks resulting from the dependency on an ICT third-party provider.”	Yes
34	Sub-outsourcing and SaaS	Association of German Public Banks “The ECB Guide refers exclusively to the portfolio of procured cloud solutions.” We suppose that it cannot be the intention, for instance, the simple external procurement of goods supported on a secondary level by cloud (e.g. for delivery planning) or service providers (not directly supporting a critical function) that use off the shelf cloud applications (such as O365) should be associated with cloud service provision. We suggest either removing or reformulating the sentence “Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply”.	The ECB has deleted the word “procured” and made clear that the ECB is referring only to outsourcing arrangements where critical or important functions are affected. However, subcontracting still remains a crucial aspect of the Guide. In order to capture all concentration risks, the ECB would need to keep the reference to subcontracting. Events such as CrowdStrike have shown the important role also played by other service providers when it comes to SaaS solutions.	Yes
54	Relationship between the Guide and DORA	ABBL - The Luxembourg Bankers' Association Additional prescriptive guidance on cloud-specific outsourcing risks is not needed given current EU regulatory frameworks such as DORA and the EBA Outsourcing Guidelines. DORA specifically contemplates the types of risks associated with ICT third-party service providers, such as cloud providers, and sets out enhanced and harmonised risk management requirements, alongside an oversight framework that industry expects will capture those Cloud Service Providers (CSPs) that pose the most significant threat to the stability of the financial sector.	The ECB rejects the notion that the Guide complicates the implementation of DORA. Instead, it provides supervised entities with the ECB’s understanding of DORA, thus making areas of supervisory concern more transparent.	No
55	Alignment of definitions with DORA	ABBL - The Luxembourg Bankers' Association Given the Guide is intended to reflect the ECB's understanding of DORA's requirements, alignment with the DORA's critical or important functions (CIFs) definition would provide welcomed clarity and consistently for industry in meeting supervisory expectations.	The definition of “critical or important function” has been aligned with DORA.	Yes
56	Proportionality	ABBL - The Luxembourg Bankers' Association The Guide applies the proportionality and risk-based principles embedded in DORA inconsistently throughout – applying	The ECB considers that the proportionality principle is sufficiently highlighted in	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		expectations for risk-management of service providers and subcontractors that support CIFs to certain requirements, but not others. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity.	Section 1.2 “Scope and effect”: When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.	
57	Subcontracting	ABBL - The Luxembourg Bankers' Association Where the Guide intends to capture subcontractors, it should explicitly apply a materiality threshold to supply chain scope (in alignment with DORA). Without the consistent application of a risk-based approach, the supervisory expectations in the Guide could be interpreted as applying to a very expansive scope of CSPs and their subcontractors. This further complicates the interpretation and application of the Guide's supervisory expectations consistently with DORA and the EBA Guidelines.	When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality... As risks are not dependent on the length of the sub-contracting chain, the ECB has refrained from introducing another threshold.	No
75	Granularity of the Guide	AFME The Guide introduces prescriptive and granular expectations that 'gold plate' existing requirements on outsourcing, cloud and ICT risk management that will have potential contractual, operational and commercial impacts for FIs, as well as potential impacts to the resilience and competitiveness of EU financial markets more broadly. The Guide should not prescribe specific technology solutions and methodologies to address tech-specific risks that could easily become outdated. Specific technology solutions have downstream impacts on the technology stacks of financial entities that reduces the ability of entities to build stacks that are appropriate for their infrastructure. The Guide should provide flexible guidance that allows FIs to adapt risk management frameworks to cloud-specific risks. With financial entities under severe pressure to ensure DORA requirements are met by Jan 2025, as they also await crucial additional guidance in technical standards yet to be finalized, the Guide's prescriptive and expansive expectations add further complexity - rather than clarity - to the already challenging implementation of DORA. The current landscape includes a number of overlapping and often conflicting regulatory expectations (including the EBA Outsourcing Guidelines which the Guide references, however which industry anticipates will soon be updated to align with DORA).	The Guide is technology-agnostic and is not intended to be prescriptive in the use of certain technologies. c Where good practice examples are mentioned, they merely recognise and illustrate a good practice that supervised entities are free to deviate from.	No
76	Definitions	AFME For the purposes of this Guide, it should be confirmed that critical and important functions within scope should be limited to only those functions from which systemic impacts may arise, in line with the ECB's definition reported in the section "Definitions of terms for the purposes of this Guide". This must be clearly and visibly stressed throughout the Guidance to avoid confusion with the wider definition of Critical and Important Functions under DORA. With the exception of CIFs, the ECB should adopt and ensure consistency with DORA terminology, for example, the definition of ICT asset should align with that set out within DORA.	The definition of “critical or important function” has been aligned with DORA, as has the definition of “ICT asset”.	Yes
77	Proportionality and definitions	AFME The Guide states that firms should take proportionality into scope but does not reference the rigorous proportionality principle embedded in DORA or the EBA Guideline. Proportionality references within the chapters are also applied randomly within individual chapters. For instance, the Guide applies requirements to services supporting CIFs in some cases, but not others. Additionally, it does not reflect the varying levels of risk or technical feasibility relevant to different types of cloud services (i.e. IaaS, PaaS and SaaS). Similarly, the Guide fails to apply materiality to supply chain scope. Without a clear and risk-based approach to the application of supervisory expectations to subcontractors, this could capture an unnecessarily broad scope of subcontractors. Given the Guide is intended to inform the ECB’s expectations of DORA compliance, it should apply a materiality threshold that is consistent with DORA and what is ultimately applied in the final draft regulatory technical standard on subcontracting (i.e. subcontractors which “effectively underpin” CIFs).	The definition of “critical important function” has been revisited. The ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”:	Yes
78	Scope of	AFME	We specified that the	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	application	The ECB propose that where a non-CSP TPP is reliant on cloud services provided by a CSP the same supervisory expectations apply. This does not appear to consider the materiality or criticality of the services provided by the TPP, or define what is meant by "reliant" in this instance. The EBA's draft Technical Standards on the subcontracting of Critical or Important Functions limits its scope to those subcontractors which provide an ICT service which support critical or important functions, or material parts thereof. Furthermore, we understand that the EBA is considering specifying that these requirements would only apply to those subcontractors which "effectively underpin" ICT service supporting critical or important functions or material parts thereof, in line with its draft ITS on the Register of Information. Requiring firms to assess ALL of their Third-Party Providers, regardless of materiality, criticality or risk, to determine the degree of their reliance on CSPs would represent an extraordinarily disproportionate operational burden which could materially impact the commercial viability of institutions at a time when the ECB has been vocal about the need for banks to have sustainable business models. Furthermore, the ECB has failed to explain how these requirements should be applied to TPPs which are reliant on CSPs. Given that the population of institutions' TPPs which are reliant on CSPs is likely to be substantially greater than the number of services provided by CSPs, the ECB should clearly explain how each expectation should be delivered for both CSPs and TPPs. We would propose that the ECB remove this extension of scope and limit their expectations to institutions' use of cloud services provided by CSPs, and rely on the EBA's expected Technical Standards on the subcontracting of Critical or Important Functions to set out robust standards for the management of risks associated with subcontracting.	supervisory expectation applies only to non-CSP TPPs that effectively support critical or important functions.	
79	Scope of application	AFME There is inconsistency in terms of the types of cloud services within scope of the guidance, and parts within. For example, whether this relates to cloud services supporting CIFs or all services, and which types of cloud service (IaaS/SaaS/ PaaS) are subject to specific requirements.	When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.. All procurement models may be subject to the supervisory expectations.	Yes
80	Legal nature of the Guide	AFME The ECB does not indicate the timeline for its planned application of these expectations. As many of the proposed expectations go beyond the requirements of DORA, and institutions' implementation programmes are already well advanced, it would be helpful for the ECB to allow sufficient time for firms to implement their expectations following the completion of implementation of the legal requirements under DORA.	The ECB Guide is to take effect from date of publication. It does not constitute a new legal requirement.	No
81	Legal nature of the Guide	AFME It is not always clear with who the obligation sits, whether a CSP or the financial entity.	The Guide explicitly addresses financial entities. It also acknowledges that in some cases, a joint test with a CSP might not be possible.	No
82	Reference to NIS 2	AFME The Guides consistently references the NIS2 Directive for interpretation even if there are equivalent requirements included in DORA. As DORA is lex specialis to NIS2, these references should be removed.	The ECB has removed all references to the NIS 2 Directive.	Yes
83	Terminology	AFME The use of the word "undertaking" in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and in those commonly used (e.g. from NIST). It should be substituted with "business", "enterprise" or "institution" to avoid uncertainty in the definitions.	The wording has been aligned with the EBA Guidelines on outsourcing arrangements.	Yes
145	Request for more granular guidance	ECIIA What are general controls that should always be covered through cloud audits - and what are the specific controls for specific services?	The ECB Guide is not intended to be prescriptive in the type of controls that are necessary, which may vary depending on the outsourced function.	No
146	Terminology	ECIIA	The wording has been	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		The use of the word "undertaking" in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and in those commonly used (e.g. from NIST). It should be substituted with "business", "enterprise" or "institution"	aligned with the EBA Guidelines on outsourcing arrangements.	
147	Definition of critical or important function	ECIIA The ECB's definition of critical or important functions reported in the section "Definitions of terms for the purposes of this Guide" is: "Activities, services or operations whose discontinuance is likely to lead to disruptions of services that are essential to the real economy in one or more member states or the disruption of financial stability, given the size, market share, external and internal interconnectedness, complexity or cross border nature of an institution or group's activities, particularly as regards the substitutability of those activities, services or operations." It should be confirmed that for the purposes of this Guide, critical functions are only those from which systemic impacts may arise.	The definition of "critical or important function" has been aligned with DORA (Article 3, paragraph 22).	Yes
148	Definition of ICT asset	ECIIA We suggest to align the definition of "ICT asset" to the definition contained in DORA: "a software or hardware asset in the network and information systems used by the financial entity"	The definition of "ICT asset" has been aligned with DORA.	Yes
149	Scope of application	ECIIA Could you specify the cloud service provider which is a subsidiary of a credit institution is not in the scope when it delivers a private or community cloud	The ECB would clarify that the Guide applies only to the sub-outsourcing of critical or important functions. The ECB has included definitions for outsourcing and sub-outsourcing. As long as no sub-outsourcing is involved, the Guide does not apply to in-house solutions provided by subsidiaries of a credit institution.	No
193	Definitions	Confédération Nationale du Crédit Mutuel] Please use the same definition as in GL EBA Outsourcing and DORA	When reviewing the Guide, the ECB aligned further definitions with DORA.	Yes
195	Scope of application	Confédération Nationale du Crédit Mutuel Could you specify the cloud service provider which is a subsidiary of a credit institution is not in the scope when it delivers a private or community cloud	The Guide covers outsourcing arrangements to CSPs. Therefore, it does not apply to in-house solutions.	No
205	Definition of CIF	ABI - ITALIAN BANKING ASSOCIATION The ECB's definition of critical or important functions reported in the section "Definitions of terms for the purposes of this Guide" is: "Activities, services or operations whose discontinuance is likely to lead to disruptions of services that are essential to the real economy in one or more member states or the disruption of financial stability, given the size, market share, external and internal interconnectedness, complexity or cross border nature of an institution or group's activities, particularly as regards the substitutability of those activities, services or operations." It should be confirmed that for the purposes of this Guide, critical functions are only those from which systemic impacts may arise	The definition of "critical or important function" has been aligned with DORA.	Yes
206	Legal nature of the Guide	ABI - ITALIAN BANKING ASSOCIATION "For the purposes of this Guide, it should be confirmed that critical and important functions within scope should be limited to only those functions from which systemic impacts may arise, in line with the ECB's definition reported in the section "Definitions of terms for the purposes of this Guide".	The definition of "critical or important function" has been aligned with DORA. When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.	Yes
207	Definition of undertaking	ABI - ITALIAN BANKING ASSOCIATION The use of the word "undertaking" in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and in those commonly used (e.g. from NIST). It should be substituted with "business", "enterprise" or "institution" to avoid uncertainty in the definitions.	The wording has been aligned with the EBA Guidelines on outsourcing arrangements.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
208	Definition of ICT asset	ABI - ITALIAN BANKING ASSOCIATION Alignment of the definition of "ICT asset" to the definition contained in DORA is highly recommended: "a software or hardware asset in the network and information systems used by the financial entity".	The definition of “ICT asset” has been aligned with DORA.	Yes
209	Scope of application	ABI - ITALIAN BANKING ASSOCIATION The sentence "Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply" should be limited in scope in order to be only addressed to critical or important functions.	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are addressed.	Yes
210	Scope of application	ABI - ITALIAN BANKING ASSOCIATION The Guide states: "The supervisory expectations set out in the ECB Guide are addressed to institutions that are supervised directly by ECB Banking Supervision.". Confirmation is sought that the Guide applies to the Banks reported in the list of supervised entities only (as published on the SSM website).	The ECB can confirm that the ECB Guide applies only to significant entities directly supervised by the ECB and included on the list of supervised entities published on the SSM website.	No
257	Proportionality	Banking and Payment Federation Ireland (BPFI) In our view, the draft Guide does not reflect the DORA proportionality principle that considers the nature of the engagement or dependency on a financial entity’s services or activities. Effective and proportionate risk management should take into account the cloud service and not be applied on a blanket basis across all SaaS, PaaS and IaaS solutions. We therefore recommend that the ECB Guide recognises the DORA proportionality principle or refers to the criticality of the cloud services on a financial entity’s services or activities. We would therefore make the following drafting recommendation: 1.2: “When applying these expectations, account should be taken of the principle of proportionality as reflected in Article 28(1)(b) of DORA.”	The ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”:	No
258	Definition of critical or important function	Banking and Payment Federation Ireland (BPFI) We believe that the Guide creates interpretation issues by inconsistently applying expectations for outsourced cloud services that support Critical or Important Functions (CIFs) in certain chapters and not in others. For example, criticality is referenced in relation to cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring, but not disaster recovery strategy, ICT security and location of data. As a consequence, we believe this approach would be disproportionate and add complexity to the framework. For instance, applying disaster recovery ‘spot check’ requirements across every SaaS provided by a firm would be disproportionate and overly burdensome to achieve. As cloud technologies cover a significant array of outsourced activities, this would constitute a vast level of operational change with limited benefit nor recognition of effective risk management practices. We recommend that the ECB includes a more detailed proportionality principle that applies to all Chapters or is more specific concerning their expectation for cloud outsourcing as it relates to CIFs. Furthermore, the terminology and definitions around criticality is itself inconsistent and could result in firms taking vastly different approaches to implementation of the guide and DORA, ultimately hampering harmonisation. Specifically, the draft guidance uses two definitions regarding the criticality of functions supported by CSPs, “critical or important functions”, and “critical functions”. “Critical or important functions” is defined on page 2 in the definitions table under section 1.1 with a definition which appears derived from (but not identical to) the definition of “Critical Functions” from BRRD rather than the more recent definition of a “Critical or important function” under DORA. Under section 2.2.2 Proportionate requirements for critical functions the ECB then use the term “Critical Functions”, which they note is as defined in paragraph 29(a) of the EBA Guidelines on outsourcing arrangements. Paragraph 29(a) of the EBA’s Guidelines on outsourcing arrangements defines the term “Critical or important functions” for the purposes of those guidelines.	The definition of “critical or important function” has been aligned with DORA. When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.	Yes
259	Scope of application	Banking and Payment Federation Ireland (BPFI) We would highlight that the extension of the ECB’s expectations to TPPs which are reliant on cloud services provided by a CSP fails to define what it means by “reliance”,	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		and does not consider either materiality or risk. The EBA's draft Technical Standards on the subcontracting of Critical or Important Functions limits its scope to those subcontractors which provide an ICT service which support critical or important functions, or material parts thereof. Furthermore, we understand that the EBA is considering specifying that these requirements would only apply to those subcontractors which "effectively underpin" ICT service supporting critical or important functions or material parts thereof, in line with its draft ITS on the Register of Information. Requiring firms to assess all of their Third-Party Providers, regardless of materiality, criticality or risk, to determine the degree of their reliance on CSPs would represent an extraordinarily disproportionate operational burden which could materially impact the commercial viability of certain institutions at a time when the ECB has been vocal about the need for banks to have sustainable business models. Furthermore, the ECB has failed to explain how any of the proposed requirements should be applied to TPPs which are reliant on CSPs. Given that the population of institutions' TPPs which are reliant on CSPs is likely to be substantially greater than the number of services provided by CSPs, the ECB should further elaborate how each expectation should be delivered for both CSPs and TPPs. We would, however, propose that the ECB remove this extension of scope and limit their expectations to institutions' use of cloud services provided by CSPs, and rely on the EBA's expected Technical Standards on the subcontracting of Critical or Important Functions to set out robust standards for the management of risks associated with subcontracting. At a minimum, we would recommend that the ECB defer further development of its expectations on cloud outsourcing until the Technical Standards on the subcontracting of CIFs is complete, to enable them to align their proposals with the EBA and avoid divergence.	addressed.	
280	Definitions	European Cloud User Coalition (ECUC) The guide is using the BRRD (Bank Recovery and Resolution Directive) definition of critical and important functions (CIFs), rather than the DORA definition or other set definition from NIS2 or EBA guidelines which are understood to be different. Neither is any reference made to the EBA Guidelines on outsourcing, guidelines that use concepts that are also different from this ECB Guide.	The definitions used in the Guide have been aligned with the DORA definitions.	Yes
292	Reference to NIS 2	European Cloud User Coalition (ECUC) The ECB Guide states in the second paragraph of this chapter that it "does not lay down legally binding requirements ... nor should it be construed as introducing new rules or requirements". However the general wording of the ECB Guide seems to set explicit expectations that in our opinion go beyond the DORA-requirements. In order to avoid misunderstandings, we would welcome a very clear distinction between explicit (binding) expectations on the one hand, and (non-binding) best practices – only clarifying a possible approach – on the other hand. As DORA constitutes lex specialis with regard to NIS 2 (see Recital 16 DORA), we assume that institutions are allowed to implement this ECB Guide according to the proportionality principle in DORA. Please confirm.	All references to the NIS 2 Directive have been removed from the Guide. Good practice examples are explicitly described as such in the Guide, and the remaining passages represent the ECB's understanding of the applicable legislation, so the Guide does not include binding provisions beyond the Union and implementing regulations provisions referred therein.	Yes
293	Legal nature of the Guide	European Cloud User Coalition (ECUC) On the one hand the ECB guide takes EBA guidelines on outsourcing as a starting point and DORA is considered as much as possible. On the other hand, DORA precedes over the other 2. Please clarify if the ECB Guide is meant to reflect that the ECB Guide should be read in conjunction with DORA and EBA Guidelines on outsourcing arrangements and that DORA takes precedence over this ECB Guide or whether it's meant to reflect that DORA takes precedence over both this ECB guide and the EBA guidelines on outsourcing arrangements. Wouldn't it be better to bring this guide under DORA instead of separately?	We confirm that the ECB Guide does not constitute a new piece of legislation, but is intended to provide further transparency as to the ECB's supervisory focus on the risks stemming from cloud outsourcing. The DORA regulation is directly binding in its entirety on all addressees, as are the EBA Guidelines on outsourcing arrangements. The ECB Guide provides the ECB's interpretation of DORA for supervised entities and provides examples of good practices for risk	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			management in cloud outsourcing arrangements.	
294	Legal nature of the Guide	European Cloud User Coalition (ECUC) ECB states that the Guide does not provide for additional rules, nor that it replaces existing rules. However, in many paragraphs, rules/guidelines are mentioned referring to 'good practice': can you be more specific on the basis of such good practice? Where is that specifically mentioned?	The good practice examples are derived from supervisory activities and experience. The ECB does not expect supervised entities to implement them in their entirety, as other solutions might be considered more proportionate and therefore preferable for technological or other reasons. However, the good practice examples can serve as a starting point for further supervisory dialogue on risk management in cloud outsourcing arrangements.	No
295	Legal nature of the Guide	European Cloud User Coalition (ECUC) In relation to the foregoing question, please elaborate more on the binding status of the various requirements as laid down in the Guide; on the one hand it is mentioned that the Guide 'does not lay down legally binding requirements', but on the other hand on various occasions it appears that financial institutions are required to comply to the requirements by using the words 'institutions should', see for instance 2.1.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.2., 2.3.2., 2.3.4.1., 2.3.4.2., 2.4.1., 2.4.2., 2.4.3., 2.5., 2.5.1., 2.5.2., 2.5.3 and Is the use of the word 'ensure' in the last bullet in 2.2.2.. Is the assumption correct that the words 'should' and 'ensure' imply that there is not strict obligation to comply, but merely imply a non-binding suggestion? Please advice and instruct.	The ECB Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
318	Prescriptiveness of the Guide	European Banking Federation The ECB Guide (hereinafter: “the Guide”) adds further prescriptive guidance that significantly expands DORA’s scope and adds another layer of overlapping guidance for ECB supervised entities to comply with. The ECB should not prescribe specific forms of technology solution that define a Financial Entity’s (hereinafter: FEs) future technology stack and adoption.	The ECB rejects the notion that the Guide prescribes certain technological solutions.	No
319	Definition of ICT asset	European Banking Federation The definition of an “ICT Asset” to be aligned with the one contained under DORA. Whilst the ECB Guide is using "[…] that is found in the business environment", DORA defines ICT assets as software or hardware assets "in the network and information systems used by the financial entity".	The definition of “ICT asset” has been aligned with DORA.	Yes
320	Scope of application	European Banking Federation We seek clarification if the Guide has a primary focus on IaaS/PaaS or if it applies to all cloud service types (IaaS, PaaS and SaaS).	The ECB Guide applies to all cloud outsourcing arrangements, although the expectations are subject to the proportionality principle.	No
321	Scope of application	European Banking Federation The sentence "Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply" should be limited in scope in order to be only addressed to critical or important functions.	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are addressed.	Yes
322	Scope of application	European Banking Federation The Guide applies requirements to services supporting critical or important functions in certain chapters, but not in others. It also applies expectations for the risk management of all types of cloud services without reflecting the varying levels of risk and technical specification relevant to different types of cloud such as IaaS, PaaS and SaaS. Where the Guide intends to capture subcontractors, it should explicitly apply a materiality threshold to supply chain scope in alignment with DORA.	When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality., including sub-outsourcing arrangements.	Yes
323	Scope of application	European Banking Federation We suppose that it cannot be the intention, for instance, the simple external procurement of goods supported on a secondary level by cloud (e.g. for delivery planning) or service	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		providers (not directly supporting a critical function) that use off the shelf cloud applications (such as O365) should be associated with cloud service provision. Therefore, we suggest either removing or reformulating the sentence “Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply”, by clarifying what is meant by “reliant on”.	addressed.	
324	Definition of outsourcing	European Banking Federation We would like it to be clarified that the use of the term ‘outsourcing’ does not correspond to the meaning according to relevant external requirements, e.g., EBA Guidelines on outsourcing. In the Guide, the term is used in a way that is conceptually incorrect. As an example, ‘institutions’ outsourcing of cloud services’ is misleading in that banks outsource functions to cloud service providers; banks do not outsource cloud services to cloud service providers. Also, ‘outsourcing of ICT services’ is misleading. Banks purchase ICT services within a framework where occasional outsourcing situations arise, an example of which is the use of cloud services.	The definition of outsourcing is now aligned with the EBA Guidelines on outsourcing arrangements.	Yes
325	Scope of application	European Banking Federation The Guide states: "The supervisory expectations set out in the ECB Guide are addressed to institutions that are supervised directly by ECB Banking Supervision.". Confirmation is sought that the Guide applies to the Banks reported in the list of supervised entities only (as published on the SSM website).	The ECB can confirm that the ECB Guide applies only to significant entities directly supervised by the ECB and included on the list of supervised entities published on the SSM website.	No
387	Legal nature of the Guide, definition of “cloud service” and proportionality	Dutch Banking Federation (DBF) To start with, we need clarity on the legal status and binding nature of the supervisory expectations. On one hand, the Guide does not provide additional rules, but on the other hand, it appears that rules are indeed being imposed. Furthermore, the basis for most of the mentioned rules is not specified, and they seem to be in addition to the existing rules of DORA, NIS2, CDD, and EBA. The definition of “cloud service” lacks clarity. Institutions seek explicit guidance on which cloud services are not considered outsourcing. The concern is that widely available and not customized cloud services are not available for negotiation due to their standardized terms. We need clarification that using such cloud services do not constitute outsourcing when they won’t significantly impact critical processes. Since DORA constitutes lex specialis with regard to NIS 2 (see Recital 16 DORA), we assume that institutions are allowed to implement this ECB Guide according to the proportionality principle in DORA. Could you please confirm this. Last point that needs to be clarified: Article 21 of NIS 2 also includes some proportional approaches. Could you explain how these principles/approaches in NIS 2 and DORA interrelate and how entities can use them without risking conflicting interpretations.	The ECB Guide does not lay down new legally binding requirements. It provides supervised entities with the ECB’s understanding of relevant legal requirements, thus making areas of supervisory concern more transparent. The definition of “cloud service” is aligned with the EBA Guidelines on outsourcing arrangements. The ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”.	No
388	Legal references	Dutch Banking Federation (DBF) Article 74 of the Capital Requirements Directive (CRD)3 deals with internal governance and recovery and resolution plans. It outlines robust governance arrangements for institutions. Article 74 also touches on accounting standards and remuneration practices. While it doesn’t directly combine with DORA-Article 5, both are essential for financial stability and risk management. Our recommendation is to combine Article 74 with Article 5 of DORA.	The ECB considers the legal references to sufficiently justify its supervisory expectations.	No
389	Legal nature of the Guide	Dutch Banking Federation (DBF) We would request further clarification on the expectations. The guidance is stated to be non-binding, and secondary to the legally binding obligations of DORA. The language throughout shifts from practices which "should" be undertaken, to suggested best practice. If the ECB expects strict adherence to all aspects of the guidance, rather than allowing firms to take a risk-based, proportionate approach, this requirement should be explicitly stated.	The ECB Guide aims to provide supervised entities with the ECB’s understanding of relevant legally binding requirements. When applying these expectations, supervised entities should take account of the principle of proportionality (see Section 1.2).	No
390	Definition of	Dutch Banking Federation (DBF)	The definition of “outsourcing” has been	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	outsourcing	We need more guidance and clarity on the definitions EBA outsourcing rules. Because the definitions in EBA outsourcing rules differ and are not similar to the DORA, NIS2 definitions. To start with, there is unclarity about the definition of outsourcing.	added to the table of definitions provided in Section 1.1.	
391	Definition of critical or important function	Dutch Banking Federation (DBF) BRRD (Bank Recovery and Resolution Directive) defines 'critical or important functions' different then the definition from EBA outsourcing and DORA. We recommend to alter definition or include expand name.	The definition of “critical or important function” has been aligned with DORA.	Yes
392	Definitions and scope of application	Dutch Banking Federation (DBF) We strongly advise to remove existing definitions and refer to applicable guidelines. For example, align definitions as 'service provider' with the definition of 'third party service provider' under DORA. Another example it is unclear what is meant by CPS in case of SaaS, do you mean the SaaS provider or the underlying cloud platform provider.	The definitions have been aligned with DORA and the EBA Guidelines on outsourcing arrangements. SaaS not offered by CSPs but by other TPPs is covered if it effectively supports critical or important functions.	Yes
393	Scope of application	Dutch Banking Federation (DBF) We would request confirmation regarding the Guide is only applicability to Banks included in the list of supervised entities, as published on the SSM website.	The ECB can confirm that the ECB Guide applies only to significant entities directly supervised by the ECB and included on the list of supervised entities published on the SSM website.	No
394	Terminology	Dutch Banking Federation (DBF) We would like to point out that the use of the word ‘undertaking’ in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and those commonly used (e.g., from NIST). To avoid misinterpretation in definitions, we suggest substituting it with ‘business,’ ‘enterprise,’ or ‘institution.’”	The wording has been aligned with the EBA Guidelines on outsourcing arrangements.	Yes
395	Legal nature of the Guide	Dutch Banking Federation (DBF) The Guidance notes that DORA requirements are legally binding obligations. However, specific provisions within the guidance may necessitate additional contractual adjustments. Given the urgency for financial entities to meet DORA requirements by January 2025, we asking confirmation that there is no expectation of further remediation.	The ECB expects supervised entities to adhere to legally binding requirements such as DORA. The ECB guide does not constitute a new legal requirement but rather provides supervised entities with the ECB’s understanding of DORA, thus making areas of supervisory concern more transparent.	No
396	Application date	Dutch Banking Federation (DBF) We require clarity that the guidance, as the ECB's view on DORA, does not come into effect until the application of DORA from 17th Jan 2025.	The ECB Guide is to take effect from date of publication. It does not constitute a new legal requirement.	No
397	Legal nature of the Guide	Dutch Banking Federation (DBF) Further clarification is required regarding which party bears the obligation, whether it is the CPS or the financial entity. For example the proposed approach on joint testing is unlikely to work in practice unless CPS is target of certain provisions.	The Guide is explicitly addressed to financial entities. It also acknowledges that in some cases, a joint test with a CSP might not be possible.	No
398	Legal nature of the Guide	Dutch Banking Federation (DBF) We would prefer clarification on whether the ECB Guide is intended to indicate that it should be read alongside DORA and the EBA Guidelines on outsourcing arrangements. Unclear is it meant to convey that DORA takes precedence over both the ECB guide and the EBA guidelines on outsourcing arrangements. Our recommendation is to consolidate the ECB Guide within DORA instead of keeping them separate.	The ECB Guide should be read in conjunction with DORA and aims to provide supervised entities with the ECB’s understanding of DORA, thus making areas of supervisory concern more transparent	No
399	Clarification of “good practice”	Dutch Banking Federation (DBF) ECB states that the Guide neither provides additional rules nor replaces existing ones. However, many paragraphs mention rules/guidelines that refer to "good practice". We require more clarity on what constitutes "good practice".	“Good practice” refers to examples of effective practices among supervised entities observed during ongoing supervision as well as on-site inspections and should complement	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			supervisory expectations.	
400	Legal nature of the Guide	Dutch Banking Federation (DBF) The Guide states that the existing EBA guidelines continue to apply. The overlapping regulatory requirements create conflicting expectations, prevent scattered details across different guidances. For example, whether the provisions should apply to CIFs or to all services. The ECB should bear in mind that the ESAs want to address duplication between the DORA and the EBA guidelines, and therefore take a similar approach by stating that these guidelines take precedence.	The ECB Guide does not lay down new regulatory requirements. It should be read in conjunction with DORA and the EBA Guidelines on outsourcing arrangements, which have been taken into consideration to the extent possible.	No
401	Definitions	Dutch Banking Federation (DBF) We strongly recommend aligning the definitions with DORA. The Guide currently uses the BRRD definition of Critical and Important Functions, which misaligns with DORA. Another example is the definition of ICT assets, which differs from the DORA definition. Last example 'outsourcing' is not clearly defined in regulation and more confusion for supervised institutions will be caused if there is no common terminology in relation to outsourcing	The definitions of “critical or important function” and “ICT asset” have been aligned with DORA. The definition of “outsourcing” has been added to the table of definitions provided in Section 1.1.	Yes
402	Scope of application	Dutch Banking Federation (DBF) We strongly recommend to provide more consistency regarding the types of cloud services within the scope. For example, whether this relates to cloud services supporting CIFs or all services, and which types of cloud service (IaaS/SaaS/ PaaS) are subject to specific requirements. If SaaS falls within the scope, it remains unclear whether it is expected to have full visibility of each cloud region topology supporting the SaaS. Without clarity the Guide will be lacking in proportionality and enforceability.	When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.. All procurement models may be subject to the supervisory expectations.	Yes
403	Scope of application	Dutch Banking Federation (DBF) It is unclear to what extent the requirements should apply down the supply chain. We recommend limiting them to direct cloud services with which the financial entity has a contractual relationship. Without this limitation, there would be a lack of proportionality. For example, the sentence: 'Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply' should be limited in scope in order to be only addressed to CIFs.	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are addressed.	Yes
471	Benefits of cloud service usage	DIGITALEUROPE The Guide states that cloud service usage is inherently riskier than other ICT solutions. 1.1 (first bullet) should be amended to read: '…THE USE OF CLOUD SERVICES CAN BRING NUMEROUS BENEFITS TO THE BANKING INDUSTRY, INCLUDING ACCESS TO INNOVATIVE TECHNOLOGIES, SCALABILITY, FLEXIBILITY, AND ENHANCED SECURITY AND OPERATIONAL RESILIENCE. HOWEVER, IT CAN ALSO INCREASE INSTITUTIONS' EXPOSURE TO SEVERAL RISKS, NOTWITHSTANDING THE COMMITMENT OF CSP TO COMPLY WITH THE HIGHEST STANDARDS'.	The Guide expresses a technology-agnostic view. Apart from highlighting risks that are particularly important in cloud environments, it also acknowledges the benefits of cloud technologies.	No
472	Objectives of DORA	DIGITALEUROPE The third bullet should be amended as follows: DORA, which focus on 'ENSURING THAT ALL PARTICIPANTS IN THE FINANCIAL SYSTEM HAVE THE NECESSARY SAFEGUARDS IN PLACE TO MITIGATE ICT RISKS, INCLUDING ICT THIRD-PARTY RISKS'.	The wording has been changed to reflect the broader objectives of DORA.	Yes
473	DORA requirement in relation to the Guide	DIGITALEUROPE The ECB Guide exclusively focuses on cloud services whereas DORA focuses on a broader range of ICT services. 'WHILE THE GUIDE FOCUSES ON THE USE OF CLOUD SERVICES, THE SSM THE SSM SUPERVISORY EXPECTATIONS ON CLOUD OUTSOURCING ARE ALIGNED WITH DORA SCOPE AND AIM. THE SAME LEVEL OF RESILIENCE AS PER DORA SHOULD BE ENSURED...'	The Guide is technology-agnostic and is not intended to be prescriptive in the use of certain technologies.	No
474	Definition of critical or important function	DIGITALEUROPE The definition of the 'critical or important function' does not correspond to the definition of Art. 3(22) of DORA Regulation, which is the following: 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would	The definition of “critical or important function” has been aligned with DORA.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law'.		
475	Definitions	DIGITALEUROPE The ECB Guide uses terms that have already been defined in other documents such as DORA or the EBA Guidelines on outsourcing arrangements (or the BRRD). The 'Definitions of terms for the purpose of this Guide' table should be deleted in its entirety and replaced with a cross-reference to the relevant pieces of legislation that the ECB has in mind.	The definitions have been aligned with DORA and the EBA Guidelines on outsourcing arrangements.	Yes
476	Legal nature of the Guide	DIGITALEUROPE The ECB Guide states that 'THE SUPERVISORY REGIME UNDER DORA THAT WILL ENTER INTO FORCE ON 17 JANUARY 2025 HAS BEEN TAKEN INTO CONSIDERATION TO THE EXTENT POSSIBLE' (own emphasis). This sentence should be clarified as it is unclear at present why it would not be possible to take into account the mandatory (including for the ECB) supervisory regime established by DORA.	The ECB Guide does not lay down new regulatory requirements. It should be read in conjunction with DORA and the EBA Guidelines on outsourcing arrangements, which have been taken into consideration to the extent possible.	No
499	Legal nature of the Guide	European Association of Public Banks The guidance is stated to be non-binding, and secondary to the legally binding obligations of DORA. The language throughout shifts from practices which "should" be undertaken, to suggested best practice. This leads to uncertainty over the ECB's expectations.	The ECB Guide aims to provide supervised entities with the ECB's understanding of relevant legally binding requirements. When applying these expectations, supervised entities should take account of the principle of proportionality (see Section 1.2).	No
500	Scope of application	European Association of Public Banks What is exactly meant by CSP in case of SaaS? The SaaS provider or the underlying cloud platform provider?	SaaS not offered by CSPs but by other TPPs is covered if it effectively supports critical or important functions.	No
501	Definition of critical or important function	European Association of Public Banks Align the definition of "critical or important function" with the DORA definition of "Critical or Important Function"	The definition of "critical or important function" has been aligned with DORA.	Yes
502	Definition of ICT asset	European Association of Public Banks Align the definition of "ICT assets" with the DORA definition of "ICT asset"	The definition of "ICT asset" has been aligned with DORA.	Yes
503	Definition of service provider	European Association of Public Banks Align the definition of 'service provider' with the definition of 'third party service provider' under DORA	The definition of "service provider" has been aligned with the EBA Guidelines on outsourcing arrangements.	Yes
504	Definition of outsourcing	European Association of Public Banks Which definition of outsourcing is used here?	The definition of "outsourcing" has been added to the table of definitions provided in Section 1.1.	Yes
505	Definition of CIF	European Association of Public Banks The definition of a critical or important function differs from the definition as outlined in the EBA Guidelines on outsourcing arrangements as well as under DORA. In the ECB Guide critical/important is more or less seen from a macro perspective and not just from an individual financial institutions impact whereas later in this guide the definition within DORA is explicitly referenced.	The definition of "critical or important function" has been aligned with DORA.	Yes
506	Definition of ICT asset	European Association of Public Banks The definition of an "ICT Asset" also slightly differs from DORA. Whilst the ECB guide is using "[…] that is found in the business environment", DORA defines ICT assets as software or hardware assets "in the network and information systems used by the financial entity".	The definition of "ICT asset" has been aligned with DORA.	Yes
507	Legal nature of the Guide	European Association of Public Banks While the guidance notes that DORA requirements remain the legally binding obligations, certain provisions within the guidance could require further contractual remediation.	The ECB expects supervised entities to adhere to legally binding requirements such as DORA. The ECB guide does not constitute a new	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			legal requirement, but rather provides supervised entities with the ECB's understanding of DORA, thus making areas of supervisory concern more transparent.	
508	Application date	European Association of Public Banks It should be clarified that the guidance, as the ECB's view on DORA, does not come into effect until the application of DORA from 17th Jan 2025.	The ECB guide is to take effect from date of publication. It does not constitute a new legal requirement.	No
509	Legal nature of the Guide	European Association of Public Banks It is not always clear with who the obligation sits, whether a CSP or the financial entity.	The Guide is explicitly addressed to financial entities. It also acknowledges that in some cases, a joint test with a CSP might not be possible.	No
510	Legal nature of the Guide	European Association of Public Banks The proposed guidance states that the existing EBA Guidelines remain applicable. ECB should be mindful that the ESAs are looking to address duplication between DORA and the EBA Guidelines, and thereby take a similar approach by stating these Guidelines supersede.	The ECB Guide does not lay down new regulatory requirements. It should be read in conjunction with DORA and the EBA Guidelines on outsourcing arrangements, which have been taken into consideration to the extent possible.	No
511	Definitions	European Association of Public Banks The Guidance is using the BRRD definition of Critical and Important Functions, rather than the DORA definition which is unhelpful misalignment. Similarly, the definition of ICT asset should be that which is used in DORA.	The definitions of "critical or important function" and "ICT asset" have been aligned with DORA.	Yes
512	Scope of application	European Association of Public Banks There is inconsistency in terms of the types of cloud services within scope of the guidance, and parts within. For example, whether this relates to cloud services supporting CIFs or all services, and which types of cloud service (IaaS/SaaS/ PaaS) are subject to specific requirements. If SaaS is in scope, is it expected to have full visibility of each Cloud region topology (for example 3 different campus) supporting the SaaS?	When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.. All procurement models may be subject to the supervisory expectations.	Yes
513	Scope of application	European Association of Public Banks Similarly there is a lack of clarity over how far down the supply chain the requirements should apply. It should be limited to direct cloud services, with which the financial entity has a contractual relationship. The sentence "Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply" should be limited in scope in order to be only addressed to CIFs.	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are addressed.	Yes
514	Legal nature of the Guide	European Association of Public Banks The guidelines state "Also, the ECB Guide may be complemented by publications produced by other supervisory authorities within the Single Supervisory Mechanism (SSM)". The aim of DORA was to align different/scattered guidances and legislations. This seems contradictory to the aim of DORA.	The ECB Guide does not lay down new regulatory requirements. It should be read in conjunction with DORA and the EBA Guidelines on outsourcing arrangements, which have been taken into consideration to the extent possible.	No
515	Sub-outsourcing and SaaS	European Association of Public Banks "The ECB Guide refers exclusively to the portfolio of procured cloud solutions." We suppose that it cannot be the intention, for instance, the simple external procurement of goods supported on a secondary level by cloud (e.g. for delivery planning) or service providers (not directly supporting a critical function) that use off the shelf cloud applications (such as O365) should be associated with cloud service provision. We suggest either removing or reformulating the sentence "Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply".	The ECB has removed the word "procured" When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality.. However, subcontracting is still a crucial aspect of the Guide. In order to capture all concentration risks, we would need to keep the existing reference to subcontracting. Events such as CrowdStrike have shown	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			the important role also played by other service providers when it comes to SaaS solutions.	
598	Relationship between the Guide and DORA and concentration risks	Bitkom 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:	The ECB believes that the reasons for issuing an ECB guide specifically addressing cloud outsourcing are sufficiently substantiated in Section 1.1 of the document. This does not diminish or compromise the applicability of DORA to all ICT TPPs. The Guide expresses a technology-agnostic view. Apart from highlighting risks that are particularly important in cloud environments, it also acknowledges the benefits of cloud technologies. The ECB provides in the Guide its understanding of the relevant DORA provisions and recommends good practices, so the Guide does not introduce new requirements beyond Union legislation thereby referred. When analysing the outsourcing registers of supervised entities in the SSM, the ECB happens to see the threat of increasing levels of concentration among only a few major providers, especially when considering sub-outsourcing.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		"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.		
599	DORA requirements in relation to the Guide	Bitkom 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 ECB considers the wording "the ECB Guide does not lay down legally binding requirements" to be sufficiently precise in clarifying the nature of the document.	No
640	Definition of critical or important function	European Savings and Retail Banking Group (ESBG) The definition of the "critical or important function" does not correspond to the definition of Article 3(22) of DORA Regulation, which is the following: " 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law".	The definition of "critical or important function" has been aligned with DORA.	Yes
647	Legal nature of the Guide	Futures Industry Association The Guide introduces prescriptive requirements that	The ECB rejects the notion that the Guide complicates the implementation of	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		significantly expand upon existing regulatory expectations in DORA and the EBA Outsourcing Guidelines. Particularly given the Guide has been issued at a time when industry is working to implement its compliance with DORA's requirements (and awaiting the finalisation of crucial technical standards), the Guide adds a further layer of complexity to existing overlapping regulatory expectations spanning outsourcing, third-party risk, ICT and cyber risk and risks undermining DORA's harmonization objectives. In particular, we urge the ECB not to prescribe specific forms of technology solutions. A strict interpretation and application of the Guide could significantly impact cloud adoption, resilience and innovation in the EU financial sector.	DORA. It rather provides supervised entities with the ECB's understanding of DORA, thus making areas of supervisory concern more transparent. Moreover, the Guide is technology-agnostic and is not intended to be prescriptive in the use of certain technologies.	
648	Definition of CIF and subcontracting	Futures Industry Association To facilitate the sector's implementation of DORA and the ECB's supervisory expectations, the Guide should align with DORA's scope and technical requirements. In particular, the Guide should adopt DORA's definition of critical and important functions (CIFs) to support the sector in its understanding and implementation of the diversity in terminology used to identify "critical" functions. The Guide also separately references the EBA Outsourcing Guidelines in the context of "critical functions" Similarly, we urge the ECB to adopt its terminology and scope with respect to subcontractors. The Guide references "suppliers of subcontracted services supporting the CSP" which is not used in DORA. The Guide should adopt the language in the draft ITS on the Register of Information (i.e. "subcontractors that effectively underpin the provision of ICT services supporting CIFs), to avoid further confusion and to ensure the appropriate application of materiality to supply chain scope.	The definition of "critical or important function" has been aligned with DORA. When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality., including sub-outsourcing arrangements.	Yes
649	Proportionality	Futures Industry Association Amendment Recommendation: 1.2: "When applying these expectations, account should be taken of the principle of proportionality as reflected in Article 28(1)(b) of DORA." The Guide does not take sufficiently into account the proportionality principle embedded in the Digital Operational Resilience Act (DORA) nor does it consider the various types and materiality of outsourced cloud services. The proportionality principle of DORA in relation to ICT Third Party Risk (Article 28) states that financial entities should take into account "the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities." The ECB's Guide does not reflect the DORA principle in regards of cloud services and therefore does not consider the cloud services relationship or dependency on the financial entity's services or activities. When managing third-party risk, it's essential to consider the cloud service specifically rather than applying a one-size-fits-all approach across all SaaS, PaaS, and IaaS solutions. For instance, Microsoft have a SaaS data visualisation tool, called Power BI, which can support CIFs but, if non-functioning, would not result in any impact to the service provided to the customer or cause any financial impact. A more detailed proportionality principle would, furthermore, align to the EBA's principle of proportionality whereby an institution should take into account "the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities. We suggest that the ECB Guide acknowledge the proportionality principle outlined in DORA or consider the significance of cloud services for a financial entity's operations.	The ECB considers that the proportionality principle is sufficiently explained in Section 1.2 "Scope and effect":	No
667	Definition of critical or important function	German Banking Industry Committee (GBIC) The definition of a "critical or important function" differs significantly from the definition as outlined in the EBA Guidelines on outsourcing arrangements as well as under DORA (Art. 3 Sec. 22). According to the draft ECB Guide, critical/important shall be more or less seen from a macro perspective and not just from an individual financial institution's impact. We do not consider such a different definition to be useful, not least because an institution's risk management can	The definition of "critical or important function" has been aligned with DORA.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		ultimately only take its own perspective. Instead, reference should be made to the DORA definition. The macro perspective is under the remit of the supervisory authorities.		
668	Definition of ICT asset	German Banking Industry Committee (GBIC) The definition of an „ICT Asset“ also slightly differs from DORA. Whilst the ECB guide is using "... that is found in the business environment", DORA defines ICT assets as software or hardware assets "in the network and information systems used by the financial entity". If the intended meaning does not differ between the two, we suggest to relate to the existing DORA definition.	The definition of “ICT asset” has been aligned with DORA.	Yes
669	Definitions	German Banking Industry Committee (GBIC) The definition of “cloud“, “hybrid cloud“ and „hybrid cloud“ differ from EBA/REC/2017/03 as of 20.12.2017.	The wording has been aligned with the EBA Guidelines on outsourcing arrangements.	Yes

2.2 Table 2 – Comments on Section 2.1: Governance of cloud services

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
36	Risk management	Association of German Public Banks Under Art. 28 (4) DORA, institutions are required to conduct risk analysis...prior to entering into a new outsourcing arrangement with a CSP. In order to adequately identify . the institutions should: We suggest to replace “institutions should” by “best practice shows...”	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
37	Exit strategy	Association of German Public Banks Art. 2.1.2. mentions „vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required“ as good practice to consider risk. We suggest to add “if required and possible” given the strong contractual ties.	The ECB is of the view that supervised entities should maintain, where required by Article 28 of DORA, exit strategies that are practicable in all circumstances.	No
38	Risk management	Association of German Public Banks The consideration of "physical risks and region-specific risks (e.g. political stability risks)" and "the risk of a considerable fall in in quality or a significant increase in price (both of which are common scenarios in a highly concentrated market)" go beyond the existing EBA requirements or DORA. Additionally, the risk of a considerable fall in quality is highly subjective and should be deleted. Both references should be deleted	While the ECB is of the view that DORA does not exhaustively enumerate the risks scenario to consider, the ECB recommends considering such risks as a matter of good practice only.	No
59	Risk management	ABBL - The Luxembourg Bankers' Association Risk management and contractual frameworks between FIs and third-parties impose appropriate risk management obligations on third-parties. We therefore suggest the following amendment: Consequently, institutions should ensure that their CSPs have established equivalently effective risk management practices, processes and controls.	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
60	Risk management	ABBL - The Luxembourg Bankers' Association The requirement to: “assess the CSP’s ability to provide the information required	The ECB is of the view that the measures set out in this paragraph are needed in order to assess the relevant	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		for these checks" lacks clarity; • "ensure that the CSP has itself properly implemented the relevant checks" lacks clarity and should be reframed as "assess that.."; • consider "the risk of a considerable fall in quality", is subjective and not feasible at the pre-contractual stage. This risk is managed through contractual provisions and the ongoing monitoring process addressing service level quality and performance. • consider "the risk of a significant increase in price" is not feasible at the pre-contractual stage. This risk is managed through contractual provisions. • consider "the risk of a significant increase in price" is not feasible at the pre-contractual stage. This risk is managed through contractual provisions.	risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	
84	Risk management	AFME The ECB includes a requirement to for institutions to "ensure that the CSP has itself properly implemented the relevant checks", however it does not clearly establish what is means by "relevant checks". It would be helpful for the ECB to more clearly explain the scope and nature of the checks that CSPs should be expected to perform.	From a regulatory standpoint, the supervised entity must ensure that risk management processes and controls in line with their ICT risk framework are in place. This may include the supervised entities collaborating with the CSP.	No
85	Risk management	AFME The final sentence on ensuring that CSPs have equivalent risk management practices, could lead to misunderstanding that CSPs have to mirror the obligations on FEs. This expectation goes beyond current regulatory expectations and reasonable risk management practices. The sentence should be deleted given the repetition with the preceding one, or at least it should be clarified that this is about assessing that "CSPs have established equivalently effective risk management practices."	The ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures. For this reason, this is indicated as a good practice in the Guide.	No
86	Risk management	AFME The risk considerations are prescriptive, expand existing requirements in DORA and EBA and do not reflect a risk-based approach. Additionally, some of the considerations are subjective, lack clarity, and also are not appropriate to be assessed at the pre-contractual phase, in particular the requirement to: • "assess the CSP's ability to provide the information required for these checks" lacks clarity; • "ensure that the CSP has itself properly implemented the relevant checks" lacks clarity and should be reframed as "assess that.."; • consider "the risk of a considerable fall in quality", • consider "the risk of a significant increase in price"	The ECB is of the view that the measures set out in this paragraph are needed in order to assess the relevant risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	No
87	Risk management	AFME Section states, "perform thorough analysis of control processes that will be established"— it is unclear if this is referring to controls that are to be established by the FI or CSP? If the latter, the concern is that fIs would be dictating to CSPs what their controls should be.	From a regulatory standpoint, the supervised entity must ensure that risk management processes and controls in line with their ICT risk framework are in place. This may include the supervised entities collaborating with the CSP.	No
88	Risk management	AFME It is unclear if financial service firms are being asked to audit the cloud providers individually. Would there be the option to have industry-wide joint pooled audits of CSPs? If this is an option, it would be beneficial to understand roles and responsibilities as well as ownership of action items.	The possibility of a pooled audit is addressed in paragraph 2.5.	No
89	Risk management	AFME It should be added that institutions should perform analysis of the control processes""on the basis of the data flows provide"".	The ECB is of the view that the unavailability of the information needed to	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		Proposed new wording: perform thorough analysis of the control processes that will be established on the basis of the dataflows provided.	exercise control over their outsourcing is not a valid excuse for failing to perform such controls.	
90	Governance processes	AFME There seems to be a broadening of the DORA strategy on ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to risk as stated in DORA.	The ECB finds advisable that the decision to outsource to a CSP follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing arrangement.	No
150	Risk management	ECIIA The sentence Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and control"" is unclear.	The ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the entity following internal governance procedures. For this reason, this is indicated as a good practice in the Guide.	No
418	Business continuity	Dutch Banking Federation (DBF) To avoid compromising the security of network and information systems, the ECB considers that backups of critical or important systems should not be stored in the cloud hosting the relevant services. It is unclear whether this can be applied when the backup is located in another region. It is also unclear whether it is acceptable for the backup to be immutable at another CSP. Can you clarify whether you want all banks to maintain separate Solid State Drivers (SSDs) and/or Tape Robot to back up all Cloud data. We need more guidance what this mean in practice, for example with SaaS solutions primary servers handle live data and backup servers are designed to create and store copies of data from primary servers.	The ECB finds advisable that the supervised entity implements a backup conservation strategy capable of withstanding the failure of a CSP. The text has been reworded to clarify this point.	Yes
152	Risk management	ECIIA The sentence "assess the CSP's ability to provide the information required for these checks;" should be modified as follow: "assess that the CSP has properly implemented relevant checks;"	Checking that the CSP has run the relevant checks following proper procedure must be enabled and ensured.	No
153	Data protection	ECIIA Since the environment provided to the credit institution can be hosted anywhere in the planet we recommend to add: • The possibility of a credit institution to select the geographical area to store data • The compliance of the CSP with the local regulations that may apply • The practices applied for continuous monitoring of the regulatory framework as well and periodic assessment	These are specifically addressed in the data location risk and in the physical risks to be considered.	No
154	Risk management	ECIIA It is unclear what the phrase "the risks of a multi-tenant environment" means in the context of a pre-outsourcing assessment	As widely observed within the industry, using a shared infrastructure carries the risk of producing a multi-tenant environment.	No
155	Governance processes	ECIIA There seems to be a broadening of the concept reported in DORA, which requires the definition of a strategy limited to ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to strategy on ICT third-party risk as stated in DORA. It also needs to be clear on who should approve the cloud	The ECB finds advisable that the decision to outsource to a CSP follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		strategy, e.g. Board. And how often.	arrangement.	
194	Responsibility model	Confédération Nationale du Crédit Mutuel It is not possible for the credit institution to be fully accountable if there is no regulatory requirements for cloud service provider	The ultimate accountability is set out in Article 28(1)(a) of DORA.	No
211	Risk management	ABI- Italian Banking Association The request about the level of diligence regarding risk management, processes, and controls seems more far reaching than regulation. The sentence “Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls.” Should be modified as follows: “Consequently, Institutions should assess that their CSPs have established equivalent risk management practices, processes and controls.”. Clarification would be useful on what “equivalent” means in practice.	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
212	Risk management	ABI- Italian Banking Association The sentence “ensure the CSP has properly implemented relevant checks,” should be modified as follow: “assess that the CSP has properly implemented relevant checks,”	Checking that the CSP has run the relevant checks following proper procedure must be enabled and ensured..	No
213	Risk management	ABI- Italian Banking Association The reference to the risks of a multi-tenant environment is not clear. Cloud Services are multi-tenant by design.	Cloud services are indeed multi-tenant by design, although multi-tenancy carries specific risks that must be assessed and addressed.	No
214	Governance processes	ABI- Italian Banking Association There seems to be a broadening of the concept reported in DORA, which requires the definition of a strategy limited to ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to strategy on ICT third-party risk as stated in DORA	The ECB finds advisable that the decision to outsource to a CSP d follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing.	No
261	Risk management	Banking and Payment Federation Ireland (BPFI) The ECB includes a requirement to for institutions to “ensure that the CSP has itself properly implemented the relevant checks”, however it does not clearly establish what is means by “relevant checks”. It would be helpful for the ECB to more clearly explain the scope and nature of the checks that CSPs should be expected to perform.	From a regulatory standpoint, the supervised entity must ensure that risk management processes and controls in line with their ICT risk framework are in place. This may include the supervised entities collaborating with the CSP.	No
262	Risk management	Banking and Payment Federation Ireland (BPFI) The risk-considerations are unnecessarily prescriptive, expands DORA's requirements without reflecting the risk-based approach taken in DORA and the EBA guidelines with respect to ex-ante risk assessments. The Guide should expressly state that financial entities should, on a risk-based approach, identify and assess all relevant risks …etc. Additionally, it would not be feasible to assess some of the risk considerations at the pre-contractual stage, while we would argue that the risk considerations described therein lack clarity or could be considered subjective – including: • assess the CSP's ability to provide the information required for these checks; - lacks clarity • ensure that the CSP has itself properly implemented the relevant checks; - lacks clarity • the risk of a considerable fall in quality; - subjective and not feasible at the pre-contractual stage. This risk is managed through contractual provisions and the ongoing monitoring process addressing service level quality and performance. • the risk of a significant increase in price; - not feasible at the pre-contractual stage. This risk is managed through contractual provisions.	The ECB is of the view that the measures set out in this paragraph are necessary to assess the relevant risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	No
420	Business continuity	Dutch Banking Federation (DBF) The requirement that back-ups of CIFs should not be stored in the cloud, goes beyond the EBA/DORA existing requirements and suggests a disconnect from technical reality. Recent	The ECB finds advisable that the supervised entity implements a backup conservation strategy	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		experiences (for example with Unisuper) has demonstrated that back-up from within the same cloud service is at times critical for recovery. Organizations may struggle to segregate hosting and service backups due to specific databases used by the cloud provider. In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the BC through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	capable of withstanding the failure of a CSP. The text has been reworded to clarify this point.	
282	Risk management	European Cloud User Coalition (ECUC) There is a lack of clarity over how far down the supply chain the requirements should apply. It should be limited to direct cloud services, with which the FI has a contractual relationship.	The ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the institution following internal governance procedures.	Yes
283	Risk management	European Cloud User Coalition (ECUC) The only way that an FI can enforce a complete answer to any of suggested requirements in Pre-outsourcing analysis is via a contract, yet this provision is aimed at the pre-contractual phase. Could you please clarify the expectation?	The ECB is of the view that the measures set out in this paragraph are necessary to assess the relevant risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	No
296	Scope of the document	European Cloud User Coalition (ECUC) This governance /responsibility is not new and already part of existing and applicable EU regulatory (DORA, EBA). Advise to delete	As stated in Section 1.1 of the document: “The aim of the ECB Guide is to provide clarity on the ECB’s expectations and to promote good practices with regard to the related requirements set out in DORA, thereby fostering supervisory consistency and helping to ensure a level playing field by increasing transparency."	No
297	Risk management	European Cloud User Coalition (ECUC) Whilst it is referred to clause 28(4) DORA, various actions are listed for the FE's to perform, partly based on 'good practice', but is not clear where those actions originate from exactly. Can you please elaborate?	The good practices have been gathered from observations of the prevailing situation.	No
298	Pre-outsourcing analysis	European Cloud User Coalition (ECUC) "Assess whether the institution has the expertise and human resources required to implement and perform these checks;" This is very hard/impossible to check. Please verify how to do that.	The assessment as to the human resources needed to run the checks should be part of the pre-outsourcing analysis.	No
309	Risk management	European Cloud User Coalition (ECUC) "Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls." This is a broad and unspecific requirement. Please clarify how "equivalence" can be sufficiently achieved. While the intention is understood it will be inefficient and potentially ineffective If this is to be ensured by each institution individually.	The ECB finds advisable that supervised entities determine “equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
326	Risk	European Banking Federation	The ECB finds advisable that supervised entities	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	management	"Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls." The request about the level of diligence regarding risk management, processes, and controls seems more far-reaching than regulation. The sentence should be modified as follows: "Consequently, institutions should assess that their CSPs have established equivalently effective risk management practices, processes and controls." In addition, clarification would be useful on what "equivalent" means in practice.	determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the institution following internal governance procedures.	
327	Risk management	European Banking Federation The sentence "ensure the CSP has itself properly implemented relevant checks", should be modified to: "assess that the CSP has itself properly implemented relevant checks".	Checking that the CSP has run the relevant checks following proper procedure must be enabled and ensured..	No
328	Risk management	European Banking Federation • assess the CSP's ability to provide the information required for these checks; - lacks clarity • ensure that the CSP has itself properly implemented the relevant checks; - lacks clarity • the risk of a considerable fall in quality; - subjective and not feasible at the pre-contractual stage. This risk is managed through contractual provisions and the ongoing monitoring process addressing service level quality and performance. • (or) the risk of a significant increase in price; - not feasible at the pre-contractual stage. This risk is managed through contractual provisions.	The ECB is of the view that the measures set out in this paragraph are necessary to assess the relevant risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	No
422	Business continuity	Dutch Banking Federation (DBF) We suggest deleting the following phrase because it is overly limiting, especially when it comes to the use of SaaS Solutions: "The institution must maintain the ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers". It should be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. Please clarify that backups can be stored with the same service provider, as long as the provider has redundancy in place to ensure that backup data or critical systems are not stored in the same cloud.	The ECB finds advisable that the institution should implement a backup conservation strategy capable of withstanding the failure of a CSP. The text has been be reworded to clarify this point.	Yes
330	Risk management	European Banking Federation The reference to the risks of a multi-tenant environment is not clear. Cloud Services are multi-tenant by design.	Cloud services are indeed multi-tenant by design, although this multi-tenancy carries specific risks that must be assessed and addressed.	No
331	Governance processes	European Banking Federation There seems to be a broadening of the concept reported in DORA, which requires the definition of a strategy limited to ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to strategy on ICT third-party risk as stated in DORA	The ECB finds advisable that the decision to outsource to CSPs follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing.	No
404	Applicability of the measures	Dutch Banking Federation (DBF) We would like to get the confirmation that the assumption is correct that the word use 'should' and 'ensure' imply that there is not strict obligation to comply, but merely imply a non-binding suggestion. Please clarify the binding status of the various requirements as laid down in the Guide; on the one hand, it is stated that the	The ECB believes that these terms should be treated as a suggestion that supervised entities are invited to follow unless they decide not to after duly considering the matter based on a risk-	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		Guide "does not establish legally binding requirements", but on the other hand, it appears on several occasions that financial institutions are obliged to comply with the requirements by using the words "institutions should", see, for example, 2. 1.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.2., 2.3.2., 2.3.4.1., 2.3.4.2., 2.4.1., 2.4.2., 2.4.3., 2.5., 2.5.1., 2.5.2., 2.5.3. and also the use of the word "ensure" in the last bullet in 2.2.2.	based approach.	
517	Responsibility model	European Association of Public Banks The guidelines state: To protect its information, the institution should ensure that roles and responsibilities are clearly understood and defined internally and contractually agreed when procuring cloud computing services." Please clarify this paragraph. The first sentence of 2.1.1 already sets forth that the institution must have a clear governance framework. This sentence implies the governance framework is only needed to protect information. which seems to narrow. Also, the management body's responsibility is not limited to management of ICT risk, but remains responsible for outsourced activities under EBA outsourcing GL. Would suggest to replace the last to sentences of this paragraph by: "Nevertheless, the outsourcing contract must set out a clear and unambiguous allocation of roles and responsibilities."	The term "to protect its information" has been removed.	Yes
406	Risk management	Dutch Banking Federation (DBF) The guidelines state: "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. Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls". Please replace 'equivalent' by 'appropriate'. Most customers will outsource part of the services and keep part on premise. The term equivalent seems to imply that the service provider must apply the same risk management processes and controls as the institution. The service providers will work for a range of customers and they are unlikely to adjust their risk management processes and controls for each individual customer. The customer must verify whether the risk management processes and controls are appropriate, taking into account proportionality.	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
407	Scope of the document	Dutch Banking Federation (DBF) We advise to delete in the paragraph the governance responsibility. It is not new and already part of existing and applicable EU regulatory (DORA, EBA).	As stated in Section 1.1 of the document: “The aim of the ECB Guide is provide clarity on the ECB’s expectations and promote good practices with regard to the related requirements set out in DORA, thereby fostering supervisory consistency and helping to ensure a level playing field by increasing transparency."	No
408	Risk management	Dutch Banking Federation (DBF) Our recommendation is to rewrite the whole paragraph because of lack of feasibility and to ensure a more realistic approach. The current requirements exceed what can reasonably be contractually imposed on suppliers. Furthermore, the actual requirements are so high level that it is hard to understand the actual requirements. The only way that a financial entity can enforce any of these suggested requirements is via a contract, yet this provision is aimed at the pre-contractual phase. As an alternative framing, consider: "assess that the CSP has properly implemented relevant checks".	The ECB is of the view that the measures set out in this paragraph are necessary to assess the relevant risks in a pre-outsourcing analysis with a CSP. However, a risk-based approach may be used to adapt the depth of the measures to the scale of the foreseen migration.	No
409	Risk management	Dutch Banking Federation (DBF) We don't recognize the challenge of identifying an alternative provider. The real difficulty lies in the time and effort needed to migrate to an alternative provider. We recommend reconsidering the following text: "vendor lock - in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required".	While the challenge of migrating could be a function of the time factor, such time constitutes a risk that must be analysed from a risk management perspective.	No
410	Risk management	Dutch Banking Federation (DBF) Could you please clarify whether localisation risk is included within the category of Data Storage and Processing risks.	Data location is indeed included in the categories mentioned.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
411	Risk management	Dutch Banking Federation (DBF) Three risk scenarios/sentences may trigger an exit strategy. Both risks can be mitigated by switching providers, which aligns with the bullet point (vendor lock-in risk). Consider removing the following elements because of a lack of feasibility: 1) "the risk of a considerable fall in in quality or a significant increase in price' The risk of significant price increases often occurs in consolidating markets, where buyers raise prices after takeovers to recoup costs upon contract renewal. 2) The risk of considerable fall in quality is hard to predict. 3) Physical risks and region-specific risks. We expect physical risk to be region-specific.	The ECB is of the view that these risks should be properly analysed and suitable action plans drawn up for such risk scenarios.	No
412	Risk management	Dutch Banking Federation (DBF) Regarding multi-tenant environments, it is unclear what additional risks are considered beyond unauthorized data access.	Performance considerations, capacity management or failure of the CSPs to maintain isolation are some examples of risks that could arise from a multi-tenant environment.	No
413	Risk management	Dutch Banking Federation (DBF) Although DORA refers to clause 28(4), the listed actions for financial entities to perform, partly based on 'good practice', but is not clear where those actions originate from exactly.	The good practices have been gathered from observations of the prevailing situation.	No
414	Pre-outsourcing analysis	Dutch Banking Federation (DBF) We need more guidance how we can verify the following: "Assess whether the institution has the expertise and human resources required to implement and perform these checks".	The assessment as to the human resources needed to run the checks should be part of the pre-outsourcing analysis.	No
415	Risk management	Dutch Banking Federation (DBF) The guidance does not make a differentiation between CSPs classified as 'critical' or not critical under DORA.	The ECB believes this issue should be addressed from a risk-based approach.	No
416	Governance processes	Dutch Banking Federation (DBF) The guidance extends beyond DORA obligations, with a broadening focus on ICT third-party risk management. In the ECB Guide, there's a requirement for a strategy that encompasses not only risks but also business elements and an operating service model. It's crucial to clarify that the concept of an outsourcing strategy should remain limited to risk management, as stated in DORA.	The ECB finds advisable that the decision to outsource CSPs follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing.	No
417	Responsibility model	Dutch Banking Federation (DBF) The content is unclear because the requirements in the paragraph do not match 2.2.2. Does the whole section refer only to critical and important functions? There is ambiguity about the scope of all outsourced Cloud services. Does it address the entire chain including CoIF or not. Does ""in the cloud hosting the services" mean at the CSP level or some other separation level. Unclear it is then not suffice if you apply only CSP approach.	The ECB believes this issue should be addressed from a risk-based approach.	No
151	Risk management	ECIIA The sentence "• perform thorough analysis of the control processes that will be established" is unclear	The wording has been adapted to make the ECB's expectations on the matter clearer.	Yes
419	Scope of the document	Dutch Banking Federation (DBF) Can you advise us what is meant with 'cloud services', does it mean Iaas, Paas, Saas.	Please refer to the definition of the term provided in the Guide	No
281	Risk management	European Cloud User Coalition (ECUC) Without clarity that this relates to cloud services supporting CIFs, the guide will be lacking in proportionality and feasibility. Additionally, without clarification as to the type of cloud service subject to specific requirements, there are certain expectations which are not even practically possible for e.g. contractual obligations in pre-outsourcing analysis	Provision for a risk-based approach is clearly stated at the beginning of the paragraph.	No
421	Business continuity	Dutch Banking Federation (DBF) The proposed worst-case scenario of an entire CSP being unavailable and uncooperative is not plausible. The only way to mitigate this would be to develop, maintain and scale several parallel systems performing the same functions with	The ECB believes that such a scenario is indeed plausible.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		different architectures and infrastructure, which would mean doubling the cost and maintenance effort.		
329	Risk management	European Banking Federation A comprehensive risk analysis before a new cloud outsourcing arrangement can be resource-intensive and time-consuming requiring significant effort to identify and assess all relevant risks. Better allow for a scaled risk analysis approach based on the size and risk profile of the institution.	Provision for a risk-based approach is clearly stated at the beginning of the paragraph.	No
423	Business continuity	Dutch Banking Federation (DBF) The guidelines emphasize that Business Continuity Management (BCM) measures should address a worst-case scenario. Specifically, in this scenario, relevant cloud services provided by one or more CSPs are unavailable, and the institution must perform an exit under stress or without cooperation from the CSP(s). However, setting realistic Recovery Time Objectives (RTOs) for worst-case scenarios remains challenging, especially when migrating services to another cloud provider without assistance. The complexity and risks of synchronizing operations across multiple providers add further complications. DORA 12 (6) relates to RTO and RPO.	It is up to the supervised entity to establish the measures for addressing a worst-case scenario in accordance with its risk appetite.	No
477	Risk management	DIGITALEUROPE We agree that financial entities should establish appropriate governance frameworks aligned with DORA, however, 2.1.1 states that the use of cloud services makes 'a clear and unambiguous allocation of responsibilities more challenging'. Subsequently, it also introduces de-facto new requirements for CSPs to have 'equivalent risk management' practices, processes and controls, which are not included in DORA. We propose that in paragraph 3, the word 'EQUIVALENT' should be DELETED AND REPLACED with the word 'RELEVANT'.	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
478	Risk management	DIGITALEUROPE Pre-outsourcing analysis is an important aspect of a financial entity's move to the cloud. However, the Guide presupposes the presence of several unsubstantiated risks, including concentration risks, a decline in service quality, price increases, and risks of a multi-tenant environment are present risks rather than unsubstantiated assertions; and also introduces de-facto requirements not present in DORA. Additionally, the Guide fails to account for 'lock-ins' with respect to in-sourced software development and on-premise infrastructure maintained by financial entities. To align proposed sub-subsection 2.1.2 with DORA, the following AMENDMENTS should be incorporated. The sentences 'ASSESS THE CSP'S ABILITY TO PROVIDE THE INFORMATION REQUIRED FOR THESE CHECKS; and 'ENSURE THAT THE CSP HAS ITSELF PROPERLY IMPLEMENTED THE RELEVANT CHECKS' should be DELETED. Additionally, the ENTIRE PARAGRAPH after 'IT IS GOOD PRACTICE FOR A PRE-OUTSOURCING ANALYSIS TO CONSIDER THE FOLLOWING RISKS' should also be DELETED.	In the opinion of the ECB, based on lessons learned from its on-site inspections, these risks may be observed when performing a pre-outsourcing analysis.	No
516	Risk management	European Association of Public Banks The final sentence on ensuring that CSPs have equivalent risk management practices, could lead to misunderstanding that CSPs have to mirror the obligations on FEs. The sentence should be deleted given the repetition with the preceding one, or at least it should be clarified that this is about ensuring that "CSPs have established equivalently effective risk management practices." This also goes beyond EBA guidelines.	The ECB finds advisable that supervised entities determine “equivalent risk management” for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
12	Risk management	AWS 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 wording has been adapted accordingly to incorporate this suggestion.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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."		
518	Risk management	European Association of Public Banks The guidelines state: "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. Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls". Please replace 'equivalent' by 'appropriate'. Most customers will outsource part of the services and keep part on premise. The term equivalent seems to imply that the service provider must apply the same risk management processes and controls as the institution. The service providers will work for a range of customers and they are unlikely to adjust their risk management processes and controls for each individual customer. The customer must verify whether the risk management processes and controls are appropriate, taking into account proportionality.	The ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regards to their own risk management practices and that this equivalence is validated by the supervised entity following internal governance procedures.	No
519	Risk management	European Association of Public Banks "Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls."	The ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
520	Risk management	European Association of Public Banks Under Art. 28 (4) DORA, institutions are required to conduct risk analysis...prior to entering into a new outsourcing arrangement with a CSP. In order to adequately identify . the institutions should: We suggest to replace "institutions should" by "best practice shows..."	The ECB is of the view that it is the responsibility of the supervised entities, as per Article 28(4) of DORA, to conduct a risk analysis. In the ECB's opinion, in order to identify the relevant risks the supervised entity should perform at least the analysis suggested.	No
521	Exit strategy	European Association of Public Banks Art. 2.1.2. mentions „vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required" as good practice to consider risk. We suggest to add "if required and possible" given the strong contractual ties.	The ECB is of the view that supervised entities should maintain, where required by Article 28 of DORA, exit strategies that are practicable in all circumstances.	No
522	Risk management	European Association of Public Banks It is unclear why the ECB has said some considerations should be required and others are good practice. Is the expectation in practice going to differ?	The ECB believes that the term "good practice" should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	No
523	Risk	European Association of Public Banks	The ECB is of the view that	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	management	It should be added that institutions should perform analysis of the control processes "on the basis of the data flows provided".	the unavailability of the information needed to exercise control over their outsourcing is not a valid excuse for failing to perform such controls.	
524	Risk management	European Association of Public Banks The consideration of "physical risks and region-specific risks (e.g. political stability risks)" and "the risk of a considerable fall in in quality or a significant increase in price (both of which are common scenarios in a highly concentrated market)" go beyond the existing EBA requirements or DORA. Additionally, the risk of a considerable fall in quality is highly subjective and should be deleted. Both references should be deleted	While the ECB is of the view that DORA does not exhaustively enumerate the risks scenario to consider, the ECB recommends considering such risks as a matter of good practice only.	No
525	Risk management	European Association of Public Banks DORA is not limited to outsourcing -> definition of outsourcing in this document is confusing.	While DORA is not limited to outsourcing, the document addresses cloud outsourcing.	No
526	Risk management	European Association of Public Banks The guidelines state "vendor lock - in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required;" typically, before entering into an outsourcing contract an organization will perform an RFP involving multiple potential suppliers. We do not recognize the challenge of identifying an alternative provider. The challenge is the time and effort required to migrate to an alternative provider.	While the challenge of migrating could be a function of the time factor, such time constitutes a risk that must be analysed from a risk management perspective .	No
527	Risk management	European Association of Public Banks Data Storage and processing risks: Does this also include data localisation risks, i.e. risks of transferring data to a country and impediments in transferring data out of that country?	Data location is indeed included in the categories mentioned.	No
528	Risk management	European Association of Public Banks physical: We would expect that physical risks are also region specific?	They are indeed.	No
529	Risk management	European Association of Public Banks Increase in price: The risk of a significant increase in price occurs in practice a consolidating market where after a takeover the buyer increases the price to earn back the purchase price upon renewal of the contract. Also a risk of considerable fall in quality is hard to predict. Both circumstances may form a trigger in an exit strategy. Isn't this already covered by the first bullet, the vendor lock in risk? Both risks can be mitigated by migrating to a different provider.	Although related, these are seen as two distinct classes of risks having different origins.	No
530	Risk management	European Association of Public Banks Multi-tenant environment risk: What specific risks are meant, on top of unauthorized access to data?	Performance considerations, capacity management or failure of the CSPs to maintain isolation are some examples of risks that could arise from a multi-tenant environment.	No
531	Governance processes	European Association of Public Banks There seems to be a broadening of the DORA strategy on ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to risk as stated in DORA.	The ECB finds advisable that the decision to outsource to CSPs follow the decision-making processes of the supervised entity, with the management body's involvement to be commensurate to the scale of the outsourcing.	No
600	Risk management	Bitkom 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 ECB finds advisable that supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
601	Risk management	Bitkom 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”).	Under Article 28(4) of DORA, supervised entities are required to conduct a risk analysis prior to entering into a new outsourcing agreement. The aim of this guidance is not to lay down legally binding requirements. The recommendations are focused on identifying and assessing possible risks. It is not asserted that the risks will materialise in every outsourcing arrangement with CSPs, rather that they need to be considered and assessed. The ECB also believes that CSPs form a concentrated market.	No
602	Risk management	Bitkom 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.	There is a risk that the failure of a CSP could prevent a supervised entity from accessing its data. This risk needs to be assessed and managed as part of the contract between the supervised entity and the CSP concerned.	No
603	Pre-outsourcing analysis	Bitkom 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.	Under Article 28(4) of DORA, supervised entities are required to conduct a risk analysis prior to entering into a new outsourcing agreement. The aim of this guidance is not to lay down legally binding requirements. The recommendations are focused on identifying and assessing possible risks. It is not asserted that the risks will materialise in every outsourcing arrangement with CSPs, rather that they need to be considered and assessed. The ECB also believes that CSPs form a concentrated market.	No
604	Risk management	Bitkom 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	In the opinion of the ECB, based on lessons learned from its on-site inspections, these risks may be observed when performing a pre-outsourcing analysis.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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."		
605	Pre-outsourcing analysis	Bitkom 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.	The Guide suggests integrating the CSP outsourcing strategy into the supervised entity's general outsourcing strategy.	No
606	Risk management	Bitkom 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 wording has been adapted accordingly to incorporate this suggestion.	Yes
657	Pre-outsourcing analysis	Futures Industry Association (FIA) The risk considerations are unnecessarily prescriptive and expand existing due diligence practices and requirements. Additionally, the Guide does not adequately apply a risk based approach (only references CIFs in reference to consideration of sub-outsourcing risk). DORA and the EBA GLs apply proportionality to their respective requirements surrounding ex ante risk assessments. The potential risks associated with a "considerable fall in quality" would be managed through performance expectations in contractual arrangements / in SLAs for critical engagements, and through ongoing monitoring of the service provider's performance. It would be difficult to assess such risks at the onboarding stage.	The prescription set out in this paragraph is that just a pre-outsourcing risk analysis should be standard practice. This way, a lack of quality could indeed be addressed by monitoring the contract, although this situation would need to be analysed as part of the pre-outsourcing risk management analysis.	No
670	Risk management	German Banking Industry Committee (GBIC) For the ECB, Article 28(1)(a) DORA means that institutions that choose to outsource must have the same controls, processes and risk management in place as institutions that choose to retain these services internally. While equivalent controls should be established in principle, for example, an appropriate level of detail should be applied when monitoring the external service provider. Particularly in the case of cloud outsourcing, the level of detail is naturally limited, including with regard to the infrastructure used (server level). Only controls such as access controls or monitoring of system activities should be established. External controls, which are assumed by the cloud service provider, would be physical security, availability of services, data backup and recovery, as well as compliance with data protection regulations, etc.	The ECB finds advisable supervised entities determine "equivalent risk management" for their outsourcing arrangements with CSPs based on their specific risk profiles with regard to their own risk management practices, and that this equivalence is validated by the supervised entity following internal governance procedures.	No
671	Risk management	German Banking Industry Committee (GBIC) "Under Art. 28 (4) DORA, institutions are required to conduct risk analysis...prior to entering into a new outsourcing arrangement with a CSP. In order to adequately identify ... the	The ECB is of the view that it is the responsibility of supervised entities to conduct a risk analysis, as	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		institutions should ..." We suggest to replace “institutions should” by “best practice shows ...”	per Article 28(4) of DORA. In the ECB’s opinion, in order to identify the relevant risks the supervised entity should perform at least the analysis suggested.	
672	Exit strategy	German Banking Industry Committee (GBIC) "vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required"	The ECB is of the view that supervised entities should maintain, where required by Article 28 of DORA, exit strategies that are practicable in all circumstances.	No

2.3 Table 3 – Comments on Section 2.2: Availability and resilience of cloud services

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
2	BCM vs exit strategies	Deutsche Börse Group Deutsche Börse Group suggests maintaining the approach laid out in 2.4.2 where business continuity management and exit management are treated separately. We are of the view that (partial) unavailability of relevant cloud services is a temporary scenario and not equal to an exit scenario which would terminate the business relationship with a CSP.	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
3	Exit without cooperation	Deutsche Börse Group Deutsche Börse Group would like to ask for a clarification in terms of whether and "exit without cooperation from the CSP" is relating to a scenario where we observe unwillingness of a CSP to fulfil contractual obligations.	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
4	BCM vs exit strategies	Deutsche Börse Group Deutsche Börse Group suggests maintaining the approach laid out in 2.4.2 where business continuity management and exit management are treated separately. We are of the view that (partial) unavailability of relevant cloud services is a temporary scenario and not equal to an exit scenario which would terminate the business relationship with a CSP.	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
5	Back on premises	Deutsche Börse Group Deutsche Börse Group is of the view that a strict rule to have a mandatory "back on-premise" ability for each application as part of business continuity or disaster recovery processes is disproportionate and will essentially stop all cloud adoption, as it would require to have all on-premise infrastructure in place at all times. We are of the view that such approach would also stop all investments in building back-up capabilities with a 2nd or 3rd CSP, decreasing operational resilience and increasing costs.	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes
13	Backup not in the same cloud; Exit without cooperation	AWS 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	The final version of the Guide will no longer advise against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
14	Architectures for resilience	AWS 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.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not uniformly used by CSPs.	Yes
15	DR testing	AWS 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-	The final version of the Guide contains the expectation that supervised entities assess the CSP’s disaster recovery plan and	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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	tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		THE INSTITUTION'S STRATEGY AND IN LINE WITH ITS BUSINESS CONTINUITY POLICY AND REQUIREMENTS".		
16	Concentration risk; Provider lock-in	AWS 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	Section 2.2.4 has been revised so as to make clear that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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)."		
29	DORA vs NIS 2	Nordea Abp The guide contains several references to the NIS2 Directive, even though it has been confirmed that DORA is lex specialis to NIS2. Hence, there are a number of references in the Guide which can lead to misinterpretation. Consider removing references to NIS2.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
30	Concentration risk	Nordea Abp DORA requirements which already raises a number of new parameters for tracking concentration risk (Recitals 66, 67, including the definition of ICT concentration risk in Article 3, 29 which is missing in the Guide, article 28 and 29 of DORA main regulation and Recital 6 of the ITS of the Register of Information, there are also references to concentration risk in several other RTS:s). Additionally, a risk assessment is already carried out for the purpose of contracting ICT services by the TPPs and another one when the TPP shoud consider changing a subcontractor which supports critical or important functions. Hence, separate risk assessment done only for CSPs, would make the assessment processes more complicated and add burden to the banks' risk management Practises. We propose to amend the section and refer to banks applying a risk-based approach and DORA.	Section 2.2.4 has been revised to ensure its consistency with Article 29 of DORA and moved to Section 2.1.2 – Box 1.	Yes
39	Back on premises	Association of German Public Banks It indicates that institutions must have the capacity to bring the data and backups on-premises. The expectation "The institution must maintain the ability to bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. We therefore suggest deleting the phrase "The institution must maintain the ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers"	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes
40	Back on premises;Portability;Backup not in the same cloud	Association of German Public Banks The interpretations regarding the ability to bring data back on-premises and regarding portability go far beyond the DORA and should therefore be deleted or formulated to "may". Separate storage locations for backups can be costly and operationally challenging, particularly for smaller institutions.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			insourcing the data and applications. The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	
41	DR testing	Association of German Public Banks Spot checks on all services as part of disaster recovery tests would not be possible. Should be applied through a materiality lens. Similarly, not relying on disaster recovery certifications should be limited to IaaS.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
42	Concentration risk	Association of German Public Banks The Guide should expressly state that financial entities (FEs) concentration risk should be assessed on a risk-based approach. Additionally, the concentration risk indicators are overly expansive, incorporating numerous factors that lack sufficient relevance to an accurate assessment of concentration risk and imposing both an unrealistic and unmanageable burden on risk management practices. This accounts in particular for the assessment of the scalability of the cloud which allows it to be gradually extended to encompass new functions.	The risk assessment carried out when entering into a contractual arrangement with a CSP should also look at concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. Section 2.2.4 has been revised in order to better clarify that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
58	DORA vs NIS 2	ABBL - The Luxembourg Bankers' Association The Guides consistently references the NIS2 Directive for interpretation even if there are equivalent requirements included in DORA. As DORA is lex specialis to NIS2, these references should be removed.	All references to the NIS 2 Directive have been removed from the final version of the Guide.	Yes
61	Backup not in the same cloud	ABBL - The Luxembourg Bankers' Association The suggestion that back-ups of CIFs should not be stored in the cloud service provider that hosts the services will not always be practically possible or in the best interests of the institution and its resilience. There are several technical difficulties with storing back-up data in a different CSP: • For any service which uses or is native to the CSP, the data format will not allow for use in another CSP or another equivalent service without conversion. For example, data stored in one CSP using their storage solution would not be usable within the storage solution in another CSP. If the original CSPs storage solution is proprietary then	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		conversion of the data would be required before it could be used. This can be difficult and can take significant time making its use in a recovery or resilience scenario limited. • It is also possible that a native tool is not designed for the data to be extracted. In these cases, a requirement to have backup in another CSP would prevent the use of certain CSP-native tools. • In the scenario of a complete outage, data stored in another CSP would take significant time to get transferred back to the original CSP. The amount of data is increasing exponentially. When data reaches the scale of petabytes, digital means of transfer begin to become impractical and it becomes necessary to explore the physical transport of data between premises. It is also the case that data alone will have limited resilience benefit. Even in an ideal scenario in which the firm had perfect data back-up in an alternative CSP, it would take weeks to build the infrastructure and applications needed to provide the service from that CSP and test their functionality. This means that the financial entity would almost certainly breach its maximum tolerable level of disruption. In a severe scenario, any market-wide impacts resulting from an outage of that financial entity or its services, would not be prevented by maintaining back-up data in another CSP. To achieve the resilience outcome that the ECB seem to be targeting, it would be necessary to maintain live-live functionality across multiple CSPs. This also faces technical limitations, most notably the near impossibility of maintaining data synchronisation across different infrastructures and platforms operating in different geographic locations. It would also preclude the use of cloud-native tooling for which redundancy in a different CSP would not be possible owing to the proprietary nature of the service (this could include most SaaS offerings). Finally, even if the technical challenges could be overcome, the business implications would be substantial. The de-facto ban on using cloud-native tooling would significantly undermine the business case for using cloud. It would also be only the best resourced firms which could afford to maintain this setup. An alternative approach being considered by many firms is logical segregation of backups within the same cloud provider. Recent incidents such as the UniSuper outage (https://cloud.google.com/blog/products/infrastructure/details-of-google-cloud-gcve-incident) demonstrate that, even under the most extreme scenarios, provided the firm has a well-architected recovery capability, logically segregated data can be vital to recovery. We would propose that instead of prohibiting the use of the same CSP for backups, the ECB should instead require institutions to assess the resilience of their backups based on the risk associated with the services provided, including for instance the storage of back-ups in different cloud regions, use of active / active backups, multi-cloud strategies, secondary back-ups outside of the primary cloud etc. This should be in line with the measures considered within section 2.2.2 Proportionate requirements for critical functions.	restriction on backup and recovery procedures being limited to the storage of data has been removed.	

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
62	Back on premises	ABBL - The Luxembourg Bankers' Association The expectation that "The institution must maintain the ability to bring data and applications back on-premises" has caused significant concern among the industry given the technical difficulties with achieving this. For many cloud uses, such as cloud-native tools, bringing the data and applications back on premise would require the financial entity to maintain comparable capabilities as the CSP. Given the tools used may be proprietary, this often not be possible. To use the example from above, data stored using a CSPs storage tool would not be compatible with a storage tool from another CSP or what the financial entity maintains on premise. Moving the data back on presmise in this example would require conversation and significant testing rendering the strategy ineffective for limiting disruption to within agreed tolerance levels. From a resource perspective, maintaining these cloud computing capabilities would not be feasible excpet for perhaps the very largest financial entities. Even then, it would be cost prohibitive for Fis to use cloud under this requirement. This requirement would represent a de-facto ban on the majority of cloud-native tools and would likely significant impact EU financial entities ability to use SaaS offerings. The strategy suggested by the ECB of containerisation and virtual machine based-applications, while technically possible, would equate to treating CSPs as data centre providers. This is likely far below the strategies of most EU FIs and would effectively erode the value added of cloud computing which has led to such wide-spread adoption of the technology. Operating under these limits would see EU financial entities face a significant competitive disadvantage to firms in other markets who will be able to improve the security, resilience and product offerings in a way that EU financial entities will not be able to access. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. We therefore suggest deleting the phrase "The institution must maintain the ability to bring data and applications back on-premises"	In the final version of the Guide, the ability to transfer data and applications to other service providers will be provided as an alternative to insourcing the data and applications.	Yes
63	Deficiencies in DR	ABBL - The Luxembourg Bankers' Association Whilst it is reasonable to expect the remediation of deficiencies identified during testing, it is unclear how this would be addressed by renegotiating the contract with the CSP. Gaps identified during BCP testing should be addressed in the BCP plan, and the control environment of the CSP.	The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
64	Concentration risk	ABBL - The Luxembourg Bankers' Association The Guide should expressly state that financial entities concentration risk should be assessed on a risk-based approach. DORA does not refer to “data residency” and the inclusion of such term in the Guide could lead to confusion among financial entities. Hence, the second paragraph of 2.2.4 should be amended to indicate: “…alongside aspects of data (to delete the word "residency") location.”	The risk assessment carried out when entering into a contractual arrangement with a CSP should also address concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. In the final version of the Guide, “data residency” has been replaced with “location of data”. Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	Yes
91	Backup not in the same cloud	AFME The suggestion that back-ups of CIFs should not be stored in the cloud service provider that hosts the services will not always be practically possible or in the best interests of the institution and its resilience. There are several technical difficulties with storing back-up data in a different CSP: • For any service which uses or is native to the CSP, the data format will not allow for use in another CSP or another equivalent service without conversion. For example, data	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		stored in one CSP using their storage solution would not be usable within the storage solution in another CSP. If the original CSPs storage solution is proprietary then conversion of the data would be required before it could be used. This can be difficult and take significant time making its use in a recovery or resilience scenario limited. • It is also possible that a native tool is not designed for the data to be extracted. In these cases, a requirement to have backup in another CSP would prevent the use of certain CSP-native tools. • In the scenario of a complete outage data stored in another CSP would take significant time to transfer back to the original CSP. The amount of data is increasing exponentially. When data reaches the scale of petabytes, digital means of transfer begin to become impractical and it becomes necessary to explore the physical transport of data between premises. It is also the case that data alone will have limited resilience benefit. Even in an ideal scenario in which the firm had perfect data back-up in an alternative CSP, it would take weeks to build the infrastructure and applications needed to provide the service from that CSP and test their functionality. This means that the financial entity would almost certainly breach its maximum tolerable level of disruption. In a severe scenario, any market-wide impacts resulting from an outage of that financial entity or its services, would not be prevented by maintaining back-up data in another CSP. To achieve the resilience outcome that the ECB seem to be targeting, it would be necessary to maintain live-live functionality across multiple CSPs. This also faces technical limitations, most notably the near impossibility of maintaining data synchronisation across different infrastructures and platforms operating in different geographic locations. It would also preclude the use of cloud-native tooling for which redundancy in a different CSP would not be possible owing to the proprietary nature of the service (this could include most SaaS offerings). Finally, even if the technical challenges could be overcome, the business implications would be substantial. The de-facto ban on using cloud-native tooling would significantly undermine the business case for using cloud. It would also be only the best resourced firms which could afford to maintain this setup. An alternative approach being considered by many firms is logical segregation of backups within the same cloud provider. Recent incidents such as the UniSuper outage demonstrate that, even under the most extreme scenarios, provided the firm has a well-architected recovery capability, logically segregated data can be vital to recovery. We would propose that instead of prohibiting the use of the same CSP for backups, the ECB should instead require institutions to assess the resilience of their backups based on the risk associated with the services provided, including for instance the storage of back-ups in different cloud regions, use of active / active backups, multi-cloud strategies, secondary back-ups outside of the primary cloud etc. This should be in line with the measures considered within section 2.2.2 Proportionate requirements for critical functions.	should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
92	Scope of backup	AFME The ECB interprets Article 12 of DORA to require institutions to include back-ups for all CSPs. However, DORA Article 12 requires financial entities to develop and document policies and procedures specifying the scope of data that is subject to backup, and the minimum frequency of the backup, based on the criticality of information or confidentiality level of the data. The ECB's interpretation does not account for the legislative provision that this should be based on the criticality and confidentiality of the data stored. We would propose that the ECB amend this provision to explicitly recognise that institutions should determine the backup requirements based on an assessment of these factors.	The final version of the Guide states that the scope of the data subject to backup and the minimum frequency of the backup should be based on the criticality of the information or the confidentiality level of the data.	Yes
93	Definition of critical or important function	AFME The ECB does not define a 'critical or important system' – this could be interpreted to be any system which in any way supports a critical or important function, which would not consider materiality. The ESAs' technical standards on the use of ICT services to support critical or important functions includes a risk assessment of the service provided by a TPP (which would include CSPs) to inform the degree of application of the requirements, including the potential impact of disruptions on the continuity and availability of the financial entity's activities. We would propose that the ECB's requirements for the use of CSPs to support critical or important functions be based on an assessment of the risks associated with those services, rather than be applied across all CSP services regardless of the risks associated with them.	All references to critical or important systems have been removed. The Guide adheres to relevant regulations. When specific prescriptions apply only to critical or important functions, these have been addressed accordingly. The definition of "critical or important function" provided in Section 1.1has been modified to ensure its alignment with DORA.	Yes
94	Scope of backup	AFME There seems to be some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact technical feasibility or ability to be utilized in a resilience scenario). In particular: In the first part of the paragraph the focus is on data while in the following part the backup procedure involve also critical or important systems.	In the final version of the Guide, the restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
95	Exit without cooperation	AFME The proposed worst case scenario of an entire CSP being not available and not cooperative is lacking in plausibility. Ultimately, this would require having it duplicated in a data centre. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort. It also does not consider the resilience measures in place within individual CSPs which would prevent such a failure from happening in the first place, or allow rapid recovery from such a failure. In the absence of a clear rationale of how such a failure could occur without mitigation by CSPs' own resilience measure, presumption of this degree of failure does not appear in line with the 'severe but plausible' basis of most stress scenarios. Furthermore, a CSP being unavailable would apply to all commercial and individual users of the CSP and would constitute a significant economic and political event with severe financial stability implications for the global economy. We instead believe that BCM measures should address severe but plausible scenarios impacting the cloud services which they leverage, which would consider the mitigations which can be deployed by the CSPs themselves in plausible scenarios.	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
96	Back on premises	AFME The expectation that "The institution must maintain the ability to bring data and applications back on-premises" has caused significant concern among the industry given the technical difficulties with achieving this. For many cloud uses, such as cloud-native tools, bringing the data and applications back on premise would require the financial entity to maintain comparable capabilities to the CSP. Given the tools used may be proprietary, this often will not be possible. To use the example from above, data stored using a CSPs storage tool would not be compatible with a storage tool from another CSP or what the financial entity maintains on premise. Moving the data back on premise in this example would require conversion and significant testing rendering the strategy ineffective for limiting disruption to within agreed tolerance	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		levels. From a resource perspective, maintaining these compute capabilities would not be feasible save for perhaps the very largest financial entities. Even then, it would be cost prohibitive to use cloud under this requirement. This requirement would represent a de-facto ban on the majority of cloud-native tools and would likely significant impact EU financial entities ability to use SaaS offerings. The strategy suggested by the ECB of containerisation and virtual machine based-applications, while technically possible, would equate to treating CSPs as data centre providers. This is likely far below the strategies of most EU financial entities and would effectively erode the value add of cloud computing which has led to such wide-spread adoption of the technology. Operating under these limits would see EU financial entities face a significant competitive disadvantage to firms in other markets who will be able to improve the security, resilience and product offerings in a way that EU financial entities will not be able to access. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. We therefore suggest deleting the phrase "The institution must maintain the ability to bring data and applications back on-premises"		
97	Architectures for resilience	AFME Given the ESAs' development of technical standards covering Article 6, it seems unusual that the ECB would separately develop its own interpretations of Article 6(8) which go beyond the standards developed by the ESAs in their mandate under DORA, and which could be interpreted as the ECB seeking to take on a regulatory role rather than a supervisory role. Regarding the ECB's interpretation of Article 6(8) in particular, DORA requires (which is expanded upon in the ESAs' technical standards) that institutions develop an operational resilience strategy, and sets the components explaining how it will deliver against its operational resilience goals. It does not require institutions to consider specific resilience measures. Furthermore, the specification of specific resilience measures risks the guidance quickly becoming out of date. We would propose that the ECB amend section 2.2.2 to remove the reference to specific resilience measures. If not, applying these measures to SaaS and PaaS cloud services may be particularly difficult to the extent of unfeasibility or have negative impacts. Therefore, we would suggest that the focus of these measures should be on IaaS, where institutions have more control over the underlying infrastructure.	The final version of the Guide will make it clearer that the list of business continuity measures is provided as a good practice of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not uniformly used by CSPs.	Yes
98	Architectures for resilience	AFME Maintaining multiple CSPs increases operational and cybersecurity risk. Operationally, multi-cloud options require multi-lingual internal teams and a greater risk of complexity due to differing control places alongside on-premises infrastructure. Cybersecurity risk increases due to attack surfaces materially increasing, which adds further risks relating to oversight. These are all considerations that should be taken account of in any form of cloud adoption. It would also be prohibitively expensive. A multi-cloud live cloud adoption is the most costly form of adoption and would materially increase the operational budgets of ECB-firms to maintain, thus likely creating a highly uncompetitive market in the EU.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not uniformly used by CSPs.	Yes
99	Portability	AFME Recommend deleting: To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions	and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	
100	Scope of DR; Reference to regulation	AFME The ECB's interpretation of Article 28(8) go beyond the requirements envisioned in the primary legislation, as well as conflicting with the technical standards developed by the ESAs on the use of ICT services supporting Critical or Important functions. In particular, Article 10 of these technical standards states that, "the financial entity shall ensure that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements". Both the primary text and the technical standards seek to ensure that exit strategies address plausible scenarios and reasonable assumptions in relation to the services being leveraged. The ECB's expectation that institutions be able to remain fully operational in circumstances explicitly outside of the exit plans appears to go beyond these requirements. Furthermore, the ECB's specification of these requirements in relation to "Critical Functions", which they define by referring to the definition of "Critical or Important Functions" per the EBA's guidelines on outsourcing, which is not aligned to the definition of "Critical or Important Functions" under DORA does not appear in line with the scope of Article 28(8) in DORA, which is applied to ICT services supporting Critical or Important Functions (using the DORA definition).	Section 2.2.2 has been revised. In the final version of the Guide, the footnote providing a definition of critical functions has been removed. Reference to "fully operational" has been removed as well.	Yes
101	Definition of critical functions	AFME The guide in this chapter refers to the EBA guidelines in footnote 7 to define critical functions. We suggest to eliminate this reference to maintain consistency with the definitions provided in the table "Definitions of terms for the purposes of this Guide" on page 2.	In the final version of the Guide, the footnote providing a definition of critical functions has been removed. Definition of critical function has aligned with DORA definition.	Yes
102	DR testing	AFME Right to audit notice clauses (e.g. 30 days notice) may impact ability to conduct spot checks at short notice in order to assess CSP readiness. We suggest rewording the sentence "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." as follows: When conducting disaster recovery tests with the CSP, the institution should perform, whenever possible, spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event."	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
103	DR testing	AFME Spot checks on all cloud services as part of disaster recovery tests would not be possible. Without proportionality, this would constitute spot tests across all IaaS, PaaS and SaaS individual services that a financial entity utilises, which can be hundreds of services. Equally, DORA introduces a significantly expanded testing regime for financial institutions and their third parties, including threat-led penetration testing. The Guide gold-plates with the addition of 'spot checks' while not recognising that these forms of test will have to be agreed by the relevant CSP. Similarly, not relying on disaster recovery certifications should be limited to IaaS.	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
104	Deficiencies in DR	AFME The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. Whilst it is reasonable to expect the remediation of deficiencies identified during testing, it is unclear how this would be addressed by renegotiating the contract with the CSP. Gaps identified during BCP testing should be addressed in the BCP plan, and the control environment of the CSP. Additionally the non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation and the Guidance should recognise these practical difficulties. These difficulties will be exacerbated when applied to non-CSP third-party provider (TPP) reliant on cloud services provided by a CSP.	The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
105	DR testing	AFME With regard to the shared responsibility model, clarification is needed on whether the DRP is related to CSP infrastructure or to Institution's configurable services running on cloud environment.	Section 2.2.3 states that Article 11(6), paragraph two of DORA (which states that the testing plans of financial entities must include, among others, scenarios involving cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity) applies to situations where the supervised entity uses the CSP's ICT infrastructure. The title of 2.2.3 has been changed to clarify that the subsections refer to the CSP's disaster recovery strategy.	Yes
106	Concentration risk	AFME The concentration assessment provisions, which we undertstand to be at the entity level, fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical ICT Third Party Provider regime and other DORA Level 2 technical standards, some of which are still to be finalised. These should be leveraged, rather than expecting assessments on a regular basis by the firm. The preliminary assessment of ICT concentration risk obligated by Article 29 DORA is the key.	Section 2.2.4 has been revised to ensure its consistency with Article 29 of DORA and has been moved to Section 2.1.2 – Box 1.	Yes
130	Backup not in the same cloud	[XXX][American Chamber of Commerce to the European Union] Remove the prescriptive expectation in Article 2.2.1 about not storing back-ups in the cloud that hosts the primary system and instead focus on effective restoration and recovery as an outcome.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
131	Portability	American Chamber of Commerce to the European Union Remove the prescriptive expectation in Article 2.2.2. about minimising the impact of using a solution specific to an individual CSP and using virtual machine-based applications and/or containerised applications (which does not technically apply to all system architectures), and instead focus on effective migration as an outcome.	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes
137	Backup not in the same cloud	American Chamber of Commerce to the European Union Article 2.2.1 contains an expectation for institutions not to store back-ups of critical or important systems in the cloud that hosts the primary system. This is narrower than Article 12(3) of DORA, which says 'When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system.'	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
138	Back on premises	American Chamber of Commerce to the European Union Article 2.2.2 contains an expectation for institutions to 'bring data and applications back on premises'. This is narrower than Article 28(8) of DORA, which refers to both 'transfer[ing] them	In the final version of the Guide, the ability to transfer data and applications to other service providers is	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		to alternative providers or reincorporat[ing] them in-house'.	provided as an alternative to insourcing the data and applications. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	
139	DR testing	American Chamber of Commerce to the European Union Article 2.2.3 contains an expectation for institutions to directly tests their CSP's disaster recovery plans (including spot checks and tests on short notice). This goes beyond the requirement to test the financial entity's ICT response and recovery plans in Article 11(6) and creates undue risk for the CSP's other customers, which includes other financial entities.	In the final version of the Guide, supervised entities are expected to perform spot checks and/or tests at short notice when testing that the CSP's DRP has been removed. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
156	DR testing	ECIIA Current regulations strengthen the idea of having good business continuity plans and adequate testing plans. This forces entities to stress their test models on premise systems with data in provider's cloud. We welcome the idea to strengthen t that entities get involved in carrying out and obtaining the results of the tests carried out by cloud providers.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
157	BCM vs exit strategies	ECIIA This provision could implicitly introduce new requirements, while referring to the concept of a Holistic Perspective. Whenever the expectation is to consider both Business Continuity (Backup/Restore) and Exit Strategy elements in a unique framework, we foresee a potential risk in a dramatic increase in complexity, significantly limiting the architectural alternatives to be considered and further complicating the verification and control actions towards CSPs. There seems also to be in certain cases some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact). In particular: In the first part of the paragraph the focus is on data while in the following part the backup procedure involve also critical or important systems.	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
158	Backup not in the same cloud	ECIIA In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the BC through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
159	BCM vs exit strategies	ECIIA The paragraph collapses Business Continuity and Exit Strategy considerations and introduces the concept of an "exit under stress or an exit without the cooperation of the CSP(s)".	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		We believe this requirement is quite impossible to be respected, a recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort.	the ability to perform an exit under stress or without cooperation from the CSP.	
160	Architectures for resilience	ECIIA "multiple data centers" needs to be clarified what is deemed to be a data centre, and to what tiering (e.g. Tier IV, III etc..). AWS viewed Availability Zones (AZ) as Data Centres, but the US-East 1 outage incident details exposed information that suggested Azs are not on par with on-prem Bank data centre resilience capabilities.	In the final version of the Guide, the description of the business continuity patterns has been amended to avoid terms that have not been defined in the Guide and that are not commonly used among CSPs.	Yes
161	Architectures for resilience	ECIIA "A multi-region approach" makes an assumption that multi-region enhances security, however, it doesn't handle data privacy laws. This should include a statement to caveat where it doesn't breach laws etc..	Section 2.2 deals with business continuity, while data protection is addressed in Section 2.3.	No
162	Definition of critical functions	ECIIA The guide in this chapter refers to the EBA guidelines in footnote 7 to define critical functions. We suggest to eliminate this reference to maintain consistency with the definitions provided in the table "Definitions of terms for the purposes of this Guide" on page 2.	In the final version of the Guide, the footnote defining critical functions has been removed.	Yes
163	Reference to regulation	ECIIA "as defined in the institution's internal policies" Plus laws, regulatory rules and regulations in case internal policies have not been considered.	In the final version of the Guide, the reference to "internal policies" has been replaced with a reference to the "ICT business continuity plan".	Yes
164	Back on premises	ECIIA The expectation "The institution must maintain the ability to bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. We therefore suggest deleting the phrase "The institution must maintain the ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers"	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes
165	DR testing	ECIIA "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" We suggest to modify as follows: "with reference to IasS Cloud test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications"	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications.	Yes
166	DR testing	ECIIA We suggest to amend the sentence "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." as follows: "When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event"	In the final version of the Guide, supervised entities are expected to perform spot checks and/or tests at short notice when testing that the CSP's DRP has been removed. The Guide now includes as a good practice that , supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure,	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			full site loss, loss of a region and partial failures).	
167	Concentration risk	ECIIA It should be clarified by Authorities what would constitute a meaningful concentration of services in a specific location or in a specific function/service, or how much weight should be given to the assessed concentration risk. In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
168	Roles and responsibilities	ECIIA In the section "When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services " clarification needs to be made to establish clear responsibilities towards the three lines.	Responsibilities should be established, as for ICT risk management. Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	No
197	Backup not in the same cloud	BSI The statement in the second last paragraph of subsection 2.2.1 is not feasible for all kinds of cloud usage. It applies to mere lift-and-shift scenarios, i.e. where physical servers are moved to cloud but they do not apply to contemporary cloud usage where workload is redesigned for cloud usage. This redesign also affects internal processes of the supervised entity, e.g. for IT-operations. In short: A supervised entity shall assess to which extend it is possible to extract data (and where possible, this shall be tested as the guideline says). But for parts of own IT where there is no possibility of backing up (e.g. serverless applications like AWS Lambda or security functions like CloudTrail; other CSPs have also such services), the BCM strategy becomes much more complex and this shall be mentioned here. The supervised entity must be aware of those parts that cannot be just backed up and has to adopt a well-informed decision when moving to the cloud.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
198	Architectures for resilience	BSI Please change "Multiple datacentres in different geographical regions" to "Multiple datacentres or availability zones (that consists of different datacentres) in different geographical regions.	In the final version of the Guide, the description of the business continuity patterns has been amended to avoid terms that have not been defined in the Guide and that are not commonly used among CSPs.	Yes
199	Architectures for resilience	BSI Please add in a new bullet point the CAP theorem (https://en.wikipedia.org/wiki/CAP_theorem) in order to keep everybody aware that it is impossible (in a strict scientific and mathematical sense) to build a solution that is always consistent, available and partition tolerant at the same time. Hence strategic decisions and orders of supervising authorities should not demand what is impossible	Not relevant; the Guide does not require ICT systems to be always consistent, available and partition-tolerant at the same time.	No
200	Back on premises	BSI In the last bullet point before paragraph 2.2.3, everything after "would expect in an orderly transition under the exit plan." shall be deleted. The meant text describes a situation where an institution is just using some cloud in a lift-and-shift scenario. Moving to cloud is in most cases a transformation process. Infrastructure becomes code, duties fulfilled by servers may be done by serverless functions, AI services are used that are much to expensive to be build onprem, monitoring functions that are to expensive onprem may be used (and lead to more security) to mention just a few aspects. Demanding institutions to "retain the ability to bring data and applications back on-premises" is demanding them to not use the full power of cloud services. It also implies that staff must be retained in institutions to operate all IT back in on-prem infrastructure if needed in extreme scenarios which will cost a lot and lead to systematic disadvantages for old institutions with an on-prem IT in comparison to younger supervised institutions that already started with a cloudified IT. It is absolutely clear that the first part of the bullet point is of utmost importance and institutions shall be very aware of their dependencies and shall document those well-informed decisions. The clear risk that a CSP turns off the service abruptly is not a risk that can be fully mitigated within	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		supervised institutions. If this is done - like in the text that shall be deleted - this leads to large unwanted side-effects sketched above. One may also conclude that this risk is of such outstanding importance for EU society to survive that additional legislation is needed (e.g. for taking over the EU-parts of CSPs or other extreme measures).		
215	BCM vs exit strategies	ABI – Italian Banking Association This provision could implicitly introduce new requirements, while referring to the concept of a Holistic Perspective. Whenever the expectation is to consider both Business Continuity (Backup/Restore) and Exit Strategy elements in a unique framework, we foresee a potential risk in a dramatic increase in complexity, significantly limiting the architectural alternatives to be considered and further complicating the verification and control actions towards CSPs. There seems also to be in certain cases some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact). In particular: In the first part of the paragraph the focus is on data while in the following part the backup procedure involve also critical or important systems.	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
216	Backup not in the same cloud	ABI – Italian Banking Association The statement regarding institutions' response and recovery planning and Business Continuity Management seems to require the implementation of multi cloud environments. The criticality of such statement is even higher considering also exit strategies. The complexity of implementing exit strategies in a multi cloud configuration is not measurable, also considering vendor lock-in during exit strategy implementation. The result of the statement is: multi cloud environment or on-premises environment, there aren't alternative legit configurations	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
217	Backup not in the same cloud	ABI – Italian Banking Association The suggestion that back-ups of Critical or Important Functions should not be stored in the cloud which hosts the services will not always be practically possible or in the best interests of the institution and its resilience. In addition many initiatives that have been deployed in the cloud could be significantly impacted by this requirement The guide indicates that "back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned". In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the Business Continuity through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP). We would propose that instead of prohibiting the use of the same cloud for backups, the ECB should require institutions to assess the resilience of their backups based on the risk associated with the services provided, accordingly art. 12,(3) of DORA (e.g. "When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system").	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
218	BCM vs exit strategies	ABI – Italian Banking Association The last paragraph "For the purposes of Article 12(6) of DORA, the ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question." collapses Business Continuity and Exit Strategy considerations and introduces the concept of	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		an "exit under stress or an exit without the cooperation of the CSP(s)". This requirement appears quite impossible to be respected, since a recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort.		
219	Architectures for resilience	ABI – Italian Banking Association The statement regarding multi region and multi availability zone approach seems to be a requirement not present in the current regulation. We propose to delete the sentence in brackets "(A multi-region approach is even better, offering additional security relative to a set-up with multiple virtual zones in the same region.)" and the sentence "in different availability zones".	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	Yes
220	Portability	ABI – Italian Banking Association The statement regarding virtual machine-based applications and containerisation development seems to exclude SaaS solutions	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes
221	Architectures for resilience	ABI – Italian Banking Association With reference to the request "appropriate cloud resilience measures", confirmation is sought that this provision is applicable only with reference to IaaS Clouds	The supervised entity should consider all cloud services, not only IaaS, when assessing the resilience requirements for the cloud outsourcing services provided and the data managed and, following a risk-based approach, when deciding on the most appropriate cloud resilience measures.	No
222	Definition of critical functions	ABI – Italian Banking Association The Guide in this chapter refers to the EBA guidelines in footnote 7 to define critical functions. Deletion of this reference is suggested, to maintain consistency with the definitions provided in the table "Definitions of terms for the purposes of this Guide" on page 2.	In the final version of the Guide, the footnote defining critical functions has been removed.	Yes
223	Back on premises	ABI – Italian Banking Association The ECB consultation document as proposed makes the use of cloud solutions difficult or even impossible, making it not economically sustainable and/or not feasible. ECB wants banks to be "responsible" for the solutions they adopt, and this is correct in principle, but then the written policies require that banks have "instant" internal recovery capabilities of what is managed in the cloud or "switch" , always instant, on another provider. This is practically not possible because: • If you should have a "ready-to-use" internal solution, the costs are doubled and, in that case, you'd better use the internal capabilities without using the cloud; on the other hand, a "ready-to-use" solution is not always possible • Instant switching to another provider, in addition to increasing costs (probably making the cloud uncompetitive), is not always possible The expectation "The institution must maintain the ability to	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. The phrase "The institution must maintain the ability to bring data and applications back on-premises" should be deleted or alternatively reworded in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers".		
224	DR testing	ABI – Italian Banking Association The proposal is to amend the sentence "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" as follow: "When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event"	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
225	DR testing	ABI – Italian Banking Association The proposal is to amend the sentence "If joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution", as follow "In relation to critical services outsourced, if joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"	The final version of the Guide contains the expectation that supervised entities should assess the CSP's disaster recovery plan and test, instead of performing tests themselves,.	Yes
226	DR testing	ABI – Italian Banking Association The statement regarding testing plan contents and related scenarios seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence in brackets "(including component failure, full site loss, loss of a region and partial failures)"	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
227	DR testing	ABI – Italian Banking Association The statement regarding disaster recovery testing of CSP infrastructure seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence "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 Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
228	DR testing	ABI – Italian Banking Association The statement regarding institutions' testing of components within CSP's area of responsibility seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence "the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"	The final version of the Guide contains the expectation that supervised entities should assess the CSP's disaster recovery plan and test, instead of performing tests themselves	Yes
229	DR testing	ABI – Italian Banking Association When writing "an institutions should test its CSP's disaster recovery plans" please clarify what kind of test is expected. As the test would necessarily be conducted with the participation of the CSP, please clarify the expected role of the institution in the test activities.	The final version of the Guide contains the expectation that supervised entities should assess the CSP's disaster recovery plan and test, instead of performing tests themselves.	Yes
231	DR testing	ABI – Italian Banking Association Considered the share responsibility model, clarification is needed about whether the DRP is related to CSP infrastructure or to Institution's configurable services running on cloud	Section 2.2.3 states that Article 11(6), paragraph two of DORA (which states that the testing plans of financial entities must include, among	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		environment.	others, scenarios involving cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity) applies to situations where the supervised institution uses the CSP's ICT infrastructure. The title of 2.2.3 has been changed to clarify that the subsections refer to the CSP's disaster recovery strategy.	
232	Concentration risk	ABI – Italian Banking Association The concentration assessments cannot be carried out by single institutions, such assessment can be performed only in a centralised manner (i.e. via a joint assessment coordinated by the ECB). This provision should therefore be deleted	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
233	Concentration risk	ABI – Italian Banking Association It should be clarified by Authorities what would constitute a meaningful concentration of services in a specific location or in a specific function/service, or how much weight should be given to the assessed concentration risk. In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
260	Portability; DORA vs NIS 2;Timeline	Banking and Payment Federation Ireland (BPFI) Based on the comments provided under para 3 of "introduction 1.2 scope and effect" we would recommend the following text be deleted: 2.2.2: "For example, institutions should consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions." The Guide, furthermore, includes multiple references to the NIS2 Directive when informing the ECB's supervisory expectations, despite DORA being confirmed as lex specialis to NIS2, which will cause interpretation concerns for the sector. References are included in 2.2.1, 2.2.3, and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management), and all refer to requirements in NIS2 that exist within DORA in a greater level of detail. DORA includes a Chapter (Chapter 6; Article 24-26) within the Risk Management Framework dedicated to business continuity plans and disaster recovery while the references to incident response and recovery are intrinsic to the RTS in its entirety. The Guide would be aligned to DORA if the CIF definition was made consistent and references to NIS2 were removed. Finally, there is no clear indication of the timeline over which the ECB expects the requirements set out in the guide to be delivered. As many of the requirements go beyond existing requirements (under DORA or otherwise) and industry practice, implementation will take a substantial amount of time. Given industry's ongoing work to achieve compliance with DORA, the introduction of new additional requirements at this late juncture could endanger institutions' implementation of DORA requirements, and could generate additional operational risks and harm institutions' resilience.	All references to the NIS 2 Directive have been removed from the Guide. The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios. The Guide has been reviewed to ensure that it does not include requirements that go beyond DORA and other regulations. Similar to other ECB Guides, this Guide does not introduce binding requirements. Hence, it is not necessary to indicate a date for entering into force.	Yes
263	Scope of backup; Backup not in the same cloud; Definition of critical functions; Exit without cooperation	Banking and Payment Federation Ireland (BPFI) The ECB's Guide prescribes particular forms of technology solutions to scenarios which may not be appropriate, risk-based or the most resilient solution depending on the ECB's scenario. Whereas DORA Article 12 requires financial entities to develop and document policies and procedures specifying the scope of data that is subject to backup, and the minimum frequency of the backup, based on the criticality of information or confidentiality level of the data, the ECB's interpretation that this requires institutions to include back-ups for all CSPs. In our view, this does not account for the legislative provision that this should be based on the criticality and confidentiality of the data stored. We would therefore recommend that the Guide should consider what risks a financial entity may need to consider instead of prescribing a solution. Enforcing back-ups	The final version of the Guide states that the scope of the data subject to the backup and the minimum frequency of the backup should be based on the criticality of the information or the confidentiality level of the data. The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		outside of the individual CSP that hosts services is a blanket requirement that could also be resolved with a multi-regional back-up, on premises back-up or a differing architecture of workloads to aid resilience or portability. The level of back-up required, in addition, is unclear and could infer a multi-cloud active deployment which is highly complex to maintain, the highest cost of any deployment (with significant colleague training increases) and subject to considerable cybersecurity risk due to the expansion of the attack surface. The Guide also says back-ups critical or important systems 'should not be stored in the cloud' which hosts the service rather than 'should not be stored with the same CSP'. Is it correct to understand that data backed up to a different cloud with the same provider (e.g. in a different data centre) would be acceptable? This seems to be the case but given the preceding sentences refer to failure of the service provider it would be good to confirm this in the final Guide. Separately, the ECB do not define a 'critical or important system'. This could be interpreted to be any system which in any way supports a critical or important function, which would not consider materiality. The ESAs' technical standards on the use of ICT services to support critical or important functions includes a risk assessment of the service provided by a TPP (which would include CSPs) to inform the degree of application of the requirements, including the potential impact of disruptions on the continuity and availability of the financial entity's activities. We would propose that the ECB's requirements for the use of CSPs to support critical or important functions be based on an assessment of the risks associated with those services, rather than be applied across all CSP services regardless of the risks associated with them. Additionally, there are many benefits to institutions of maintaining back-ups within the same cloud as the service provided, including speed of recovery and reduction of impacts with certain issues, as demonstrated by the recent UniSuper case. Furthermore, if the final Guide applies these requirements for all CSPs, we would propose that instead of prohibiting the use of the same cloud for backups, the ECB should instead require institutions to assess the resilience of their backups based on the risk associated with the services provided, including for instance the storage of back-ups in different cloud regions, use of active / active backups, multi-cloud strategies, secondary back-ups outside of the primary cloud etc. This should be in line with the measures considered within section 2.2.2 Proportionate requirements for critical functions. The ECB's expectations that institutions address a scenario in which all cloud services provided by multiple CSPs are not available concurrently if applied to all ECB-supervised financial entities, could not occur technically in a realistic scenario. ECB expectations should be predicated on scenarios that are more realistic. Furthermore, such a scenario does not consider the resilience measures in place within individual CSPs which would prevent such a failure from happening in the first place, or allow rapid recovery from such a failure. In the absence of a clear rationale of how such a failure could occur without mitigation by CSPs' own resilience measure, presumption of this degree of failure does not appear in line with the 'severe but plausible' basis of most stress scenarios. We instead believe that BCM measures should address severe but plausible scenarios impacting the cloud services which they leverage, which would consider the mitigations which can be deployed by the CSPs themselves in plausible scenarios.	systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	
264	Architectures for resilience	Banking and Payment Federation Ireland (BPFI) Given the ESAs' development of technical standards covering Article 6, it seems unusual that the ECB would separately develop its own interpretations of Article 6(8) which seem to go beyond the standards developed by the ESAs in their mandate under DORA, and which could be interpreted as the ECB seeking to take on a regulatory role rather than a supervisory role. Regarding the ECB's interpretation of Article 6(8) in particular, DORA requires (which is expanded upon in the ESAs' technical standards) that institutions develop an operational resilience strategy and sets the components explaining how it will deliver against its operational resilience goals. It does not appear to require institutions consider specific resilience measures. Furthermore, the specification of specific resilience measures risks the guidance quickly	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		becoming out of date. We would propose that the ECB amend section 2.2.2 to remove the reference to specific resilience measures. The Guide's inclusion of various forms of cloud adoption for cloud resiliency do not reference the difference in operational and cybersecurity risk between each type of adoption. While the sector appreciates the inclusion of a risk-based approach for cloud adoption, the significant increases in complexity and trade-offs should be recognised by the ECB. For instance, a hybrid cloud architecture will introduce data transfer considerations and a reduction in a financial entity's end-to-end security visibility. The use of multiple CSPs to switch workloads introduces technical issues that can be unfeasible to implement across all of a CSP's services, as recognised by the EU's Data Act. These operational risk considerations have to be considered by a financial entity before determining their cloud adoption and should not be enforced via supervisory guidance. We therefore recommend that the risk-based approach stated by the ECB should also reflect the cloud resiliency option as well as the services or data represented. Between these two sets of consideration, we propose that section 2.2.2 be amended to read as below, without the bullet points which currently follow it. 2.2.2: "… the institution should assess the resilience requirements for cloud outsourcing services provided and the data managed and, following a risk-based approach that takes into account the cloud adoption measure, decide on the appropriate cloud resilience measures."	business continuity patterns has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	
265	Scope of DR; Definition of critical functions; Back on premises	Banking and Payment Federation Ireland (BPFI) The ECB's interpretation of purposes of Article 28(8) appears to go beyond the requirements envisioned in the primary legislation, as well as conflicting with the technical standards developed by the ESAs on the use of ICT services supporting Critical or Important functions. In particular, Article 10 of these technical standards states that, "the financial entity shall ensure that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements". Both the primary text and the technical standards seek to ensure that exit strategies address plausible scenarios and reasonable assumptions in relation to the services being leveraged. The ECB's expectation that institutions be able to remain fully operational in circumstances explicitly outside of the exit plans appears to go beyond these requirements. Furthermore, the ECB's specification of these requirements in relation to "Critical Functions", which they define by referring to the definition of "Critical or Important Functions" per the EBA's guidelines on outsourcing, which is not aligned to the definition of "Critical or Important Functions" under DORA does not appear in line with the scope of Article 28(8) in DORA, which is applied to ICT services supporting Critical or Important Functions (using the DORA definition). The Guide also includes enforcement measures that would result in a significant change to the technology stack of financial entities and would enforce a simplification of workloads supporting Critical or Important Functions. The ECB is clear that, for critical functions, a financial entity "must retain the ability to bring data and applications back on-premises." The SaaS, PaaS, or IaaS providers that could be supporting a critical function do not all provide critical services and, if they are non-operational, will not affect the service that is provider to the customer or the ICT system they are supporting. There are, in addition, significant technical complexities in architecting portability between CSPs and on-premise infrastructure, especially in relation to SaaS or PaaS. Continued innovation of services would have to be consistently updated within an entity's on-premises infrastructure and, in certain circumstances, could be beyond the capabilities of a financial entity's data centres. In this respect, it is not an appropriate risk management approach to mandate one specific cloud resilience option that does not reflect the cloud service being used. Multi-region capability, for instance, provides a significant degree of resilience and a financial entity could architect certain aspects of the service to be portable to their on-premise infrastructure, which can ensure the continuation of the service for the customer. Furthermore, the	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. Reference to "fully operational" has been removed and definition of critical or important function has been aligned with DORA. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		maintenance of on-premises infrastructure to enable the ability to bring data and applications back on-premises would directly and immediately counteract almost all of the commercial benefit to the use of cloud services. This would substantially harm the commercial viability of EU financial institutions, and could undermine the business model sustainability of firms. It is also likely to increase costs for EU customers, and inhibit institutions' abilities to provide financing and services to the real economy. This very specific requirement for financial entities to implement specific and extremely costly technology infrastructure does not appear to be grounded in either the primary DORA legislation, or the supplementary technical standards. We therefore recommend greater flexibility is applied and that the ECB does not enforce technology infrastructure requirements on financial entities via Supervisory Guidance. 2.2.2 "The institution should consider the ability to bring data and applications back on-premises depending on the cloud service."		
266	DR testing	Banking and Payment Federation Ireland (BPFI) The Guide expands the testing requirements placed on ECB-supervised entities for their third-party providers. DORA already includes a material expansion for the testing requirements placed on financial entities, including testing backup procedures, ICT response and recovery plans, ICT tools and systems and more rigorous Threat-Led Penetration Testing that will apply to ECB supervised firms. The Guide in our view further expands this requirement to include spot checks on cloud providers to assess readiness for disaster events. It is unclear if this is achievable in reality and if CSPs would be able to continually allow spot tests across all ECB-supervised entities alongside shared TLPTs in their control environment. The addition of spot checks is disproportionate and unclear regarding its utility to demonstrate readiness for a disaster event. For instance, an industry table top exercise, or the validation of CSPs' plans via audit could provide greater levels of information. We recommend that the suggestion for spot checks is removed.	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
267	Deficiencies in DR	Banking and Payment Federation Ireland (BPFI) The ECB also states in the draft guide that a mechanism where a financial entity can secure remediation of deficiencies identified during testing is via a renegotiation of a contract with a CSP. The Guide should not encourage continual off-cycle contract renegotiations, which creates an undesirable legal environment without meaningfully addressing the deficiencies that have been identified and their potential solutions. Gaps identified should be addressed within the business continuity plan and the control environment of the CSP. We recommend this suggestion is removed.	The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
268	Concentration risk	Banking and Payment Federation Ireland (BPFI) In our view, the indicators are overly expansive, imposing additional risk management burden and lacking sufficient relevance to the assessment of concentration risk. Additionally, the Guide should expressly state that concentration risk should be assessed on a risk-based approach. The expectation to consider reliance by other entities is unreasonable and reflects sector-level concentration risk which is not feasible for a financial entity to take into consideration.	The risk assessment carried out when entering into a contractual arrangement with a CSP should also address concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
284	Exit without cooperation; BCM vs exit strategies	European Cloud User Coalition (ECUC) The ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the FI has to perform an exit under stress or an exit without cooperation from the CSP(s) whereas we suggest we should address severe but plausible scenarios, as worst-case scenarios are highly unlikely and subjective. Also, exit under stress is not necessarily required and exit should be done only after assessing the	In the final version of the Guide, the worst-case scenario will no longer include lack of cooperation from CSPs. In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		circumstances. The lack of proportionality in not limiting Exiting under stress requirements to only services supporting CIFs is stretching the feasibility of the guidance. We suggest to maintain the approach laid out in 2.4.2 where business continuity management and exit management are not the same. The (partial) unavailability of relevant cloud services is in our understanding a temporary scenario and not equal to an exit scenario which will terminate the business relationship with a CSP.	under stress or without cooperation from the CSP.	
285	Back on premises	European Cloud User Coalition (ECUC) Certain requirements relating to having on-premise solutions for CIFs or having multiple CSPs for a service may not be necessarily feasible and practical to implement as it does not address the risk posed instead leads to different concentration risk. 'The institution must retain the ability to bring data and applications back on-premises'. What is exactly expected? This is a new requirement which is practically not feasible. A strict rule to have a mandatory "back on-premise" ability for each application as part of business continuity or disaster recovery processes is disproportionate and will essentially stop all cloud adoption, as it would require to have all on-prem infrastructure in place at all times. It would also stop all investments in building up back-up capabilities with a 2nd or 3rd CSP and consequently renders the previous bullet void. Our view is that this approach would decrease operational resilience and increase costs. In addition, it is a very far-reaching requirement that does not seem to fit in a world (as supported by the ESA's) in which on-premise solutions are replaced with SAAS and where alternative SAAS providers serve as proper backups. Most Services have never been on premise. Measures like alternative back-up/ providers should be sufficient.	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes
286	Backup not in the same cloud	European Cloud User Coalition (ECUC) 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'. Is it the security or the continuity? In addition: what does this mean in practice? For SAAS solutions primary servers handle live data and backup servers are designed to create and store copies of data from primary servers. This is a far-reaching requirement. What is the real risk that is supposed to be mitigated? Please advise. Does the requirement only address critical or important functions?	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
287	Portability	European Cloud User Coalition (ECUC) Some text is perceived too prescriptive; this will ensure that the guidance quickly becomes out-of-date as practices and technologies rapidly evolve in this space. This occurred with the 2013 MAS Risk Management Regulations. E.g. we recommend deleting: “To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions” (Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions)	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes
288	DR testing	European Cloud User Coalition (ECUC) "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." Is it the obligation of the institution to initiate a.o. spot checks?	The Guide now includes as a good practice that supervised entities assess the CSP’s DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		It is suggested to delete the obligation for conducting spot checks as it is considered unrealistic to conduct spot checks by each institution for all services. In all cases a materiality lens should be applied through to follow proportionality principles.		
289	Concentration risk	European Cloud User Coalition (ECUC) The concentration assessment provisions fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical Third Party regime. These should be leveraged, rather than expecting assessments on a regular basis by the firm. We suggest to also refer to the EBA guidelines on outsourcing (which should also be part of the supervisory approach of the ECB as long as these guidelines are not revoked or amended – if not; justification should be given why the EBA Guidelines are not taken into account).	Section 2.2.4 has been revised to ensure its consistency with Article 29 of DORA and has been moved to Section 2.1.2 – Box 1.	Yes
299	Definition of critical functions	European Cloud User Coalition (ECUC) Clarify on sentence: when selecting a CSP an institution should ensure that business continuity, resilience and disaster recovery capabilities can be maintained, including for all outsourced cloud services. Is the purpose here focus on entire chain including CoIF and non-CoIF / 4/5th party, or else? What is the scope of All outsourced cloud services?	In the final version of the Guide, the reference to all outsourced cloud services has been removed.	Yes
300	Definition of cloud services	European Cloud User Coalition (ECUC) When considered 'cloud Services' is this then Infrastructure (IaaS), Platform (PaaS), Software (SaaS) or all or/and the strict 'Definition in definition of terms for purpose of this Guide'? Please advise.	See definition of “Cloud services” in Section 1.1.	No
301	Definition of critical functions	European Cloud User Coalition (ECUC) The title states "Proportionate requirements for critical functions". Advised to change it to critical or important.	In the final version of the Guide, the title of Section 2.2.2 has been changed to refer to critical or important functions.	Yes
302	Architectures for resilience	European Cloud User Coalition (ECUC) The measures mentioned to contribute to resilience that can be taken by the institution are mentioned here. However one can read these measures (particularly bullet 1,2) as measures at the vendor. In that case the measure that can be taken by the institution is on the contractual requirements and management. If so, please refer to these type of measures.	The cloud resilience measures are offered by CSPs but adopted by customers under their own responsibility (e.g. using cloud services offered in multiple data centres).	No
303	DR testing	European Cloud User Coalition (ECUC) If joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP’s area of responsibility are covered by tests conducted by the institution. Could you please advise how this should be achieved?	The final version of the Guide contains the expectation that supervised entities assess the CSP’s disaster recovery plan and test, instead of performing tests themselves.	Yes
304	Concentration risk	European Cloud User Coalition (ECUC) 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 Question: what is the alternative for functionality concentration. Please provide good practice.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
305	Concentration risk	European Cloud User Coalition (ECUC) A definition of concentration risk and lock-in risk are not defined / captured. This makes the paragraph difficult to read/scope. Could you please provide a definition and a good practice?	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
310	Exit without cooperation	European Cloud User Coalition (ECUC) It is requested to clarify if an "exit without cooperation from the CSP" is relating to a scenario where we observe unwillingness of a CSP to fulfil contractual obligations.	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
311	BCM vs exit strategies	European Cloud User Coalition (ECUC) We suggest to maintain the approach laid out in 2.4.2 where business continuity management and exit management are not the same. The (partial) unavailability of relevant cloud services	In the final version of the Guide, the business continuity measures that address the worst-case	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		is in our understanding a temporary scenario and not equal to an exit scenario which will terminate the business relationship with a CSP.	scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	
332	BCM vs exit strategies	European Banking Federation This provision could implicitly introduce new requirements, while referring to the concept of a “holistic perspective”. Whenever the expectation is to consider both “business continuity” (Backup/Restore) and “exit strategy” elements in a unique framework, we foresee a potential risk in a dramatic increase in complexity, significantly limiting the architectural alternatives to be considered and further complicating the verification and control actions towards CSPs.	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
333	Backup not in the same cloud	European Banking Federation The statement regarding institutions' response and recovery planning and Business Continuity Management seems to require the implementation of multi cloud environments. The criticality of such statement is even higher considering also exit strategies. The complexity of implementing exit strategies in a multi cloud configuration is not measurable, also considering vendor lock-in during exit strategy implementation. The result of the statement is: multi cloud environment or on-premises environment, there aren't alternative legit configurations	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
334	Backup not in the same cloud	European Banking Federation The ECB considers that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned”. We suggest clarifying the statement “back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned”, while including proportionality. Also, we wonder if the Guide implies that critical data must be backed up with different CSPs, thus asserting a multi-cloud requirement. Furthermore, should this reference be read as a back-up provision in another datacentre or another region? Should this be read literally as back-up provision in other providers? This is not a market practice and entails enormous technical and security challenges, because the cloud provider might use a specific database that cannot be backed up with another cloud provider or on-premises infrastructure. In the latter case, we argue that this should be limited to the most crucial data (such as source code).	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
335	Backup not in the same cloud	European Banking Federation The statement regarding institutions' response and recovery planning and Business Continuity Management (BCM) seems to require the implementation of multi- cloud environments. The criticality of such statement is even higher considering also exit strategies. The complexity of implementing exit strategies in a multi-cloud configuration is not measurable, also considering vendor lock-in during exit strategy implementation. The result of the statement is: multi-cloud environment or on-premises environment, as if there are no alternative legit configurations.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
336	Backup not in the same cloud	European Banking Federation The Guide indicates that "back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned". In our understanding, the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the Business Continuity through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	
337	BCM vs exit strategies	European Banking Federation The last paragraph "For the purposes of Article 12(6) of DORA, the ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question" collapses Business Continuity and Exit Strategy considerations and introduces the concept of an "exit under stress or an exit without the cooperation of the CSP(s)".	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
338	Architectures for resilience	European Banking Federation The statement regarding multi region and multi availability zone approach seems to be a requirement not present in the current regulation. We propose to delete the sentence in brackets "(A multi-region approach is even better, offering additional security relative to a set-up with multiple virtual zones in the same region.)" and the sentence "in different availability zones".	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	Yes
339	Architectures for resilience	European Banking Federation With reference to the request "appropriate cloud resilience measures", confirmation is sought that this provision is applicable only with reference to IaaS Clouds.	The supervised entity should consider all cloud services, not only IaaS, when assessing the resilience requirements for the cloud outsourcing services provided and the data managed and, following a risk-based approach, when deciding on the most appropriate cloud resilience measures.	No
340	Definition of critical functions	European Banking Federation The Guide in this chapter refers to the EBA Guidelines in footnote 7 to define critical functions. Deletion of this reference is suggested, in order to maintain consistency with the definitions provided in the table "Definitions of terms for the purposes of this Guide" on page 2.	In the final version of the Guide, the footnote defining critical functions has been removed.	Yes
341	Back on premises; Portability	European Banking Federation The provisions regarding portability of data requirement (“must retain”) and the ability of institutions to bring data back on-premises go far beyond the DORA, entailing significant operational challenges (not only for smaller institutions). Therefore, we strongly urge for the deletion of this provision. Only alternatively, this wording provision should be formulated to "may" instead of “must”.	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios. This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	
342	Back on premises	European Banking Federation The expectation "The institution must maintain the ability to bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. The sentence "The institution must maintain the ability to bring data and applications back on-premises" should be deleted or alternatively reworded in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers".	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes
343	DR testing	European Banking Federation The proposal is to amend the sentence "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" as follows: "When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event".	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
344	DR testing	European Banking Federation The proposal is to amend the sentence "If joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution", as follows: "In relation to critical services outsourced, if joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and test, instead of performing tests themselves.	Yes
345	DR testing	European Banking Federation The statement regarding testing plan contents and related scenarios seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence in brackets "(including component failure, full site loss, loss of a region and partial failures)".	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
346	DR testing	European Banking Federation The statement regarding disaster recovery testing of CSP infrastructure seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence "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 Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
347	DR testing	European Banking Federation The statement regarding institutions' testing of components within CSP's area of responsibility seems to be a new requirement that is not mentioned in the current regulation. We propose to remove the sentence "the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and test, instead of performing tests themselves.	Yes
348	DR testing	European Banking Federation When writing "an institutions should test its CSP's disaster recovery plans" please clarify what kind of test is expected. As	The final version of the Guide contains the expectation that supervised entities assess the CSP's	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		the test would necessarily be conducted with the participation of the CSP, please clarify the expected role of the institution in the test activities.	disaster recovery plan and test, instead of performing tests themselves.	
349	Roles and responsibilities; Deficiencies in DR	European Banking Federation While generally reasonable, the original phrasing of the section on personnel (both within the institution and the CSP) may diminish the capability of the institutions to include outside help (e.g. that of external consultants), where necessary. We suggest the following wording: "In the view of the ECB, it is good practice for core personnel at the institution and the CSP who are involved in disaster recovery procedures to have designated roles [...]". [..} it is also good practice for any deficiencies identified during testing to be documented and analysed in order to identify corrective measures, with a remediation plan (including details of relevant roles and responsibilities) being established and monitored via the appropriate governance bodies. Such deficiencies should be addressed – for example, by renegotiating the contract with the CSP."	Reliance on external personnel should not increase risks for the supervised entity. The same expectations apply to both internal and external personnel responsible for carrying out activities on the supervised entity's behalf. The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
350	DR testing	European Banking Federation "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 Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
351	DR testing	European Banking Federation If the proposal to delete the "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", is not taken on board, we recommend amending it as follows: "When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event."	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
352	DR testing	European Banking Federation If the sentence "test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications" is not deleted, we propose being modified as follows: "with reference to IasS Cloud test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications".	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications.	Yes
353	DR testing	European Banking Federation Considered the share responsibility model, clarification is needed about whether the DRP is related to CSP infrastructure or to Institution's configurable services running on cloud environment.	Section 2.2.3 states that Article 11(6), paragraph two of DORA (which states that the testing plans of financial entities must include, among others, scenarios involving cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity) applies to situations where the supervised entity uses the CSP's ICT infrastructure. The title of 2.2.3 has been changed to clarify that the subsections refer to the CSP's disaster recovery strategy.	Yes
354	Concentration risk	European Banking Federation The concentration assessments cannot be carried out by single institutions, such assessment can be performed only in a centralised manner (i.e. via a joint assessment coordinated by the ECB). This provision should therefore be deleted.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
355	Concentration risk	European Banking Federation It should be clarified by Authorities what would constitute a	Section 2.2.4 has been revised and moved to	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		meaningful concentration of services in a specific location or in a specific function/service, or how much weight should be given to the assessed concentration risk. In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	
356	Concentration risk	European Banking Federation The Guide should expressly state that Financial Entities concentration risk should be assessed on a risk-based approach. Additionally, the concentration risk indicators are overly expansive, incorporating numerous factors that lack sufficient relevance to an accurate assessment of concentration risk and imposing both an unrealistic and unmanageable burden on risk management practices. This accounts in particular for the assessment of the scalability of the cloud which allows it to be gradually extended to encompass new functions.	The risk assessment carried out when entering into a contractual arrangement with a CSP should also look at concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. Section 2.2.4 has been revised in order to make clear that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
424	Definition of critical functions	Dutch Banking Federation (DBF) These requirements seem to be more realistic thant the requirements in 2.2.1. But the titel states 'Critical functions', can you confirm this is the same as 'critical or important'.	In the final version of the Guide, the title of Section 2.2.2 has been changed to refer to “critical or important functions”.	Yes
425	Architectures for resilience	Dutch Banking Federation (DBF) The measures mentioned to contribute to resilience, which can be taken by the institution, are outlined here. However, one might interpret these measures (particularly bullet points 1 and 2) as actions applicable to the vendor. In that case, the institution’s responsibility lies in managing contractual requirements.	The cloud resilience measures are offered by CSPs but adopted by customers under their own responsibility (e.g. using cloud services offered in multiple data centres).	No
426	Architectures for resilience	Dutch Banking Federation (DBF) This paragraph is lacking in proportionality. It should be amended to take account of the fact that maintaining multiple CSPs would be prohibitively expensive. Focus instead on multiple back up providers.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. In addition, a reference to the principle of proportionality has been added when following a risk-based approach to decide on the most appropriate cloud resilience measures.	Yes
427	Back on premises; Portability	Dutch Banking Federation (DBF) The level of prescription below will ensure that the guidance quickly becomes out-of-date as practices and technologies rapidly evolve in this space. This occurred with the 2013 MAS Risk Management Regulations. We recommend deleting: "To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios. This is the ECB understanding of the provisions of Article 28(8)	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		solutions". We also recommend deleting: "The institution must retain the ability to bring data and applications back on-premises". Because this sentence has different requirements than previous part of the chapter.	fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	
428	Architectures for resilience	Dutch Banking Federation (DBF) The guidance will lead to variations in interpretation through the use of "may include". Would want confirmation that adapting these provisions on a proportionate basis will not conflict with ECB expectations.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. In addition, a reference to the principle of proportionality has been added when following a risk-based approach to decide on the most appropriate cloud resilience measures.	Yes
429	Architectures for resilience	Dutch Banking Federation (DBF) Regarding the reference to Article 6(8) of DORA, it should be viewed as a general provision that encompasses all technologies, including the Cloud. If we need to develop ad-hoc strategies for each project, it could weaken its implementation.	When assessing the resilience requirements for the cloud outsourcing services provided and the data managed and when deciding on the most appropriate cloud resilience measures following a risk-based approach, the supervised entity should consider all the services provided by CSPs, and not just the cloud services introduced or changed for each project.	No
430	Portability	Dutch Banking Federation (DBF) We miss alignment with the Data Act in the following part of the Guide: "To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment." The Data Act contains obligations for CSPs to ensure the portability of data and systems. These obligations for institutions are therefore also dependent on the enforcement of the Data Act on CSPs.	The Guide is aimed at supervised entities, which may leverage on the obligation for the CSPs to provide mechanisms to facilitate the portability of data.	No
431	Back on premises	Dutch Banking Federation (DBF) The institution must retain the ability to bring data and applications back on-premises. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimizing the impact of relying on a solution specific to an individual CSP. However, in the majority of cases, achieving this practicality is not feasible.	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes
432	Scope of DR	Dutch Banking Federation (DBF) We need clarification on how to interpret the following scenario: According to Article 28(8) of DORA, the ECB expects institutions to ensure that abrupt discontinuation of a CSP's outsourced cloud services for critical functions does not result in business disruption beyond the maximum tolerable downtime or data loss defined in the institution's internal policies.	In the final version of the Guide, the reference to DORA has been amended to Article 12(6), "In determining the recovery time and recovery point objectives for each function, financial entities shall take into	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met." In addition, the existing reference to internal policies has been amended to refer instead to ICT business continuity plan.	
433	DR testing	Dutch Banking Federation (DBF) To avoid misinterpretation and ambiguity, clarification is needed regarding whether the Disaster Recovery Plan (DRP) is related to CSP infrastructure or the institution's configurable services running in the cloud environment.	Section 2.2.3 states that Article 11(6), paragraph two of DORA (which states that the testing plans of financial entities must include, among others, scenarios involving cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity) applies to situations where the supervised entity uses the CSP's ICT infrastructure. The title of 2.2.3 has been changed to clarify that the subsections refer to the CSP's disaster recovery strategy.	Yes
434	DR testing	Dutch Banking Federation (DBF) It is not proportionally realistic to do spot checks of all services as part of tests for disaster recovery. It should be applied through a materiality lens. Similarly, non-reliance on disaster recovery certifications should be limited to IaaS.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
435	DR testing	Dutch Banking Federation (DBF) We recommend that the Guide actively encourage CSPs to participate in joint testing. Our suggestion is to add the following: 'In relation to critical services outsourced, if joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution'.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and test, instead of performing tests themselves.	Yes
436	Deficiencies in DR	Dutch Banking Federation (DBF) The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. The non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation, and the Guide should recognize these practical difficulties. These difficulties will be exacerbated when applied to non-CSP third-party providers (TPPs) reliant on cloud services provided by a CSP.	The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
437	DR testing	Dutch Banking Federation (DBF) We require further guidance on how to address testing when joint testing with the CSP is not possible.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and test, instead of performing tests themselves	Yes
438	Concentration risk	Dutch Banking Federation (DBF) The definitions of 'concentration risk' and 'lock-in risk' lack	Section 2.2.4 has been revised and moved to	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		clarity. It's challenging to pinpoint their scope, and we're left wondering whether market share constitutes a concentration risk, for instance. Additionally, concentration risks must be considered in the policy governing the use of ICT services that support critical or important functions, as outlined in Article 1 (h) of DORA. I would anticipate the Guide to include a reference specifically addressing concentration risk related to geographical data storage, as that represents an actual risk.	Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	
439	Concentration risk	Dutch Banking Federation (DBF) The concentration assessment provisions, which we understand to be at the entity level, fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical ICT Third Party Provider regime. These should be leveraged, rather than expecting assessments on a regular basis by the firm. The preliminary assessment of ICT concentration risk obligated by Article 29 DORA is the key. The guidance should be embedded in the wider regulatory landscape. There is also a lack of clarity over whether the concentration risk is internal or external, and a need to recognise that In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	Section 2.2.4 has been revised to ensure its consistency with Article 29 of DORA. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
440	Concentration risk	Dutch Banking Federation (DBF) Whilst it is referred to clause 28(4) DORA, various considerations on concentration are mentioned for the FE, partly based on 'good practice', but it is not clear where those considerations originate from exactly. We ask to elaborate the text.	Section 2.2.4 has been revised and definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
479	Backup not in the same cloud	DIGITALEUROPE Back-ups of critical functions are an important element of a financial entity business continuity plans, as noted by DORA. However, sub-subsection 2.2.1 of the Guide mandates financial entities to employ multi-provider requirement for critical or important functions. This is not in line with DORA and would potentially lead to increased risks and costs. The text should be amended to read: 'IN ORDER TO AVOID JEOPARDISING THE SECURITY OF NETWORK AND INFORMATION SYSTEMS, THE ECB CONSIDERS THAT BACK-UPS OF CRITICAL OR IMPORTANT SYSTEMS SHOULD BE STORED IN LOGICALLY AND PHYSICALLY SEGREGATED SYSTEMS'.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
480	Exit without cooperation	DIGITALEUROPE DORA Art. 12 (6) addresses recovery procedures and methods, while ECB Guide goes further adding unclarity and complexities related to perform exit 'under stress' or exit 'without cooperation from the CSP'. We propose to delete the paragraph 'For the purposes of Art. 12(6) of DORA, the ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question'.	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
481	Architectures for resilience	DIGITALEUROPE 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.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the descriptions of the business continuity patterns	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	
482	Reference to regulation	DIGITALEUROPE Note 7 for the 'FOR CRITICAL FUNCTIONS' term in the fifth bullet point of the first paragraph should refer to DORA, instead of the EBA Guidelines.	In the final version of the Guide, the footnote defining critical functions has been removed.	Yes
483	Back on premises	DIGITALEUROPE The last bullet of 2.2.2 should be amended as follows: The institution must retain the ability to bring data and applications back on-premises OR TRANSFER DATA AND APPLICATIONS TO AN ALTERNATIVE PROVIDER. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP.	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes
484	DR testing	DIGITALEUROPE Reliance upon disaster recovery certifications or third-party certifications is a scalable and widely acknowledged to be an appropriate and practical proxy for financial entities as part of comprehensive ICT risk management. As drafted sub-subsection 2.2.3 is not aligned with DORA and introduces de-facto new requirements. Hence, sub-subsection 2.2.3 should be amended to DELETE the FOUR SENTENCES in paragraph 1 'ON THE BASIS OF THESE PROVISIONS, THE ECB UNDERSTANDS THAT AN INSTITUTION SHOULD TEST ITS CSP'S DISASTER RECOVERY PLANS AND SHOULD NOT RELY EXCLUSIVELY ON RELEVANT DISASTER RECOVERY CERTIFICATIONS. WHEN CONDUCTING DISASTER RECOVERY TESTS WITH THE CSP, THE INSTITUTION SHOULD PERFORM SPOT CHECKS AND/OR TESTS AT SHORT NOTICE IN ORDER TO ASSESS ITS READINESS FOR AN ACTUAL DISASTER EVENT. THE TESTING PLAN SHOULD COVER A VARIETY OF DISASTER RECOVERY SCENARIOS (INCLUDING COMPONENT FAILURE, FULL SITE LOSS, LOSS OF A REGION AND PARTIAL FAILURES). THESE SCENARIOS SHOULD BE TESTED REGULARLY IN ACCORDANCE WITH THE INSTITUTION'S STRATEGY AND IN LINE WITH ITS BUSINESS CONTINUITY POLICY AND REQUIREMENTS'.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
485	Concentration risk	DIGITALEUROPE As drafted, paragraph 2.2.4 of the Guide fails to acknowledge how financial entities can architect their cloud environments to avoid concentration risks; and differs from DORA in its specific requirements on how to address these risks. Sub-subsection 2.2.4 should be amended to remove: (i) in the first paragraph, the sentence beginning '[C]ONCENTRATION RISKS ARE GENERALLY EXARCERBATED'; (II) in the second paragraph, the sentence beginning with '[W]HEN ASSESSING CONCENTRATION RISKS,'; and (iii) at the end of the second paragraph, the clause 'but also by taking into account…with potential effects on concentration risks'.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
487	Data residency	DIGITALEUROPE The second paragraph of 2.2.4 should be amended as follows: When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services (such as increased provider lock-in, less predictable costs, increased difficulty of auditing, concentration of provided functions and lack of transparency regarding the use of sub-providers), alongside aspects of data LOCATIONRESIDENCY.	In the final version of the Guide, "data residency" has been replaced with "location of data". Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	Yes
532	Backup not in the same cloud	European Association of Public Banks "the ECB considers that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned." is not realistic	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	
533	Backup not in the same cloud	European Association of Public Banks The suggestion that back-ups of CIFs should not be stored in the cloud which hosts the services will not always be practically possible. For the organization, it can be very difficult to separate hosting and service backups because the cloud provider might use a specific database that cannot be backed up with another cloud provider or on-premises infrastructure. Moreover, many initiatives that have been deployed in the cloud could be significantly impacted by this requirement. In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the BC through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
534	Exit without cooperation	European Association of Public Banks The proposed worst case scenario of an entire CSP being not available and not cooperative is lacking in plausibility. Ultimately, this requires having it duplicated in a data centre. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort.	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
535	Back on premises	European Association of Public Banks It indicates that institutions must have the capacity to bring the data and backups on-premises. The expectation "The institution must maintain the ability to bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. We therefore suggest deleting the phrase "The institution must maintain the ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers"	In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications.	Yes
536	Backup not in the same cloud	European Association of Public Banks The guidelines state "back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned". Please clarify that the back-up can be stored with the same service provider, as long as the service provider has redundancy in place to ensure back up data or critical or important systems is not stored in the same cloud.	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			has been removed.	
537	Exit without cooperation	European Association of Public Banks The guidelines state "(BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question." DORA 12 (6) relates to RTO and RPO. BCM measures will address worst case scenario's, however, typically the RTO will not be set at a realistic level for the worst case scenario, unless the institution sets RTOs for different scenario's (ie regular incident and worst case scenario's such as large scale ransomware). It seems not proportional to ensure that all services will be up and running again within for instance two hours if the service must be migrated to another cloud provider without any assistance from the provider. This would require having all operations synchronized over multiple providers which adds disproportional complexities and risks. Please clarify requirement to set RTOs and RPOs for different scenario's.	The supervisory expectations for RTOs and RPOs are intended for recovery under the scenarios reported in the business continuity plan and not for exit scenarios. In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
538	Backup not in the same cloud	European Association of Public Banks We suggest clarifying the statement “that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned”, and include proportionality. It is unclear whether this should be read as a back-up provision in other datacentre or region, or at other providers (which is not market practice). In case of the latter, this should be limited to the most crucial data (such as source code). In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Otherwise, the adoption of multi-vendor solutions will become mandatory. We wonder if this guidance implies that critical data must be backed up with different CSPs, thus asserting a multi-cloud requirement.	The final version of the Guide will no longer advise against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	Yes
539	DORA vs NIS 2	European Association of Public Banks The guidance contains several references to the NIS2 Directive, although DORA has been confirmed as lex specialis to NIS2, which could lead to interpretation issues. References in 2.2.1, 2.2.3 and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management) are included and all refer to requirements in NIS2 that are set out in more detail in DORA. The Risk Management section in Chapter 6; Articles 24-26 DORA deals with Business Continuity Plans and Disaster Recovery Plans, while the references to Incident Response and Recovery are an integral part of the overall RTS. It is unclear what further regulatory guidance will be added by the inclusion of NIS2 and to what extent this could lead to interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could lead to confusion in the financial sector regarding the lex specialis provision. Therefore, we recommend removing references to NIS2.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
540	Exit without cooperation	European Association of Public Banks The ECB states that financial institutions should have backup and recovery procedures in place by default. Necessitating a worst-case-scenario of the proportions described in paragraph 4 seems to be an excessive standard of preparedness, considering that such an „extinction level event“ may pose challenges that by far exceed what can be planned ahead for. Instead we suggest following a risk-based approach, which takes any impacting developments (including e.g. changes in the geopolitical landscape) into a broad view. Concerning an exit without cooperation from the CSPs we suggest taking into account that contracted CSPs are legally bound to support an ongoing exit-procedure for the duration of a full year. Negating any support would constitute a breach of contract that would likely jeopardize any given CSP's business model, and therefore appears to be highly unlikely. The interpretations go far beyond DORA and should therefore be deleted or formulated to "may", as this is contrary to Article 6.9 of DORA Level1 which states that “[...] financial entities may, in the context of the digital operational resilience strategy referred to in paragraph 8, define a holistic ICT multi-vendor	In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		strategy […]" and Article 12.3 which states that "When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system […]".		
541	Exit without cooperation	European Association of Public Banks Concerning an exit without cooperation from the CSPs we suggest taking into account that	In the final version of the Guide, the business continuity measures that address the worst-case scenario no longer includes the ability to perform an exit under stress or without cooperation from the CSP.	Yes
542	Portability	European Association of Public Banks Recommend deleting: To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes
543	Architectures for resilience	European Association of Public Banks The guidance will lead to variations in interpretation through the use of "may include". Would want confirmation that adapting these provisions on a proportionate basis will not conflict with ECB expectations.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. In addition, a reference to the principle of proportionality has been added when following a risk-based approach to decide on the most appropriate cloud resilience measures.	Yes
544	Architectures for resilience	European Association of Public Banks Regarding the reference to Article 6(8) of DORA, it should be viewed as a general provision that encompasses all technologies, including the Cloud.	When assessing the resilience requirements for the cloud outsourcing services provided and the data managed and when deciding on the most appropriate cloud resilience measures following a risk-based approach, the supervised entity should consider all the services provided by CSPs, and not just the cloud services introduced or changed for each project.	No
545	Architectures for resilience	European Association of Public Banks Concerning the separation of data centres when using multiple CSPs, the underlying issues (including separation of backups) may be mitigated by covering the probability of failure. This suggestion is raised also in regard to technical limitations, considering CSPs may share infrastructure to a degree where separation may no longer be a viable option. The Guide's inclusion of various forms of cloud adoption for cloud resiliency do not mention the difference in operational and cybersecurity risk between each type of adoption. While the sector appreciates the inclusion of a risk-based approach for cloud adoption, the significant increases in complexity and trade-offs should be recognised by the ECB. For instance, a hybrid cloud architecture will introduce data transfer considerations and a reduction in a financial entity's end-to-end security visibility. The use of multiple CSPs to switch workloads introduces technical issues that can be unfeasible to implement across all of a CSP's services, as recognised by the EU's Data Act. These operational risk considerations have to be considered by a financial entity before determining their cloud adoption.	The final version of the Guide will make it clearer that the list of business continuity measures is provided as good practice of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	Yes
546	Back on	European Association of Public Banks	The final version of the	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	premises; Portability; Backup not in the same cloud	The interpretations regarding the ability to bring data back on-premises and regarding portability go far beyond the DORA and should therefore be deleted or formulated to "may". Separate storage locations for backups can be costly and operationally challenging, particularly for smaller institutions.	Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications. The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	
547	Portability	European Association of Public Banks The guidelines state: 'To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment." The Data Act also includes obligations for the CSP's to ensure portability of data and systems. So these obligations for the institutions are also dependent on enforcement of the Data Act on CSP's.	The Guide is aimed at supervised entities, which may leverage the obligation for the CSPs to provide mechanisms to facilitate the portability of data in order to fulfil their obligation to move applications and data in-house or to alternative providers.	No
548	DR testing	European Association of Public Banks CSPs should be actively encouraged to participate in joint testing. The following caveat could be added: "In relation to critical services outsourced, if joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and test, instead of performing tests themselves.	Yes
549	Deficiencies in DR	European Association of Public Banks The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. The non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation and the Guidance should recognise these practical difficulties. These difficulties will be exacerbated when applied to non-CSP third-party provider (TPP) reliant on cloud services provided by a CSP. (see Row 10 comment above)	The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
550	DR testing	European Association of Public Banks With regard to the shared responsibility model, clarification is needed on whether the DRP is related to CSP infrastructure or to Institution's configurable services running on cloud environment.	Section 2.2.3 states that Article 11(6), paragraph two of DORA (which states that the testing plans of financial entities must include, among others, scenarios involving cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity) applies to situations where the supervised entity uses the CSP's ICT infrastructure. The title of 2.2.3 has been changed to clarify that the subsections refer to the	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			CSP's disaster recovery strategy.	
551	DR testing	European Association of Public Banks Spot checks on all services as part of disaster recovery tests would not be possible. Should be applied through a materiality lens. Similarly, not relying on disaster recovery certifications should be limited to IaaS.	The final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
552	Roles and responsibilities; Deficiencies in DR	European Association of Public Banks While generally reasonable, the original phrasing of the section on personnel (both within the institution and the CSP) may diminish the capability of the institutions to include outside help (e.g. that of external consultants) where necessary. We suggest the following wording: "In the view of the ECB, it is good practice for core personnel at the institution and the CSP who are involved in disaster recovery procedures to have designated roles [...]". [..} It is also good practice for any deficiencies identified during testing to be documented and analysed in order to identify corrective measures, with a remediation plan (including details of relevant roles and responsibilities) being established and monitored via the appropriate governance bodies. Such deficiencies should be addressed – for example, by renegotiating the contract with the CSP.	Reliance on external personnel should not increase risks for the supervised entity. The same supervisory expectations apply to both internal and external personnel responsible for carrying out activities on the institution's behalf. The sentence concerning remediation by renegotiating the contract has been removed from the final version of the Guide.	Yes
553	Concentration risk	European Association of Public Banks The Guide should expressly state that financial entities (FEs) concentration risk should be assessed on a risk-based approach. Additionally, the concentration risk indicators are overly expansive, incorporating numerous factors that lack sufficient relevance to an accurate assessment of concentration risk and imposing both an unrealistic and unmanageable burden on risk management practices. This accounts in particular for the assessment of the scalability of the cloud which allows it to be gradually extended to encompass new functions.	The risk assessment associated with entering into a contractual arrangement with a CSP should also look at concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. Section 2.2.4 has been revised in order to better clarify that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
588	Backup not in the same cloud	Google Cloud The guidance on back-ups for critical or important systems should focus on outcomes and not dictate methodology and must be consistent with DORA. This text should be deleted: "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." Alternatively, the text should be amended as follows:	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		In order to avoid jeopardising the security of network and information systems, the ECB considers that DATA back-ups of critical or important systems should [DELETE: not] be stored in PHYSICALLY AND LOGICALLY SEGREGATED SYSTEMS FROM THE SOURCE ICT SYSTEM [DELETE: the cloud which hosts the services concerned].	of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	
589	Back on premises ;Portability	Google Cloud The guidance should not restrict exit strategies and plans to bringing data and applications back on-premises when Article 28(8) of DORA also permits transfers to alternative providers. The text should be amended as follows: The institution must retain the ability to bring data and applications back on-premises OR TRANSFER DATA AND APPLICATIONS TO AN ALTERNATIVE PROVIDER. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while considering CONSIDERING [DELETE: minimising] the impact of using a solution specific to an individual CSP. [DELETE: For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions].	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2. The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes
590	DR testing	Google Cloud It is not safe for institutions to test a CSP's disaster recovery plans directly. The text should be amended as follows: On the basis of these provisions, the ECB understands that an institution should ASSESS [DELETE: test] its CSP's disaster recovery plans AND TESTS and should not rely exclusively on relevant disaster recovery certifications. When ASSESSING [DELETE: conducting] disaster recovery tests with the CSP, the institution should [DELETE: perform spot checks and/or tests at short notice in order to] assess its readiness for an actual disaster event. The CSP'S 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. Alternatively, the text should be amended as follows: On the basis of these provisions, the ECB understands that an institution should PARTICIPATE IN testS OF ITS its CSP's disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications. When PARTICIPATING IN [DELETE: conducting] disaster recovery tests with the CSP, the institution should [DELETE: perform spot checks and/or tests at short notice in order to] assess its readiness for an actual disaster event. The CSP'S 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 final version of the Guide contains the expectation that supervised entities assess the CSP's disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications.	Yes
591	Data residency	Google Cloud The reference to data residency in Section 2.2.4 is inconsistent with DORA. The text should be clarified as follows: When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services (such as increased provider lock-in, less predictable costs, increased difficulty of auditing, concentration of provided functions and lack of transparency regarding the use of sub-providers), alongside aspects of data LOCATION [DELETE: residency].	In the final version of the Guide, "data residency" has been replaced with "location of data". Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	Yes
607	Backup not in the same cloud	Bitkom It is importance to have robust business continuity plans. Proposed sub-subsection 2.2.1 is likely to cause confusion and	The final version of the Guide no longer advises against storing backups in	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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 same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed.	
608	Backup not in the same cloud; Exit without cooperation	Bitkom 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 final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
609	Architectures for resilience	Bitkom 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	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the descriptions of the business continuity patterns has been amended to avoid terms that are not defined in	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.	the Guide or not commonly used by CSPs.	
610	Architectures for resilience	Bitkom 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.	The final version of the Guide includes amended descriptions of the business continuity patterns so as to avoid terms that are not defined in the Guide and not commonly used by CSPs.	Yes
611	Scope of DR	Bitkom 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.	In the final version of the Guide, the reference to DORA has been amended to Article 12(6): “In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.” In addition, the reference to internal policies has been amended to refer instead to ICT business continuity plan.	Yes
612	DR testing	Bitkom 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 final version of the Guide contains the expectation that supervised entities assess the CSP’s disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications.	Yes
613	DR testing	Bitkom 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	The final version of the Guide contains the expectation that supervised entities assess the CSP’s disaster recovery plan and tests, rather than relying exclusively on relevant disaster recovery certifications. The Guide now includes as a good practice that supervised entities assess the CSP’s DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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”.		
614	Concentration risk	Bitkom 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.	Section 2.2.4 has been revised and moved to section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
615	Provider lock-in	Bitkom 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.	Section 2.2.4 has been revised in order to better clarify that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. This Section has been moved to Section 2.1.2 – Box 1.	Yes
616	Concentration risk	Bitkom 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.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
617	Concentration risk	Bitkom 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.	Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
618	Concentration risk	Bitkom Sub-section 2.2.4 links scalability of cloud and new functions	Section 2.2.4 has been revised in order to better clarify that the scalability of	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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 cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. This section has been moved to Section 2.1.2 – Box 1.	
619	Concentration risk	Bitkom 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)."."	Section 2.2.4 has been revised in order to better clarify that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
620	Concentration risk	Bitkom 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.	As per Article 8(2) of DORA, financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them. Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	Yes
641	Back on premises	European Savings and Retail Banking Group (ESBG) The institution must retain the ability to bring data and applications back on premises. To this end, the institution should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP….",	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes
642	Back on premises	European Savings and Retail Banking Group (ESBG) This situation is particularly relevant in point 2.2.2 (item 5), through the sentence "The institution must retain the ability to bring data and applications back on premises. To this end, institution should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact or using a solution specific to an individual CSP....", given that a large part of the current SaaS services on the market cannot be migrated on premises; a situation that will increase in the future, given that when manufacturers start offering their solutions in SaaS mode, they tend to stop providing the equivalent situation on premise or to reduce their functionality. There are also many services that have been born in SaaS mode and have never had an on-premise version. In the case of applications designed and developed by organisations directly in the cloud (cloud-native applications), the complexity and cost involved in making a technological platform capable of hosting these cloud-native applications available on-premise make the strategy of implementing new	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		applications or modernising existing ones directly in the cloud unfeasible in practice for most organisations.		
650	Definition of critical functions	Futures Industry Association The Guide creates interpretation issues by inconsistently applying expectations for outsourced cloud services that support Critical or Important Functions (CIFs) in certain chapters and not in others. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform "spot checks" across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. As cloud technologies cover a significant array of outsourced activities, this would constitute a vast level of operational change with limited benefit nor recognition of effective risk management practices. We recommend that the ECB includes a more detailed proportionality principle that applies to all Chapters or is more specific concerning their expectation for cloud outsourcing as it relates to CIFs. The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity's technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU's Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute "significant interference in the data, digital assets or service architecture." This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide.	The reference to critical or important systems has been removed. The Guide adheres to relevant regulations. When specific prescriptions apply only to critical or important functions, these have been addressed accordingly. The definition of "critical or important function" provided in Section 1.1 has been modified to ensure its alignment with DORA.	Yes
653	DORA vs NIS 2	Futures Industry Association The Guide includes multiple references to the NIS2 Directive when informing the ECB's supervisory expectations, despite DORA being confirmed as lex specialis to NIS2, which will cause interpretation concerns for the sector. References are included in 2.2.1, 2.2.3, and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management), and all refer to requirements in NIS2 that exist within DORA in a greater level of detail. DORA includes a Chapter (Chapter 6; Article 24-26) within the Risk Management Framework dedicated to business continuity plans and disaster recovery while the references to incident response and recovery are intrinsic to the RTS in its entirety. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
654	Portability	Futures Industry Association Recommendation to delete the following sentence: 2.2.2: "For example, institutions should consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions." Specific solutions, such as containerization, virtual machine-based applications and encryption methods, should be chosen on a risk-based basis and depending on the needs of the financial entity. Specific solutions often become obsolete with continued innovation and are subject to wider considerations beyond the regulatory intent. A financial sector must consider what is most appropriate for their services, infrastructure and	The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		within their risk appetite. We recommend that the Guide is redrafted to not prescriptive specific approaches to technology adoption.		
655	DORA vs NIS 2	Futures Industry Association The Guide includes multiple references to the NIS2 Directive when informing the ECB's supervisory expectations, despite DORA being confirmed as lex specialis to NIS2, which will cause interpretation concerns for the sector. References are included in 2.2.1, 2.2.3, and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management), and all refer to requirements in NIS2 that exist within DORA in a greater level of detail. DORA includes a Chapter (Chapter 6; Article 24-26) within the Risk Management Framework dedicated to business continuity plans and disaster recovery while the references to incident response and recovery are intrinsic to the RTS in its entirety. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. We recommend that all references to NIS2 are removed.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
658	Backup not in the same cloud; Exit without cooperation	Futures Industry Association It is unclear regarding the resilience benefit that would be provided if all ECB-supervised entities had to place their back-ups for cloud hosted applications outside the CSP that originally hosts that service. Depending on the particular cloud service, having a multi-regional cloud back-up within the same CSP would provider a higher level of resilience benefit without any impact to the service should there be a disruption. Enforcing external back-ups, without a risk assessment predicated on plausible disruption scenarios, would result in excessive cost, more operational complexity and limited resilience benefit. The only scenario would be the complete CTC eradication of a CSP, which remains an extreme scenario to account for across all outsourced cloud services. ECB Guide seems to suggest a mandatory multi-cloud strategy, and this should not be the case - regulatory expectations on multi cloud strategy do not match the real use cases. Multi cloud strategy is not a reasonable approach - it has proven to be too complex and costly: • it does not deliver the expected value in terms of technical efficiency, • it is not cost-efficient, • it is not always feasible in terms of availability of CSPs comparable solutions. • it can introduce increased cybersecurity risk and operational complexity that can reduce the resilience benefit. FIA Members express concern on the uncertainty of how to define 'under stress' as mentioned in the ECB Guide (e.g. business continuity management measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question). We note that the wording on DORA differs as it mentions 'extreme scenarios'. FIA Members deem the ECB guidance proposes unrealistic time objectives for exit. It is not realistic and feasible from a technical point of view to exit a CSP in weeks. A best practice would be securing CSP support in exiting its services within months (e.g. 6-12 months) - even in case of switching to another CSP - in alignment with ESMA guidelines. The expectations stemming from the ECB's Guide, if applied to all ECB-supervised financial entities, could not occur technically in a realistic scenario. For instance, should a bankruptcy occur which required a stressed exit (without support) from a designated Critical Third Party Provider (CTPP) that provides IaaS storage services, then in all likelihood all supervised entities would be moving for one supplier to two other suppliers at the same time. CSPs have compute power limitations and there are latency issues in relation to significant movements of data. If all EU supervised	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		entities were undertaking this switch, then a 'thundering herd' would emerge where an instantaneous movement of applications would be technically unfeasible. There is, additionally, a significant increase in operational risk if this were to occur simultaneously. ECB expectations should be predicated on scenarios that are more realistic.		
659	Architectures for resilience	Futures Industry Association Amendment recommendation: 2.2.2: "… the institution should assess the resilience requirements for cloud outsourcing services provided and the data managed and, following a risk-based approach that takes into account the cloud adoption measure, decide on the appropriate cloud resilience measures." The Guide's inclusion of various forms of cloud adoption for cloud resiliency do not reference the difference in operational and cybersecurity risk between each type of adoption. While the sector appreciates the inclusion of a risk-based approach for cloud adoption, the significant increases in complexity and trade-offs should be recognised by the ECB. For instance, a hybrid cloud architecture will introduce data transfer considerations and a reduction in a financial entity's end-to-end security visibility. The use of multiple CSPs to switch workloads introduces technical issues that can be unfeasible to implement across all of a CSP's services, as recognised by the EU's Data Act. These operational risk considerations have to be considered by a financial entity before determining their cloud adoption. We therefore recommend that the risk-based approach stated by the ECB should also reflect the cloud resiliency option as well as the services or data represented.	The final version of the Guide makes it clearer that the list of business continuity measures is provided purely as an example of some common arrangements nowadays and that it is not intended to be exhaustive or to cover all scenarios. Reference to the principle of proportionality has also been added when following a risk-based approach to decide on the most appropriate cloud resilience measures. Lastly, the description of the business continuity patterns has been amended to avoid terms that are not defined in the Guide or not commonly used by CSPs.	Yes
660	Back on premises	Futures Industry Association 2.2.2 "The institution should consider the ability to bring data and applications back on-premises depending on the cloud service." The Guide includes enforcement measures that would result in a significant change to the technology stack of financial entities and would enforce a simplification of workloads supporting Critical or Important Functions. The ECB is clear that, for critical functions, a financial entity "must retain the ability to bring data and applications back on-premises." The SaaS, PaaS, or IaaS providers that could be supporting a critical function do not all provide critical services and, if they are non-operational, will not affect the service that is provider to the customer or the ICT system they are supporting. There are, in addition, significant technical complexities in architecting portability between CSPs and on-premise infrastructure, especially in relation to SaaS or PaaS. Continued innovation of services would have to be consistently updated within an entity's on-premises infrastructure. In this respect, it is not an appropriate risk management approach to mandate one specific cloud resilience option that does not reflect the cloud service being used. Multi-region capability, for instance, provides a significant degree of resilience and a financial entity could architect certain aspects of the service to be portable to their on-premise infrastructure, which can ensure the continuation of the service for the customer. We recommend greater flexibility is applied and that the ECB does not enforce technology infrastructure requirements on financial entities via Supervisory Guidance.	This is the ECB understanding of the provisions of Article 28(8) fourth paragraph of DORA, that supervised entities should retain the ability to transfer data and applications to alternative service providers or reincorporate them in-house. To ensure consistency with exit strategy, this part has been moved to section 2.4.2.	Yes
661	Backup not in the same cloud	Futures Industry Association We take note that the ECB understanding is that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned. The back up procedures and restoration and recovery procedures should be tested periodically in accordance with Article 12(2) of DORA. Tests should be validated as regards the accuracy, completeness, and practicality of recovery procedures. In general, FIA Members consider it as a good practice to do backups (e.g. copies for financial entities' critical or important systems data, code, etc.) in different regions or segregated from the hosted services, in order to restore applications and databases in case the main CSP becomes unavailable. This process, however, to establish complete equivalent services with all data and applications being moved takes weeks or longer. However, FIA Members believe ECB guidance goes further	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. Test validation is considered	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		than the requirements laid out by DORA on this point. FIA Members would like to highlight that testing back up and restoration/recovery procedures is complex and costly. Moreover, the requirement on testing validation is already present in DORA but ECB Guide on testing validation seems to go beyond DORA requirements (e.g. tests should be validated as regards the accuracy, completeness, and practicality of recovery procedures). Disaster recovery strategy is about leveraging on the resiliency capacity of the given CSP and not of a 'secondary CSP' (e.g. disaster recovery relies on multi-regions but always within the same provider). Therefore, we agree that disaster recovery should be separated from the production environment, but we disagree on the fact that it should be hosted within another provider.	as a good practice in the Guide.	
662	Concentration risk	Futures Industry Association The concentration risk considerations are overly prescriptive and create additional complexity for FIs.	The risk assessment associated with entering into a contractual arrangement with a CSP also considers concentration risk. As a result, concentration risk cannot be evaluated using a risk-based approach, as it is itself a factor used to determine the overall risk. Section 2.2.4 has been revised and moved to Section 2.1.2 – Box 1. Definitions of concentration risk and lock-in risk have been added to Section 1.1.	Yes
673	DORA vs NIS 2	German Banking Industry Committee (GBIC) The guide contains several references to the NIS2 Directive, although DORA has been confirmed as lex specialis to NIS2, which could lead to interpretation issues. References in 2.2.1, 2.2.3 and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management) are included and all refer to requirements in NIS2 that are set out in more detail in DORA. The Risk Management section in Chapter 6; Articles 24-26 DORA deals with Business Continuity Plans and Disaster Recovery Plans, while the references to Incident Response and Recovery are an integral part of the overall RTS. It is unclear what further regulatory guidance will be added by the inclusion of NIS2 and to what extent this could lead to interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could lead to confusion in the financial sector regarding the lex specialis provision. We therefore recommend removing references to NIS2.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
674	Backup not in the same cloud; Exit without cooperation	German Banking Industry Committee (GBIC) The ECB states that a financial company should not use the same cloud service providers for data backup. Furthermore, the ECB states that financial institutions should have backup and recovery procedures in place by default and limit losses int the event of severe disruptions to its business... Instead, we suggest a risk-based approach, which takes any impacting developments (including e.g. changes in the geopolitical landscape) into a broad view. Concerning an exit without cooperation from the CSPs we suggest taking into account that contracted CSPs are legally bound to support an ongoing exit-procedure for the duration of a full year. Negating any support would constitute a breach of contract that would likely jeopardize any given CSP's business model, and therefore appears to be highly unlikely. The interpretations go far beyond the DORA and should therefore be deleted or formulated as "may".	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the worst-case scenario no longer includes lack of cooperation from CSPs.	Yes
675	Back on premises; Portability	German Banking Industry Committee (GBIC) The interpretations regarding the ability to bring data back on-prem and regarding portability go far beyond the DORA and should therefore be deleted or formulated as "may".	The final version of the Guide no longer advises against storing backups in the same cloud. Instead, backup solutions should be	Yes

№	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			configured such that the ICT systems are logically and physically segregated from the source ICT systems and should consider the risk assessment of the criticality of data and functions. In addition, the current restriction on backup and recovery procedures being limited to the storage of data has been removed. In the final version of the Guide, the ability to transfer data and applications to other service providers is provided as an alternative to insourcing the data and applications. The final version of the Guide makes it clearer that the technologies for portability are provided as examples that are available and commonly used nowadays, particularly for IaaS, and that they are not intended to be exhaustive or to cover all scenarios.	
676	DR testing	German Banking Industry Committee (GBIC) There are a number of assumptions about how a financial institution can test a cloud service provider. The ECB states that financial institutions should carry out spot checks on CSPs (cloud service providers), which would not be proportionate to do for all cloud service providers and where we see challenges in implementation	The Guide now includes as a good practice that supervised entities assess the CSP's DRP, including a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures).	Yes
677	Definition of critical functions	German Banking Industry Committee (GBIC) C.f. our comments regarding the definition of critical or important functions (ID #1): How does this relate to the more „institution-focussed" definition within DORA?	All references to critical or important systems have been deleted. The Guide adheres to relevant regulations. When specific prescriptions apply only to critical or important functions, these have been addressed accordingly. The definition of "critical or important function" provided in Section 1.1 has been modified to ensure its alignment with DORA. Section 2.2.4 has been moved to Section 2.1.2 – Box 1.	Yes
678	Concentration risk	German Banking Industry Committee (GBIC) The aspect of scalability should be deleted and rephrased by: "In particular, concentration risks should be assessed not only on the basis of the number and nature of outsourced functions, but an integrated approach of concentration risk which may among others take into account the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks)"	Section 2.2.4 has been revised in order to better clarify that the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks) is one of the reasons why concentration risk associated with CSPs should be evaluated on a regular basis. This section has been moved to Section 2.1.2 – Box 1.	Yes

2.4 Table 4 – Comments on Section 2.3: ICT and data security, confidentiality and integrity

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
6	Identity and access management	Deutsche Börse Group Deutsche Börse Group would like to ask for a clarification regarding the exact meaning and scope of "individual clauses" agreed between the institution and CSP when configuring cloud environment.	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider.	Yes
17	Protection of data	AWS 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."	This part is to be understood as an enumeration of possible measures for safeguarding data. Each financial entity is free to implement the measures it chooses, as long as they satisfy the requirements of Article 9 of DORA.	No
18	Protection of data	AWS 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	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission's proposed list may serve as a useful guide in this respect.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.”		
19	Identity and access management	AWS 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.”	The ECB agrees to align the wording with the DORA definition.	Yes
20	Contract customisation	AWS 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	As CSPs can change their offer at will, and because having a contract helps to mitigate the associated risks, the ECB considers it useful for a bank to have safeguards in the form of contractual clauses.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		increasing costs on financial entities when using cloud services and introducing requirements not present in DORA.		
31	Assets identification	Nordea Abp Propose to exclude "maintain an up-to-date inventory of all the ICT assets" as the consumer doesn't have possibility to retrieve the relevant CSP asset inventory	Please bear in mind that the whole sentence reads as follows: “As part of this practice, a supervised entity should, as a matter of good practice, maintain an up-to-date inventory of all the ICT assets it is responsible for [...].”	No
43	Encryption requirements	Association of German Public Banks The level of “best practice“ is inadequately high especially with regards to cryptographic keys. There are additional means of a similar level of security “Best practice“ should be replaced by “exemplary measures“.	The ECB believes the network protection should be one layer of in-depth protection. Micro-segmentation – while desirable - should be completed with data encryption wherever possible, as outlined in Section 2.3.1 of the Guide.	No
44	Exercise of audit rights	Association of German Public Banks „Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements.“	As described in paragraph 2.5, supervised entities are encouraged to work together to audit a CSP.	No
45	Asset identification	Association of German Public Banks “Classification of all ICT assets“ in an up-to-date inventory does not reflect enough the criticality and creates an inappropriate burden. We suggest to include a risk-based approach.	The entity should consider all the ICT assets it is responsible for, depending on the deployment model and the sharing of responsibilities between the entity and the CSP.	No
46	Identity and access management	Association of German Public Banks It may be viable to compare this requirement to standard privileged access management procedures. It should be sufficient that the IAM policy is reflecting cloud outsourcing and is regularly reviewed in the outsourcing agreement	While user roles and access implementation may change frequently, IAM policies should contain applicable principles and remain stable over time. Not amended.	No
65	Encryption requirements	ABBL - The Luxembourg Bankers' Association The Guide states that, in order to have ICT security within the cloud, that a financial entity should encrypt data “in transit, at rest and, where feasible, in use.” IaaS providers automatically de-crypt data once a user has access to the particular workload in question. Encryption, in this respect, serves no ICT security benefit. The cybersecurity risk associated with encryption from a IaaS perspective relates to access management controls, to which a malicious actor could gain access and would also receive automatic decrypted data. We recommend this requirement is risk-based depending on the cloud service. 2.3: “encryption methods in line with the institution’s data sensitivity classification policy, the type of cloud service and a risk-based approach.”	This has been changed to include reference to a risk-based approach.	Yes
66	Protection of data	ABBL - The Luxembourg Bankers' Association The Guide introduces requirements that go beyond what is in DORA (recitals 82 and 83), therefore paragraph 1 of Chapter 2.3.2 should be amended. The absence of a clear risk-based approach endangers capturing an inappropriately broad scope of subcontractors. As noted above, all references to subcontractors should explicitly apply a materiality threshold in alignment with DORA (i.e. as ultimately reflected in the final draft regulatory technical standard on subcontracting).	Provision for a risk-based approach has been added.	Yes
67	Protection of data	ABBL - The Luxembourg Bankers' Association The guidance should focus on what is substantively required, and refrain from prescribing the format and how it should be achieved. Further, this expectation does reflect the reality of how cloud services are configured and contracted for. For	The ECB agrees, so the wording has been amended to: “good practice for supervised entities to consider individual	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		instance, cloud services are typically provided for under a framework contract or Master Services Agreement (MSA). It would not be appropriate for an FI to negotiate individual clauses in contracts each time they configure workloads under the overarching contract. It would be more appropriate for the Guide to state that it is "good practice for institutions to consider (to delete the word "agree") individual clauses with the CSP when entering into a cloud outsourcing arrangement (to delete the phrase "configuring the cloud environment")."	clauses with the CSP when entering into a cloud outsourcing arrangement."	
107	Encryption requirements	AFME Article 9 of DORA requires firms to use ICT solutions and processes to address risks in relation to data security, integrity, availability and access. While we agree with the ECB that institutions need to protect their data, we would note that DORA does not set specific requirements for the encryption of data, and that this is likely intentional. Furthermore, the ESAs' final technical standards on the ICT Risk Management framework establish that institutions should have a policy on encryption and cryptographic controls, based on data classification and ICT risk assessments, and which should include rules for the encryption of data at rest, in transit and in use, where necessary. It specifically acknowledges that the encryption of data in use may not be possible, and that other measures may be used to protect data in use instead. IaaS providers, for instance, automatically de-crypt data if the individual has appropriate access levels, which makes encryption redundant. The ECB's interpretation fails to take into account firms' assessment of the ICT risks associated with the data, and its classification. There are significant technical limitations for the encryption of data at rest and in use, and our view is aligned with that of both DORA and the ESAs in that firms should select the data protection controls based on the data and risks in question, rather than be required to apply specific controls across all data.	The ECB Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
108	Protection of data	AFME Data tracing for compliance monitoring would be extremely difficult to implement, and disproportionate to the associated risks. A more appropriate measure would be for institutions to establish contractual restrictions on the locations which may be used to store the data, and to require CSPs to attest to their compliance with these requirements, potentially supported by inclusion of data location within the scope of audits where appropriate. We propose that this section be amended to allow firms to determine the most appropriate approach to monitor compliance of location restrictions for their data.	Our opinion is that while financial entities could establish contractual agreements satisfying this expectations, they should retain the ability to perform controls, as set out in paragraph 2.5.	No
109	Protection of data	AFME The requirements in this section appear duplicative with the data security measures covered under the technical standards developed by the ESAs as part of their mandate under DORA, in particular Articles 6 and 7. We would suggest that the ECB avoid duplication of requirements to reduce the risk of conflicting requirements and disconnect between the two sets of requirements should either be reviewed in the future.	The measures listed in the document should be understood as good practice, deriving directly from DORA requirements. Therefore, they do not contradict the requirements of this text.	No
110	Protection of data	AFME The recommendation should be a list of unacceptable countries based on the firm's risk management practices, rather than a list of acceptable countries. If the aim is to ensure that FIs are aware of data processing and storage requirements across jurisdictions, the ECB should not prescribe the method (e.g. list of acceptable or unacceptable countries) by which an FI does this. Additionally, subcontractors "relevant for" the cloud does not appropriately apply materiality and therefore risks capturing an inappropriately broad scope of subcontractors. As noted above, all references to subcontractors should explicitly apply a materiality threshold in alignment with DORA (i.e. as ultimately reflected in the final draft regulatory technical standard on subcontracting). The Guide states that a financial entity must monitor a CSP''s access to their data. In a shared, multi-tenant environment, this would require a financial entity to actively monitor all hosted workloads despite workloads often constituting temporary storage. This is technically impossible and outside	The ECB advises supervised entities to draw up a list of countries where their data can be stored and processed, depending on the data in question. As such the European Commission's proposed list can serve (and should be understood solely) as a guide in this respect.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		of the ability for a financial entity.		
111	Protection of data	AFME As flagged above, regarding the use of subcontractors, this is a topic on which the ESAs are developing detailed requirements as part of their mandate under DORA, which will be subject to review and adoption by the European Commission and subsequent review by the co-legislators. More specifically, the ECB's proposals fail to take into account consideration of materiality, criticality or risk associated with these subcontractors. The assessment of all subcontractors across all CSPs would be extremely onerous and disproportionate to the risks associated with those subcontractors. While the final technical standards are still in development, the requirements in relation to subcontractors are limited to where the TPP provides ICT services supporting Critical or Important Functions (CIFs), and we understand that the ESAs intend to further specify their requirements to those subcontractors which materially underpin those CIFs. Consideration of risks is a fundamental element of risk management frameworks, and should be incorporated as appropriate for all measures. We would propose the deletion of requirements which overlap and potentially conflict with the final technical standards being developed by the ESAs.	Provision for a risk-based approach has been added. Furthermore, the ECB deems this requirement to be a direct result of Article 9(4)(d) of DORA, as stated in the text.	Yes
112	Asset identification	AFME The inventory of all ICT assets appears at odds with the Cloud based scope of this guidance. Additionally, a definition of Outsourced Asset is required: the EBA Guidelines on outsourcing arrangements cover the outsourcing of "processes" or "functions". It is unclear what cloud service would constitute an asset, what would be considered different assets of the same kind or different types of assets, especially regarding the adoption of SaaS products or that of serverless services.	While the scope of the Guide is cloud services, it also refers to all ICT assets the entity is responsible for, depending on the deployment model and on how responsibilities are shared between the entity and the CSP.	No
113	Protection of data	AFME The requirement for individual clauses should be deleted. The guidance should focus on what is substantively required, and refrain from prescribing the format, and how it should be achieved. Further, this expectation does reflect the reality of how cloud services are configured and contracted for. For instance, cloud services are typically provided for under a framework contract or MSA. It would not be appropriate for an FI to negotiate individual clauses in contracts each time they configure workloads under the overarching contract. It would be more appropriate for the Guide to state that it is "good practice for institutions to consider agreeing individual clauses with the CSP when entering into a cloud outsourcing arrangement configuring the cloud environment."	The ECB agrees with the proposed amendment: "good practice for supervised entities to consider individual clauses with the CSP when entering into a cloud outsourcing arrangement."	Yes
114	Segregation of duties	AFME The Guide should specify that this expectation "the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties" is only focused on Identity and access management (IAM)	Amended to: … how the IAM structure provided by the CSP for the cloud services ...	Yes
142	Identity and access management	American Chamber of Commerce to the European union Ensure the consistent application of the proportionality and risk-based principles embedded in DORA throughout the Guide. The Guide applies expectations for the risk management of all types of cloud services without reflecting the varying levels of risk and technical specification relevant to different types of cloud such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). For example: the expectation in Article 2.3.4.1 that institutions agree on individual clauses with the CSP when configuring the cloud environment may be appropriate for SaaS, but it not consistent with the IaaS or PaaS models, where configuration is a customer responsibility and can be changed by the financial institution at will. Additionally, the Guide applies requirements to services supporting critical or important functions (CIFs) in certain chapters but not others. The Guide should include a developed approach to proportionality that is consistent with DORA. Where the Guide intends to capture subcontractors, it should	First part: the proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider. Second part (after "additionally"): this relates to a generic remark for the Guide. A provision for a risk-based approach has been added, in line with DORA.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		explicitly apply a materiality threshold to supply chain scope in alignment with DORA (ie as noted in the comment above about definitions this should be consistent with what is ultimately reflected in the final draft regulatory technical standard on subcontracting, expected to specifically apply to those subcontractors, which effectively underpin CIFs). This should also apply where the ECB seeks to set expectations for TPPs, which are themselves reliant on CSPs. Without the consistent application of a proportionality and a risk-based approach, the supervisory expectations in the Guide could be interpreted as applying to a very expansive scope of CSPs and their subcontractors.		
169	Encryption requirements	ECIIA We suggest to delete "Consequently, institutions need to protect their data (including relevant back-ups) from unauthorised access by maintaining high levels of data encryption and constantly adapting to external threats. This involves encrypting data in transit, at rest and, where feasible, in use, employing appropriate encryption methods in line with the institution's data sensitivity classification policy. "	While the ECB recognises the importance of existing minimum standards for data encryption, the ECB believes that the statement emphasising the need for robust data protection should be retained. As cyber threats continue to evolve, relying solely on minimum standards may not be sufficient to safeguard sensitive data. Maintaining high levels of encryption across all stages—whether data is in transit, at rest, or in use—ensures a more comprehensive security posture. Additionally, this approach aligns with the supervised entity's data sensitivity classification policy, which helps mitigate risks more effectively.	No
170	Protection of data	ECIIA "of data in transit and data at rest "should include data in use i.e. memory.	The ECB deems in-use memory protection to be already a well established concept among supervised entities. Therefore, this extension doesn't seem to be necessary. However, the ECB has amended the text to specify that measures shall be applied "where relevant".	Yes
171	Protection of data	ECIIA With reference to envisaged "good practice for institutions to restrict the locations where CSPs can store their data" it has to be noted that when dealing directly with a CSP - as opposed to a TPP - the location is usually an institution's own choice. How should this aspect be weighted against considerations of geographical concentration from before?	Both the supervisory expectation to restrict the locations where CSPs can store data and the need to manage geographical concentration risks must be carefully balanced. When dealing directly with a CSP, supervised entities have indeed the flexibility to choose the data storage location. However, this choice must be made with an awareness of potential geographical concentration risks. To mitigate these risks, it is essential to ensure that data location decisions align with both security practices and geographical risk management strategies, as outlined in the Guide.	No
172	Protection of data	ECIIA This reads as best practice and optional, what are the minimum requirements for FS firms t?	The ECB believes that the term "good practice" should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
173	Encryption requirements	ECIIA On responsibilities in controlling the cryptographic keys. Can companies revoke the data from the CSP after exiting the business relationship so that the CSP doesn‘t have access to the data anymore?	Financial entities are required to remain in effective control of their data, by all means deemed necessary, even after their relationship with the CSP has ended.	No
174	Protection of data	ECIIA Please clarify how the listed security measures can strengthen data security on cloud environment.	These measures are those generally put forward by the industry when addressing data protection.	No
175	Protection of data	ECIIA Will the ECB regulate the CSPs and without this, the FS firms may not be able to get all relevant information?	The ECB is not meant to regulate CSPs, although this does not relieve financial entities of their responsibility to obtain the relevant information.	No
176	Asset identification	ECIIA in relation to the provision "adopt a clear policy on the classification of all ICT assets, including those that are outsourced to CSPs", clarification is needed from the ECB on the definition of an ICT asset within Cloud services	The definition of “ICT asset” has been aligned with DORA.	Yes
177	Identity and access management	ECIIA Instead of "Roles and Responsibilities", "Roles and responsibilities for Identity & Access Management" is suggested.	Header deleted since the subsequent paragraph is IAM-related	Yes
178	Contract customisation	ECIIA we suggest the following change in the sentence "The ECB considers it good practice for institutions to agree individual clauses with the CSP regarding the configuration of the cloud environment"	Amended to: “when entering into a cloud outsourcing arrangement”.	Yes
179	Identity and access management	ECIIA "monitoring tools" should become "monitoring „and logging“ tools"	Amended: “monitoring” replaced with “monitoring and logging tools”.	Yes
201	Protection of data	BSI In the second bullet point, please refer to contemporary standards for cryptographic algorithms, key-lengths, etc.. Otherwise this is to vague and lead to more questions. E.g. the technical guidelines from the German BSI are updated on an annual basis and can be found here: https://www.bsi.bund.de/dok/TR-02102-en Please add them inline or as a footnote	Reference to contemporary standards has been added.	Yes
202	Protection of data	BSI Please add the following sentence at the end of the first paragraph: "If the institution is already working in other countries (even outside the EU), then using a CSP in that country normally does not lead to much more additional threats since that institution is already forced to comply with local laws so that search warrants, law suits etc that may apply to the CSP will also apply to the institution itself."	Although it is true that financial entities working in other countries should already have assessed the risk stemming from such geographical implantation, outsourcing to CSPs should be subject to a specific risk assessment.	No
203	Identity and access management	BSI It is unclear to me what is the content of the individual clauses the institution shall agree with the CSP. Normally, the CSP provides the Self-Service-Portal for all users and the institution can configure the service as they wish without personal interaction with the CSP. Please clarify what is meant here	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity’s IT policies and defined shared responsibilities with the provider.	Yes
204	Protection of privileged accounts	BSI Please add another bullet point reading: "Usage of privileged access to institutions workload shall (where technically feasible) be monitored and the monitoring data shall be continuously analysed for indicators of compromise. Such findings shall trigger Security alarms.	First bullet point split to incorporate the proposal.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
234	Encryption requirements	ABI – Italian Banking Association The statement regarding data protection by means of high-end data encryption seems to be a brand new requirement. We propose to remove the sentence " institutions are required to implement protection measures involving cryptographic keys whereby data are encrypted on the basis of approved data classification and ICT risk assessment processes."	The ECB Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
235	Protection of data	ABI – Italian Banking Association The statement regarding data location restriction is a good practice, it should be specified that it's a suggestion and not an obligation	The ECB believes that the term “good practice” should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	Yes
236	Protection of data	ABI – Italian Banking Association With reference to envisaged "good practice for institutions to restrict the locations where CSPs can store their data" it has to be noted that when dealing directly with a CSP - as opposed to a TPP - the location is usually an institution's own choice. It should be clarified how should this aspect be weighted against considerations of geographical concentration.	Both the supervisory expectation to restrict the locations where CSPs can store data and the need to manage geographical concentration risks must be carefully balanced. When dealing directly with a CSP, supervised entities have indeed the flexibility to choose the data storage location. However, this choice must be made with an awareness of potential geographical concentration risks. To mitigate these risks, it is essential to ensure that data location decisions align with both security practices and geographical risk management strategies, as outlined in the Guide.	No
237	Encryption requirements	ABI – Italian Banking Association The statement regarding data encryption policies and procedures is seems to be a brand new requirement. We propose to remove the following sentence "Detailed policies and procedures are in place governing the entire lifecycle of encrypted data (i.e. generation, storage, usage, revocation, expiry and renewal), as well as the archiving of cryptographic keys, including a key access justification process that has the characteristics identified Article 9(3) of DORA".	The ECB Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
238	Protection of data	ABI – Italian Banking Association "In addition to encryption technology, institutions may also (i) use multi-cloud technologies that enhance their data security, (ii) apply micro-segmentation technologies or (iii) adopt other data loss prevention measures." We would welcome further clarification on how the listed security measures could act to strengthen data security on cloud environment.	These measures are those generally put forward by the industry when addressing data protection.	No
239	Protection of data	ABI – Italian Banking Association The statement regarding acceptable countries list in terms of data processing locations is not acceptable, such a list must be defined by regulators	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission’s proposed list may serve as a useful guide in this respect.	No
240	Protection of data	ABI – Italian Banking Association The statement regarding sub-contractor risk assessment is a good practice, it should be specified that it's a suggestion and not an obligation	The ECB believes that the term “good practice” should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			considering the matter based on a risk-based approach.	
241	Encryption requirements	ABI – Italian Banking Association The statement regarding ICT asset classification policy adoption seems to be a brand new requirement. We propose to remove the following " This policy should be applied by the institution in every case and should support the institution's ability to assess and determine the controls that are necessary to ensure the confidentiality, integrity and availability of data, regardless of where the data are stored and processed."	ICT assets list and classification is not a new requirement. It is present in the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and in Article 8(1) of DORA.	No
242	Asset identification	ABI – Italian Banking Association Clarification is needed from the ECB definition of an ICT asset within Cloud services, in relation to the provision: "The ECB considers it good practice for institutions to adopt a clear policy on the classification of all ICT assets, including those that are outsourced to CSPs."	The entity should consider all the ICT assets it is responsible for, depending on the deployment model and the sharing of responsibilities between the entity and the CSP..	No
243	Asset identification	ABI – Italian Banking Association A definition of Outsourced Asset is required: the Guidelines on Outsourcing cover the outsourcing of "processes" or "functions", it is unclear what cloud service would constitute an asset, what would be considered different assets of the same kind or different types of assets, especially regarding the adoption of SaaS products or that of serverless services	The definition of "ICT asset" has been aligned with DORA.	Yes
244	Contract customisation	ABI – Italian Banking Association "The ECB considers it good practice for institutions to agree individual clauses with the CSP when configuring the cloud environment." the following change is proposed: "The ECB considers it good practice for institutions to agree individual clauses with the CSP regarding the configuration of the cloud environment"	Amended to: "when entering into a cloud outsourcing arrangement".	Yes
245	Segregation of duties	ABI – Italian Banking Association The ECB states: "the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties". The Guide should specify that this expectation is focused specifically on Identity and access management (IAM)	Amended to: "… how the IAM structure provided by the CSP for the cloud services ...".	Yes
246	Protection of privileged accounts	ABI – Italian Banking Association With reference to the sentence "Users - especially those with privileged access to the system - should be clearly identified and should always be authenticated using a strong authentication solution.", changing as follow is proposed: "When accessing to services classified as critical, users - especially those with privileged access to the system - should be clearly identified and should always be authenticated using a strong authentication solution.", in order to explicitly require the strong authentication only for privileged access or access to the services classified as critical	The paragraph has been rephrased to consider its applicability for systems supporting critical or important functions.	Yes
269	Encryption requirements	Banking and Payment Federation Ireland (BPFI) Article 9 of DORA requires firms to use ICT solutions and processes to: (a) ensure the security of the means of transfer of data; (b) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity; (c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data; (d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error. While we agree with the ECB that institutions need to protect their data, we would note that DORA very specifically does not set specific requirements for the encryption of data. Furthermore, the ESAs' final technical standards on the ICT Risk Management framework establish that institutions should have a policy on encryption and cryptographic controls, designed on data classification and ICT risk assessments, and which should include rules for the encryption of data at rest, in transit and in use, where necessary. It specifically	This part has been changed to include reference to a risk-based approach.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		acknowledges that the encryption of data in use may not be possible, and that other measures may be used to protect data in use instead. The ECB's interpretation fails to take into account firms' assessment of the ICT risks associated with the data, and its classification. There are significant technical limitations for the encryption of data at rest and in use, and our view is aligned with that of both DORA and the ESAs in that firms should select the data protection controls based on the data and risks in question, rather than be required to apply specific controls across all data. The Guide states that, in order to have ICT security within the cloud, that a financial entity should encrypt data "in transit, at rest and, where feasible, in use." IaaS providers automatically de-crypt data once a user has access to the particular workload in question. Encryption, in this respect, serves no ICT security benefit. The cybersecurity risk associated with encryption from a IaaS perspective relates to access management controls, to which a malicious actor could gain access and would also receive automatic decrypted data. The only security benefit to encryption in an IaaS context is in relation to physical security and a malicious actor stealing a specific physical disk from a server in the data centre of a cloud provider. This constitutes a level of information breach and sophistication that is unrealistic and inappropriate to account for within ECB Supervisory Guidance. We recommend this requirement is risk-based depending on the cloud service. 2.3: "encryption methods in line with the institution's data sensitivity classification policy, the type of cloud service and a risk-based approach." The monitoring of the location of a financial entity's data in a CSP via tracing is not possible in all circumstances. A financial entities data is stored in a CSP's multi-tenant environment whereby the entity, or any other individual or commercial actor, temporarily uses a particular instance that can constantly shift. No entity has the ability to monitor the entirety of a CSP's shared environment and this would constitute monitoring of all other providers that are utilizing that particular CSP. This would be overly burdensome and a disproportionate requirement that is outside of the capability of one financial entity. We recommend monitoring of the use of data is based on a risk-based approach where it is technically feasible to achieve, potentially supported by firms establishing contractual restrictions on the locations which may be used to store the data and to require CSPs to attest to their compliance with these requirements		
270	Protection of data	Banking and Payment Federation Ireland (BPFI) The requirements in this section appear duplicative with the data security measures covered under the technical standards developed by the ESAs as part of their mandate under DORA, in particular Articles 6 and 7. We would suggest that the ECB avoid duplication of requirements to reduce the risk of conflicting requirements and disconnect between the two sets of requirements should either be reviewed in the future.	The measures listed in the document should be understood as good practice, deriving directly from DORA requirements. Therefore, they do not contradict the requirements of this text.	No
271	Protection of data	Banking and Payment Federation Ireland (BPFI) The Guide should not be prescriptive as to how financial entities manage location of data processing and storage risks including, for example, by drawing up a list of acceptable countries. Rather, it is common practice for firms to determine the locations in which their data can be stored or processed by their third parties. However, the creation of a list of "acceptable countries" is a crude method to approach this. Instead, institutions should assess the locations in which their data can be stored or processed on a case-by-case basis when entering into an agreement with a third party, based on the institution's assessment of the relevant risks and in line with applicable legal and regulatory requirements regarding the transfer of data (such as GDPR and Schrems), with any subsequent proposed change by that third party being subject to risk assessment and agreement by the institution. Regarding the use of subcontractors, this is a topic on which the ESAs are developing detailed requirements as part of their mandate under DORA, which will be subject to review and adoption by the European Commission and subsequent review by the co-legislators. We would encourage the ECB to avoid	Provision for a risk-based approach has been added. The ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission's proposed list may serve as a useful guide in this respect.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		pre-empting these formal standards to reduce the risk of conflicting or overlapping requirements. More specifically, the ECB's proposals fail to take into account consideration of materiality, criticality or risk associated with these subcontractors. The assessment of all subcontractors across all CSPs would be extremely onerous and disproportionate to the risks associated with those subcontractors. While the final technical standards are still in development, the requirements in relation to subcontractors are limited to where the TPP provides ICT services supporting Critical or Important Functions (CIFs), and we understand that the ESAs intend to further specify their requirements to those subcontractors which materially underpin those CIFs. Consideration of risks is a fundamental element of risk management frameworks, and should be incorporated as appropriate for all measures.		
272	Assets identification	Banking and Payment Federation Ireland (BPFI) The Guide refers to "As part of this practice, an institution should, as a matter of best practice, maintain an up-to-date inventory of all the ICT assets it is responsible for under the policy, in order to ensure that all operational processes (monitoring, patching, incident management, change management, etc.) are extended to cover cloud assets." This would suggest given the definition provided in the document that an ICT asset consists of a software or hardware asset that is found in the business environment that there is an expectation that the institution includes CSP software and hardware assets supporting its services in its own ICT. Are we reading this correctly? This does not seem in line with the realities of how cloud resources work. In general, an institution contracts based on usage, not underlying infrastructure. The individual ICT assets, and indeed the total assets involved, will be highly dynamic. While it may be technically feasible to establish a dynamic tracking of which ICT assets are being used by a given institution at any time, the complexity and costs would be enormous, with no discernible benefits beyond the existing available information regarding firms agreed available capacity.	The Guide refers to all the ICT assets the entity is responsible for, depending on the deployment model and on how responsibilities are shared between the entity and the CSP.	No
312	Identity and access management	European Cloud User Coalition (ECUC) Could you please clarify what the mentioned "individual clauses" would cover.	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider.	Yes
314	Protection of data	International Business Machines Corporation The "list of acceptable countries where … data can be stored or processed" and the related footnote is an incomplete reference to EU data transfer law. IBM recommends more clearly aligning this statement with existing law, including for example the acceptability of using standard contractual clauses in lieu of an adequacy determination.	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission's proposed list may serve as a useful guide in this respect.	No
357	Encryption requirements	European Banking federation The statement regarding data protection by means of high-end data encryption seems to be a brand new requirement. We propose to remove the sentence " institutions are required to implement protection measures involving cryptographic keys whereby data are encrypted on the basis of approved data classification and ICT risk assessment processes."	The ECB Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
358	Protection of data	European Banking federation The statement regarding data location restriction is a good practice, it should be specified that it's a suggestion and not an obligation	The ECB believes that the term "good practice" should be treated as a suggestion that supervised entities are invited to follow, unless they	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			decide not to after duly considering the matter based on a risk-based approach.	
359	Protection of data	European Banking federation With reference to envisaged "good practice for institutions to restrict the locations where CSPs can store their data" it has to be noted that when dealing directly with a CSP - as opposed to a TPP - the location is usually an institution's own choice. It should be clarified how should this aspect be weighted against considerations of geographical concentration.	Both the supervisory expectation to restrict the locations where CSPs can store data and the need to manage geographical concentration risks must be carefully balanced. When dealing directly with a CSP, supervised entities have indeed the flexibility to choose the data storage location. However, this choice must be made with an awareness of potential geographical concentration risks. To mitigate these risks, it is essential to ensure that data location decisions align with both security practices and geographical risk management strategies, as outlined in the Guide.	No
360	Encryption requirements	European Banking federation The statement regarding data encryption policies and procedures is seems to be a brand new requirement. We propose to remove the following sentence "Detailed policies and procedures are in place governing the entire lifecycle of encrypted data (i.e. generation, storage, usage, revocation, expiry and renewal), as well as the archiving of cryptographic keys, including a key access justification process that has the characteristics identified Article 9(3) of DORA".	The ECB Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	No
361	Protection of data	European Banking federation "In addition to encryption technology, institutions may also (i) use multi-cloud technologies that enhance their data security, (ii) apply micro-segmentation technologies or (iii) adopt other data loss prevention measures." We would welcome further clarification on how the listed security measures could act to strengthen data security on cloud environment.	These measures are those generally put forward by the industry when addressing data protection.	No
362	Protection of data	European Banking federation The statement regarding acceptable countries list in terms of data processing locations is not acceptable, such a list must be defined by regulators	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission’s proposed list may serve as a useful guide in this respect.	No
363	Protection of data	European Banking federation The statement regarding sub-contractor risk assessment is a good practice, it should be specified that it's a suggestion and not an obligation	The ECB believes that the term “good practice” should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	No
364	Asset identification	European Banking federation The statement regarding ICT asset classification policy adoption seems to be a brand new requirement. We propose to remove the following " This policy should be applied by the institution in every case and should support the institution’s ability to assess and determine the controls that are necessary to ensure the confidentiality, integrity and availability of data, regardless of where the data are stored and processed."	The ICT assets list and classification is not a new requirement. It is in the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and in Article 8(1) of DORA.	No
365	Asset identification	European Banking federation Clarification is needed from the ECB definition of an ICT asset within Cloud services, in relation to the provision: "The ECB considers it good practice for institutions to adopt a	The entity should consider all the ICT assets it is responsible for, depending on the deployment model and the sharing of	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		clear policy on the classification of all ICT assets, including those that are outsourced to CSPs."	responsibilities between the entity and the CSP.	
366	Contract customisation	European Banking federation "The ECB considers it good practice for institutions to agree individual clauses with the CSP when configuring the cloud environment." the following change is proposed: "The ECB considers it good practice for institutions to agree individual clauses with the CSP regarding the configuration of the cloud environment"	Amended to: “when entering into a cloud outsourcing arrangement”.	Yes
367	Segregation of duties	European Banking federation The ECB states: "the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution’s roles and responsibilities to ensure the effective segregation of duties". The Guide should specify that this expectation is focused specifically on Identity and access management (IAM)	Amended to:“… how the IAM structure provided by the CSP for the cloud services …”.	Yes
368	Protection of privileged accounts	European Banking federation With reference to the sentence "Users - especially those with privileged access to the system - should be clearly identified and should always be authenticated using a strong authentication solution.", changing as follow is proposed: "When accessing to services classified as critical, users - especially those with privileged access to the system - should be clearly identified and should always be authenticated using a strong authentication solution.", in order to explicitly require the strong authentication only for privileged access or access to the services classified as critical	The paragraph has been rephrased to consider its applicability for systems supporting critical or important functions.	Yes
441	Protection of data	Dutch Banking Federation (DBF) The lifecycle approach to data encryption is already at risk of becoming out-of-date, and goes beyond the lifecycle stages referenced in DORA. And we fail to see how the following would strengthen data security in the cloud: "In addition to encryption technology, institutions may also (i) use multi-cloud technologies that enhance their data security, (ii) apply micro-segmentation technologies or (iii) adopt other data loss prevention measures." The guidance should enable firms to take their own risk-based approach, recognising that increasing the number of technologies also increases the number of interfaces which could be exposed. Furthermore at this moment detailed policies and procedures are in place governing the entire lifecycle of encrypted data (i.e. generation, storage, usage, revocation, expiry and renewal).	These measures are those generally put forward by the industry when addressing data protection issues. However, the term “micro-segmentation” has been amended. Additionally, the reference to a risk-based approach has been added earlier in the chapter.	Yes
442	Protection of data	Dutch Banking Federation (DBF) In our opinion the statement that "Institutions that outsource to the cloud continue to own their data. For that reason, it is good practice for institutions to restrict the locations where CSPs can store their data and apply appropriate tracing mechanisms to monitor compliance with those restrictions, while also ensuring that data can be accessed when needed." , restricts the bank from using CSP services.	The ECB understands the concern that restricting the locations where CSPs can store data might seem to limit the bank’s use of CSP services. However, these restrictions are essential for ensuring that the supervised entity maintains full control over its data and complies with regulatory requirements. Rather than limiting the bank’s use of CSPs, these practices empower the bank to leverage cloud services securely and effectively, thus safeguarding sensitive information while ensuring accessibility and compliance.	No
443	Protection of data	Dutch Banking Federation (DBF) "Institutions that outsource to the cloud continue to own their data". This is a legal discussion: ownership of data can be contractually taken care of, but local laws (such as insolvency) can impact such contractual ownership.	While the ECB acknowledges that data ownership in the context of cloud outsourcing involves complex legal considerations, the statement that “supervised entities that outsource to the cloud continue to own their data” remains a crucial point. It underscores the fundamental principle that	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			ownership does not automatically transfer to CSPs. Although local laws and specific scenarios, such as insolvency, may affect this ownership, these are exceptions that can be addressed through robust contractual agreements. Therefore, the ECB believes this statement should be retained to reinforce the supervised entity's control over its data.	
444	Protection of networks	Dutch Banking Federation (DBF) We would like to have more clarity on what is meant with "are warranted" in this context.	Please read this sentence as: When supervised entities connect their internal systems to cloud-based applications, they are expanding their secure areas to include the cloud. In such cases, it is important to carefully assess the risks and make informed decisions about managing these risks. This process should also consider the requirements outlined in Article 9 of DORA.	Yes
445	Governance framework	Dutch Banking Federation (DBF) Although several security measures are mentioned we suggest to make a reference to the internal governance framework with which the control on on-prem devops is managed. This provides the opportunity to focus on the specific cloud risks and measures.	This suggestion has been added as a new paragraph at the end of Section 2.3.	Yes
446	Protection of data	Dutch Banking Federation (DBF) To avoid misinterpretation and ambiguity we advice to delete the application of micro segmentation and multi-cloud technologies in this pragraph because it is in our opinion neither encryption related nor enhancing data security.	These measures are those generally put forward by the industry when addressing data protection issues. The term "micro-segmentation" has been amended.	Yes
447	Protection of data	Dutch Banking Federation (DBF) We ask for clarification on which risk is mitigated because data protection can be achieved and managed through different measures, e.g. IAM but also encryption in which the vendor has a major role and embeds a risk based approach.	These measures are those generally put forward by the industry when addressing data protection issues. Additionally, the reference to a risk-based approach has been added earlier in the chapter.	Yes
448	Protection of data	Dutch Banking Federation (DBF) The recommendation should be a list of unacceptable countries based on the firm's risk management practices, rather than a list of acceptable countries. If the aim is to ensure that FIs are aware of data processing and storage requirements across jurisdictions, the ECB should not prescribe the method (e.g. list of acceptable or unacceptable countries) by which an FI conducts this.	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission's proposed list may serve as a useful guide in this respect.	No
449	Protection of data	Dutch Banking Federation (DBF) The risk of litigation is not clear with regard to "Legal and political risks". Does it refer to the risk that contracts are not enforceable in a court of law because the rule of law does not provide for short term proceedings to obtain intermediate measures timely? We assume institutions should also take into account laws hindering transferring the data out of a country and data privacy related risks?	The ECB believes that both risks should be taken into account in the risk-based approach.	No
450	Assets identification	Dutch Banking Federation (DBF) We recommend to add in this paragraph the Self Build Applications on platforms next to the classification of ICT	Self-build applications are part of the software considered in the definition	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		assets outsourced to CSP's as these also need to be classified and registered.	of “ICT asset” provided in paragraph 1.1.	
451	Asset identification	Dutch Banking Federation (DBF) We ask for clarification as to whether our takeaway is correct that the inventory of all ICT assets seems contrary to its Cloud-based scope.	This paragraph refers to all the ICT assets the entity is responsible for, depending on the deployment model and on how responsibilities are shared between the entity and the CSP.	No
452	Protection of data	Dutch Banking Federation (DBF) The requirement for individual clauses should be deleted. This guidance should focus on what is substantively required, and refrain from prescribing the format, i.e. by saying "Financial entities should their practices address…" This approach is inconsistent with the existing EBA approach to date and is going beyond the DORA obligations in prescribing the form as well as substance. .	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity’s IT policies and defined shared responsibilities with the provider.	Yes
453	Protection of privileged accounts	Dutch Banking Federation (DBF) We recommend to delete or rephrase the requirement "if a CSP has access to any of the institution’s systems or data, this should be properly documented and monitored using appropriate monitoring tools (which should also be reviewed on a regular basis)", because in some cases it is not possible to review the CSPs monitoring tools.	Proposed amendment “whenever feasible” added	Yes
454	Protection of data	Dutch Banking Federation (DBF) Does the requirement for monitoring include that the subject institution is to monitor the usage of tooling that may be in place within the CSP to comply with legal requirements of the CSPs native country? Especially considering such requests may come with secrecy ("gag") orders and providing such monitoring insights to their customers may be not be allowed under their native countries' national laws. Would the ECB expect the CSPs not agreeing to this rule be grounds for exiting the cloud agreement?	Monitoring of the CSP is expected whenever possible, in accordance with applicable law and regulations.	Yes
486	Legal basis	DIGITALEUROPE Delete reference to NIS 2 (as well as on pages 6 and 7).	All references to the NIS 2 Directive have been removed from the Guide.	Yes
488		DIGITALEUROPE [Empty comment]	N/A	No
489	Protection of data	DIGITALEUROPE DORA does not require financial entities to use a multi- vendor strategy. Art. 6(9) DORA explicitly notes that the use of a multi-vendor strategy is optional rather than mandated. Affirmatively linking a multi-vendor strategy with increased security appears to contradict DORA as it implies this approach is mandatory. It is also unsubstantiated. When not properly managed a multi-vendor strategy can increase security risks. proposed sub-subsection 2.3.1 uses the phrase 'micro-segmentation technologies' without defining the term, which is likely to cause confusion for financial entities and providers. If proposed sub-subsection 2.3.1 is intended to be aligned with DORA, the term should be revised to either use a commonly understood term within the industry or a term that is defined or understood within DORA. Hence, 2.3.1 in the Guide should be AMENDED to DELETE: 'IN ADDITION TO ENCRYPTION TECHNOLOGY, INSTITUTIONS MAY ALSO (I) USE MULTI-CLOUD TECHNOLOGIES THAT ENHANCE THEIR DATA SECURITY, (II) APPLY MICRO-SEGMENTATION TECHNOLOGIES OR (III) ADOPT OTHER DATA LOSS PREVENTION MEASURES'.	The measures listed in the document should be understood as good practice, deriving directly from DORA requirements. Additionally, these measures are those generally put forward by the industry when addressing data protection issues.	No
490	Protection of data	DIGITALEUROPE We would challenge and delete the 'advice' mentioned in the first paragraph ('Institutions are advised, therefore, to draw up a list of acceptable countries where their data can be stored and processed, depending on the data in question. That Assessment should ideally take account of legal and political risks surrounding outsourcing (e.g. the risk of litigation or sanctions'.)	On the contrary, the ECB believes that it is up to the supervised entities to draw up a list of acceptable countries for the storage and processing of their data, following their evaluation of the risks and in compliance with prevailing regulations. The European Commission’s proposed list may serve as a	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			useful guide in this respect.	
491	Identity and access management	DIGITALEUROPE The second paragraph of 2.3.4 should be amended as follows: An institution's IAM policy should be extended to cover cloud assets and IMPLEMENTED EXECUTED when entering into a cloud outsourcing arrangement. This policy should cover both technical and business users	The paragraph has been rephrased to consider its applicability for systems supporting critical or important functions.	Yes
492	Identity and access management	DIGITALEUROPE As drafted, 2.3.4.1 introduces requirements that are not included in DORA, but also will not increase the resiliency of financial entities. Sub-subsection 2.3.4.1 should be DELETED. The section should be deleted, or, as a minimum, 2.3.4.1 should be clarified as follows: The ECB considers it good practice for institutions to CONSIDERAGREE individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT CONFIGURING THE CLOUD ENVIRONMENT. If this is not feasible, the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties. Any deviations can then be analysed and addressed using risk mitigation measures.	Clarification required on "individual clauses". Proposed amendment agreed: "The ECB considers it good practice for supervised entities to CONSIDER individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT."	Yes
554	Encryption requirements	European Association of Public Banks The level of "best practice" is inadequately high especially with regards to cryptographic keys. There are additional means of a similar level of security "Best practice" should be replaced by "exemplary measures".	The ECB believes network protection should be one layer of in-depth protection. Micro-segmentation – while desirable -should be completed with data encryption wherever possible, as outlined in Section 2.3.1 of the Guide.	No
555	Exercise of audit rights	European Association of Public Banks „Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements."	As set out in paragraph 2.5, supervised entities are encouraged to work together when auditing a CSP.	No
556	Asset identification	European Association of Public Banks "Classification of all ICT assets" in an up-to-date inventory does not reflect enough the criticality and creates an inappropriate burden. We suggest to include a risk-based approach.	The entity should consider all the ICT assets it is responsible for, depending on the deployment model and the sharing of responsibilities between the entity and the CSP.	No
557	Asset identification	European Association of Public Banks The inventory of all ICT assets appears at odds with the Cloud based scope of this guidance.	The scope of the guidance is cloud services, while the Guide refers to all ICT assets the entity is responsible for, depending on the deployment model and on how responsibilities are shared between the entity and the CSP.	No
558	Identity and access management	European Association of Public Banks Given the highly standardized nature of cloud environments, agreeing individual clauses (2.3.4.1.) is likely only possible for a few select key institutions, but not the industry as a whole.	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider.	Yes
559	Segregation of duties	European Association of Public Banks Risk mitigation of any deviations within this context appears to be a level of scrutiny that exceeds previous expectations, therefore we suggest limiting this to necessary instances.	Amended to: "Any deviations from the effective segregation of duties can then be analysed and addressed using risk mitigation measures on a risk-based approach".	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
560	Identity and access management	European Association of Public Banks It may be viable to compare this requirement to standard privileged access management procedures. It should be sufficient that the IAM policy is reflecting cloud outsourcing and is regularly reviewed in the outsourcing agreement	While user roles and access implementation may change frequently, IAM policies should contain applicable principles and remain stable over time. Not amended.	No
561	Protection of data	European Association of Public Banks The requirement for individual clauses should be deleted. The guidance should focus on what is substantively required, and refrain from prescribing the format, i.e. by saying "Financial entities should their practices address…" This approach is at odds with the existing EBA approach to date.	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider.	Yes
562	Identity and access management	European Association of Public Banks "agree on individual clauses" Please clarify what is meant by clauses. Typically, an institution will negotiate its own contract with the CSP on the basis of the terms of the CSP or the institution. Such contract can be used by the institution as well as its affiliates and subsidiaries.	The proposal was not meant to refer to individually tailored clauses. The paragraph has been amended to reflect the expectations of a contractual agreement in line with the entity's IT policies and defined shared responsibilities with the provider.	Yes
592	Identity and access management	Google Cloud The reference to "executing" IAM policies in Section 2.3.4 is unclear. The text should be clarified as follows: An institution's IAM policy should be extended to cover cloud assets and IMPLEMENTED [DELETE: executed] when entering into a cloud outsourcing arrangement. This policy should cover both technical and business users	The ECB agrees: "executed" replaced with "implemented".	Yes
593	Identity and access management	Google Cloud It is not practical or necessary for institutions to agree individual clauses with the CSP on a configuration-by-configuration basis. The text should be amended as follows: The ECB considers it good practice for institutions to CONSIDER [DELETE: agree] individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT [DELETE: configuring the cloud environment].	Clarification required on "individual clauses". Proposed amendment agreed: "The ECB considers it good practice for supervised entities to CONSIDER individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT."	Yes
621	Protection of data	Bitkom 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	This part is to be understood as an enumeration of possible measures for safeguarding data. Each financial entity is free to implement the measures it chooses, as long as they satisfy the requirements of Article 9 of DORA.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
622	Protection of data	Bitkom 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 term “micro-segmentation” has been replaced with “adequate network segmentation”.	Yes
623	Protection of data	Bitkom 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.”	These measures are those generally put forward by the industry when addressing data protection issues. However the term “micro-segmentation” has been amended. Additionally, reference to a risk-based approach has been added.	Yes
624	Protection of data	Bitkom "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?	The text has been amended and now reads: “The security and accuracy of data in transit and data at rest are key requirements when relying on cloud-based services, including cloud infrastructure.”	Yes
625	Protection of data	Bitkom "… 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?	Any sub-contractor, whether or not intra-group to the CSP, will be considered as far as the services provided to the entity are concerned.	No
626	Identity and access management	Bitkom 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”	The ECB agrees to align the wording with the DORA definition.	Yes
627	Contract customisation	Bitkom 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	As CSPs can change their offer at will, and because having a contract helps to mitigate the associated risks, the ECB considers it useful for a bank to have safeguards in the form of contractual clauses.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
628	Protection of privileged accounts	Bitkom "Users – especially those with privileged access to the system …" Users on the FE - and/or Users of the CSP? Please clarify.	Amended. "Users" replaced with "FE's users".	Yes
651	Encryption requirements	Futures Industry Association (FIA) The Guide creates interpretation issues by inconsistently applying expectations for outsourced cloud services that support Critical or Important Functions (CIFs) in certain chapters and not in others. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform "spot checks" across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. As cloud technologies cover a significant array of outsourced activities, this would constitute a vast level of operational change with limited benefit nor recognition of effective risk management practices. We recommend that the ECB includes a more detailed proportionality principle that applies to all Chapters or is more specific concerning their expectation for cloud outsourcing as it relates to CIFs. The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity's technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU's Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute "significant interference in the data, digital assets or service architecture." This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide.	The text has been amended to include a clear reference to a risk-based approach, which addresses both remarks. Specific expectations may not apply to all different types of cloud services, or switching back to on-premise may not be feasible using the exact same technology. However, FEs should analyse the risk of failure or unavailability of the services, and have adequate disaster recovery procedures designed and tested.	Yes
652	Encryption requirements	Futures Industry Association (FIA) The Guide creates interpretation issues by inconsistently applying expectations for outsourced cloud services that support Critical or Important Functions (CIFs) in certain chapters and not in others. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform "spot checks" across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. As cloud technologies cover a significant array of outsourced activities, this would constitute a vast level of operational change with limited benefit nor recognition of effective risk management practices. We recommend that the ECB includes a more detailed proportionality principle that	The text has been amended to include a clear reference to a risk-based approach, which addresses both remarks. Specific expectations may not apply to all different types of cloud services, or switching back to on-premise may not be feasible using the exact same technology. However, FEs should analyse the risk of failure or unavailability of the services, and have adequate disaster recovery procedures designed and tested.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		applies to all Chapters or is more specific concerning their expectation for cloud outsourcing as it relates to CIFs. The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity's technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU's Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute "significant interference in the data, digital assets or service architecture." This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide.		
656	Legal basis	Futures Industry Association (FIA) The Guide includes multiple references to the NIS2 Directive when informing the ECB's supervisory expectations, despite DORA being confirmed as lex specialis to NIS2, which will cause interpretation concerns for the sector. References are included in 2.2.1, 2.2.3, and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management), and all refer to requirements in NIS2 that exist within DORA in a greater level of detail. DORA includes a Chapter (Chapter 6; Article 24-26) within the Risk Management Framework dedicated to business continuity plans and disaster recovery while the references to incident response and recovery are intrinsic to the RTS in its entirety. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. We recommend that all references to NIS2 are removed.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
663	Protection of data	Futures Industry Association (FIA) Recommended amendment: 2.3: "encryption methods in line with the institution's data sensitivity classification policy, the type of cloud service and a risk-based approach." The Guide states that, in order to have ICT security within the cloud, that a financial entity should encrypt data "in transit, at rest and, where feasible, in use." IaaS providers automatically de-crypt data once a user has access to the particular workload in question. Encryption, in this respect, serves no ICT security benefit. The cybersecurity risk associated with encryption from a IaaS perspective relates to access management controls, to which a malicious actor could gain access and would also receive automatic decrypted data. The only security benefit to encryption in an IaaS context is in relation to physical security and a malicious actor stealing a specific physical disk from a server in the data centre of a cloud provider. This constitutes a level of information breach and sophistication that is unrealistic and inappropriate to account for within ECB Supervisory Guidance. We recommend this requirement is risk-based depending on the cloud service.	This part has been changed to include reference to a risk-based approach and therefore read: "encryption methods in line with the supervised entity's data sensitivity classification policy and following a risk-based approach."	Yes
664	Protection of data	Futures Industry Association (FIA) Data location and processing risks are assessed on a risk-based approach, including in respect of risk-assessment of subcontractors "relevant for" the cloud service. This is vague and does not appropriately apply materiality to the risk management of subcontractors to CSPs. The guidance is too prescriptive and expands existing DORA and EBA requirements. Furthermore, the suggestion to "assess additional risks" is not helpful as it broadens the scope of risks to be considered without specifying objective criteria.	The risks stemming from the location and processing of data should be addressed in the risk analysis, and sub-outsourcings may introduce additional risk, depending on the potential additional location to be considered.	No
679	Encryption requirements	German Banking Industry Committee (GBIC) The level of "best practice" is inadequately high especially with regards to cryptographic keys, especially in the light that there are additional means of a similar level of security. "Best	The ECB believes network protection should be one layer of in-depth protection. Micro-segmentation – while desirable - should be	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		practice" should be replaced by “exemplary measures“	completed with data encryption wherever possible, as outlined in Section 2.3.1 of the Guide.	
680	Protection of data	German Banking Industry Committee (GBIC) "Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements." should be clarified in order to consider risk-orientation and proportionality.	The risk-based approach results from the processed data in scope and from the location of its storage and processing. Good practice refers to examples of effective practices by supervised entities observed during ongoing supervision as well as on-site inspections and should complement supervisory expectations.	No
681	Asset identification	German Banking Industry Committee (GBIC) "Classification of all ICT assets" in an up-to-date inventory does not reflect the criticality enough and creates an inappropriate burden. We suggest to include a risk-based approach.	The entity should consider all the ICT assets it is responsible for, depending on the deployment model and the sharing of responsibilities between the entity and the CSP.	No
682	Segregation of duties	German Banking Industry Committee (GBIC) Risk mitigation of any deviations within this context appears to be a level of scrutiny that exceeds previous expectations, therefore we suggest limiting this to necessary instances.	Amended to: “Any deviations from the effective segregation of duties can then be analysed and addressed using risk mitigation measures on a risk-based approach”.	No
683	Identity and access management	German Banking Industry Committee (GBIC) It may be viable to compare this requirement to standard privileged access management procedures. It should be sufficient that the IAM policy is reflecting cloud outsourcing and is regularly reviewed in the outsourcing agreement	While user roles and access implementation may change frequently, IAM policies should contain applicable principles and remain stable over time. Not amended.	No
695	Identity and access management	Austrian Federal Economic Chamber - Division Bank and Insurance 4. Standard of care Across the ECB guide (e.g. in para 2.3.4.1) ECB refers to certain measures as “good practice”. Usually, when describing implementation measures, reference is made to a “best practice” approach, i.e. a best case scenario. With the usage of “good practice”, it could now be understood that this is the “ordinary way” to implement / transpose ECB’s expectation, therefore making it a minimum standard of care. We therefore ask to overthink this increase of standard of care or otherwise provide a concrete definition what is meant under “good practice” (and “best practice”) from ECB point-of-view.	The ECB believes that the term “good practice” should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	Yes

2.5 Table 5 – Comments on Section 2.4: Exit strategy and termination rights

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
7	Termination rights	Deustche Börse Group Deutsche Börse Group would appreciate clarification in terms of whether termination of services due to external events such as "conflicting legislation" needs to be addressed in an exit strategy in the case CSP is an EU company.	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such confusion.	Yes
21	Termination rights	AWS 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 "other 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	Similar to other ECB Guides, this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations. The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 "Scope and effect": "[...] When applying these expectations, account should be taken of the principle of proportionality." The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in the regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The ECB has also clarified the expectation regarding "significant changes" or "other changes". The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
32	Cost for exit strategy	Nordea Abp Estimated cost for Exit strategies is a new requirement and not part of DORA as referenced, as this is a new requirement which adds further administrative burden, this should be analysed from cost and benefit perspective before adding a new layer on top of DORA requirements or exit strategies and plans and their testing.	The statement is already contemplated in EBA/GL/2019/02 on outsourcing arrangements and the ECB considers it part of a comprehensive and documented plan according to Article 28(8) of DORA.	No
33	Exit plan	Nordea Abp We strongly recommend to remove paragraph 2 as it appears to add new 3rd party risk management requirements specific to Cloud in addition to those defined in DORA in the main regulation and articles 28-30. These additional requirements are already covered in the general requirements for all 3rd parties and further specification would add disproportional complexity for only one type of outsourcing.	The ECB considers this statement to be in line with the provisions of Article 28(8) of DORA: "Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically." Meanwhile, the use of external is considered acceptable, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised institution. As a result, the Guide has been amended.	Yes
47	Termination rights	Association of German Public Banks The Guidance creates new additional termination rights which go beyond existing practice. The following should be deleted: "i) an excessive increase in expenses ii) relocation of business units or data centres iii) merger or sale iv) failure to successfully execute cloud provider test migrations at the agreed times."	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations. The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 "Scope and effect": "[...] When applying these expectations, account should be taken of the principle of proportionality." The Guide has been	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised institution to be bound to a contract if no specific regulation exists. The ECB has also clarified the expectation regarding “significant changes” or “other changes”. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	
48	Termination rights	Association of German Public Banks “2.4.1 (2) describes other changes that could also lead to such a reason for terminating for termination, including in particular (iv) relocation... and (vi) change in the regulations applicable... For iv)and iv) we suggest to add “unless the data is immediately transferred to a host country that also otherwise meets the requirements of the outsourcing agreement".	The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists.. The ECB has also clarified the expectation regarding “significant changes”.	Yes
49	Exit plan	Association of German Public Banks These interpretations go far beyond DORA, we suggest to be aligned with DORA. Art. 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	The ECB considers this statement to be in line with the provisions of Article 28(8) of DORA: “Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.” Meanwhile, the use of external resources is considered acceptable, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	Yes
68	Termination rights	ABBL – The Luxembourg Banker’s Association The Guide creates new additional termination rights which are too granular and go beyond existing regulatory expectations and contracting best practice. It would be unreasonable to expect the reasons for termination detailed in the guide to be reflected in contractual arrangements with CSPs. In particular, the Guide should not include the following: • excessive increase in expenses – This is subjective and does not reflect the reality of contracting, which would not allow unilateral changes to fees. • the relocation of business units or data centres – too granular. This would be captured by material breach	Similar to other ECB Guides, this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		termination rights, given existing outsourcing requirements, that providers seek FIs consent ahead of changing the service or data storage locations • changes to national legislation or regulations applicable to data location and processing – this would be covered by contractual rights to terminate for legal/regulatory reasons under the impediments capable of altering performance concept required by the EBA Guidelines • significant changes to the management of cyber risk in the subcontracting chain – this is covered by general termination rights related to subcontractors under EBA GLs and DORA • failure to successfully execute cloud provider test migrations at agreed times – too granular. It is unclear what the material risk is here and material breach termination rights would achieve the same outcome.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”: “[...] When applying these expectations, account should be taken of the principle of proportionality.” The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends t a supervised entity to be bound to a contract if no specific regulation exists. The ECB has also clarified the expectation regarding “significant changes” or “other changes”. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	
115	Termination rights	AFME The Guidance creates new additional termination rights which go beyond existing regulatory expectations and commercial practice and do not apply proportionality and risk-based principles. It would also be unreasonable for many of these to be detailed in the contractual arrangements with CSPs for example around an excessive increase in expenses. Additionally, the Guide incorporates grounds that are covered by Article 28 of DORA, but uses different terminologies. This adds unnecessary confusion and complexity to industry’s understanding and application of DORA. The first two paragraphs of paragraph 2.4.1 should be deleted. In the event they are not, the reference in any changes in cybersecurity obligations being cause for termination should be exchanged with violations to cybersecurity obligations. Regarding the ECB’s expectation that it should be possible to terminate only some of the services provided by a CSP, this is likely to be extremely difficult in practice. Many services provided by CSPs are highly intertwined and difficult to legally separate. We would welcome the ECB’s recognition that this would be beneficial where feasible, and acknowledgement that it may not be possible in the majority of cases.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”: “[...] When applying these expectations, account should be taken of the principle of proportionality.” The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The ECB has also clarified the expectation regarding “significant changes” or “other changes”. The Guide has been amended to align with the existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	
116	Sub-outsourcing	AFME Regarding the ECB’s proposals that “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”. This overlaps significantly with the technical standards being developed by the ESAs in their mandate under DORA on the subcontracting of critical or important functions. However, the ECB does not consider either the criticality of the service being provided by the CSP or the materiality of the services being provided to the CSP by its subcontractors. This creates an extension of scope which will capture fourth party providers who do not have any material impact on an FE's abilities to provide its services, for instance an institution’s catering supplier which uses cloud services for scheduling.	The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations.	Yes
117	Exit strategy	AFME With reference to the provision: "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." clarification is needed with respect to the meaning of "principle-based"	The term “principle-based” used in the draft Guide was not clear. The Guide has been amended accordingly.	Yes
118	Exit plan	AFME This creates a subject matter expert dependency. To rebuild a service, and FE would need to have immediate access to SMEs who will be able to rebuild in a timely manner, or be allowed a feasible timeline to identify the right contact.	The ECB considers this statement to be in line with the provisions of Article 28(8) of DORA: “Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.” Meanwhile, the use of external resources is considered acceptable, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	Yes
119	Exit strategy	AFME The execution of exit plans is by nature an exceptional activity, and so often requires additional resources and capacity beyond those required for BAU activities. As such many exit plans involve the hiring of professional services and / or contractors to augment the institutions’ normal staff. The ECB’s proposed requirement for institutions to check that they have the personnel required for their exit plans could be interpreted to require institutions to maintain sufficient staff to execute against exit plans on a full-time basis, which would be an egregious additional cost beyond what is required for BAU activities. We would propose that the ECB amend this section to read: Institutions should check that they have the personnel	The ECB considers this statement to be in line with the provisions of Article 28(8) of DORA: “Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically.” Meanwhile, the use of external resources is considered acceptable,	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		required for their exit plans, or a plan for the additional staff which would be required and, by conducting a walkthrough of the tasks involved, ensure that the planned staff available are would be able to perform the proposed tasks outlined in the exit plan.	bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended."	
120	Scope	AFME The Guide does not apply an explicitly proportionate and risk-based approach to exit requirements by failing to limit expectations to services supporting CIFs to ensure the feasibility of the guidance.	The ECB limits the expectations to critical or important functions, as DORA delimits exit strategies to critical or important functions only and refers to general comments. The Guide has been amended.	Yes
121	Termination rights	AFME The reference to conflicting legislation appears to be referencing potential third country sanctions. This should be dealt with separately.	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes The Guide has been amended to avoid such confusion.	Yes
140	Termination rights	American Chamber of Commerce to the European Union Article 2.4.1 contains additional grounds of termination and termination scenarios that overlap with, conflict with and exceed the grounds of termination in Article 28(7) of DORA.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes
180	Termination rights	ECIIA The ECB should better clarify its expectations regarding the exit plans tests that must be carried out. On many occasions it is really difficult to establish very large service tests, not only because of the complexity of organizing and executing them, but also because of their cost. It would be convenient for them to establish what type of tests they require/best practices.	The ECB has reviewed the reasons for termination to align with the provisions of DORA. Point (ix) has been retained to emphasise that the ECB expects exit strategy tests to be conducted.	Yes
181	Exit strategy	ECIIA With reference to the provision "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", clarification is needed with respect to the meaning of "principle-based".	The term “principle-based” used in the draft Guide was not clear. The Guide has been amended accordingly.	Yes
182	Termination rights	ECIIA "Other changes that could also lead to such a reason for termination include [...] (vii) continuous failure to achieve agreed service levels or a substantial loss of service, and (ix) a failure to successfully execute cloud provider test migrations at the agreed times". The last two points are not classifiable as "changes" but they are specific condition. We deem necessary to separate them from the previous termination reasons. More appropriate would be "Other reasons for termination include (i)"	The ECB has reviewed the reasons for termination to align with the provisions of DORA. Point (ix) has been retained to emphasise that the ECB expects exit strategy tests to be conducted.	Yes
183	Termination rights	ECIIA "to any deterioration" is too expansive and should be replaced	Article 28(8) of DORA does not limit the scope of exit	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		by "major/significant"	strategies to material deterioration. "For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, […], a deterioration of the quality of the ICT services provided […]".	
184	Business continuity and exit strategy	ECIIA The paragraph 2.4.4 collapses Business Continuity and Exit Strategy considerations and introduces the concept of an "exit under stress or an exit without the cooperation of the CSP(s)". We believe this requirement is quite impossible to be respected, a recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort."	The ECB recommends a supervised entity to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations.	No
247	Exit strategy	ABI – Italian Banking Association With reference to the provision: "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." Clarification is needed with respect to the meaning of "principle-based"	The term "principle-based" used in the draft Guide was not clear. The Guide has been amended accordingly.	Yes
248	Exit strategy	ABI – Italian Banking Association The statement regarding exit strategy definition on outsourced cloud services performing critical or important functions seems to be a brand new requirement. We propose to remove: "Exit strategies with clearly defined roles and responsibilities and estimated costs should be drawn up for all outsourced cloud services performing critical or important functions before those systems go live, and the time required to exit should be in line with the transition period indicated in the relevant contractual agreement"	The statement is already contemplated in EBA/GL/2019/02 on outsourcing arrangements and the ECB considers it part of a comprehensive and documented plan according to Article 28(8) of DORA.	No
249	Subcontractors Cybersecurity risk	ABI – Italian Banking Association With reference to the sentence "(vii) significant changes to the management of cybersecurity risk in the chain of sub-contractors,", the proposal is to generalize the requirement as follow: "(vII) violation of the cybersecurity obligations indicated in the contractual clauses, also with reference to the chain of sub-contractors"	The ECB has clarified the expectation regarding "significant changes".	Yes
250	Termination rights	ABI – Italian Banking Association "Other changes that could also lead to such a reason for termination include […] (vii) continuous failure to achieve agreed service levels or a substantial loss of service, and (ix) a failure to successfully execute cloud provider test migrations at the agreed ti"es". The last two points are not classifiable "s "chan"es" but they are specific condition. We deem necessary to separate them from the previous termination reasons.	The ECB has reviewed the reasons for termination to align with the provisions of DORA. Point (ix) has been retained to emphasise that the ECB expects exit strategy tests to be conducted.	Yes
251	Scope	ABI – Italian Banking Association The statement regarding termination right seems to be a brand new requirement we propose to remove the chapt"r "2.4.1 Termination rig"ts" considering that many aspects are in	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure"	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		overlap with other regulations	are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	
252	Granularity of exit plans	ABI – Italian Banking Association The statement regarding detail levels of exit plans seems to be a requirement (wrt critical milestones, skill sets, etc.). we propose to remove the chapt“r "2.4.3 Granularity of exit pl”ns" considering that many aspects are in overlap with other regulations	The Guide means to specify the supervisory expectations regarding the granularity of exit plans in accordance with Article 28(8) of DORA and bearing in mind the principle of proportionality as described in Article 28(1)(b). The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	Yes
253	Business continuity and exit strategy	ABI – Italian Banking Association The paragraph 2.4.4 collapses Business Continuity and Exit Strategy considerations and introduces the concept of “n "exit under stress or an exit without the cooperation of the CSP”s)". This requirement is quite impossible to be respected, as recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort.	The ECB recommends a supervised institution to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides, this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	No
273	Termination rights	Banking and Payment Federation Ireland (BPFI) The proposed guidance on grounds for termination of arrangements with CSPs significantly expand the scope of termination rights beyond what is currently established in DORA and the EBA GLs, and does not reflect proportionate and risk-based principles. It would be unreasonable to expect the reasons for termination detailed in the guide to be reflected in contractual arrangements with CSPs. The Guide therefore creates prescriptive, but non-exhaustive and non-binding expectations that go beyond acceptable legal and market practice. This would unnecessarily complicate the implementation of effective contracts and may prompt unnecessary off-cycle contractual remediation. Existing termination rights would achieve the same protective outcomes. In particular, we would like to draw attention to the following specific elements: • excessive increase in expenses – It is not clear on what basis the ECB consider “an excessive increase in expenses under the contractual arrangements that are attributable to the CSP” to be within the considerations included within DORA 28(7). Furthermore, it is unclear what relevance this could have to termination rights, as costs normally only change at the point of renewal. In such a circumstance if the commercial terms were not acceptable an institution would move to an alternative supplier from the end of the existing contract with no need to terminate it. We would urge the ECB to remove this element from the Guide. • the relocation of business units or data centres – In our view, this requirement is too granular and would be captured by material breach termination rights given existing outsourcing requirements that providers seek Fis consent ahead of changing the service or data storage	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”: “[...] When applying these expectations, account should be taken of the principle of proportionality.” The Guide has been amended, since some items cannot be clearly defined as	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		locations. As such, we would recommend its deletion. • changes to national legislation or regulations applicable to data location and processing – similarly, this would be covered by contractual rights to terminate for legal/regulatory reasons under the impediments capable of altering performance concept required by the EBA Guidelines. We would therefore suggest the ECB does not include this in its final Guide. • significant changes to the management of cyber risk in the subcontracting chain – this is also covered by general termination rights related to subcontractors under EBA GLs and DORA and in our view, does not warrant inclusion. • failure to successfully execute cloud provider test migrations at agreed times – from our perspective this is criterion is too granular. It is also unclear what the material risk is here while material breach termination rights would achieve the same outcome. • Expectation that it should be possible to terminate only some services – From members feedback, they underline that this would be extremely difficult to do in practice. Many services provided by CSPs are highly intertwined and difficult to legally separate. We would welcome the ECB's recognition that this would be beneficial where feasible, and acknowledgement that it may not be possible in the majority of cases. • 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 – this overlaps significantly with the technical standards being developed by the ESAs in their mandate under DORA on the subcontracting of critical or important functions, the final draft of which is expected to be published for adoption by the Commission on the 17th of July. However, the ECB does not consider either the criticality of the service being provided by the CSP or the materiality of the services being provided to the CSP by its subcontractors. This consideration of criticality and materiality is fundamental to the principles of risk management, as many services provided by CSPs may not be critical to the functioning of the institution, and many of their subcontractors may not have a material impact on the CSP's ability to provide those services (e.g. catering suppliers). Given the extension of scope of this guide to also cover those TPPs which are reliant on cloud this is even more important, for instance an institution's catering supplier which uses cloud services for scheduling is not likely to warrant the enormous investment of resources that would be required to fulfil these provisions and which could be more effectively deployed in relation to more critical suppliers. The technical standards being developed by the ESAs, as instructed by the European legislature as part of DORA, have limited the application of requirements regarding subcontractors to those that support Critical or Important Functions (CIFs) as defined in DORA. Furthermore, we understand that following engagement with industry, the technical standards being developed by the ESAs will focus on those subcontractors which effectively underpin the CIF. We would suggest that the ECB remove provisions which overlap with the technical standards being developed by the ESAs to avoid duplication and / or contradiction, especially as these requirements will become legal requirements following adoption by the Commission and publication in the Official Journal of the EU after scrutiny by the European Parliament. At a minimum, the ECB should recognise that the management of CSPs' relationships with their subcontractors remains the responsibility of the CSP, and that while institutions may stipulate in their contractual agreements with CSPs that their contractual agreements with their subcontractors must follow the same provisions, it is for the CSP to comply with those contractual arrangements. More broadly, we would argue that by focusing on addressing the underlying risk, rather than prescribe specific considerations, financial entities can maintain effective risk management while avoiding unnecessary complexity in their contractual arrangements with CSPs, which could be further reflected on by the ECB. For example, the requirement to	a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The ECB has also clarified the expectation regarding "significant changes" or "other changes". The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		ensure that the termination notice period set out in the contract should allow the institution to transfer or insource in accordance with the exit plan does not reflect risk management practices whereby the notice period for termination has little to do with the transition of services, which is generally for a defined period post the effective date of the termination of services.		
274	Scope	Banking and Payment Federation Ireland (BPFI) The Guide should explicitly state that requirements on exit plans are for services supporting CIFs (consistently with / as part of the exit strategy as referenced in paragraph 2.4). Granular exit plans do not necessarily provide a useful tool and could become quickly outdated or not be relevant for the scenario.	The ECB limits the expectations to critical or important functions, as DORA delimits exit strategies to critical or important functions only and refers to general comments. The Guide has been amended.	Yes
275	Exit plan	Banking and Payment Federation Ireland (BPFI) The execution of exit plans is by nature an exceptional activity, and so often requires additional resources and capacity beyond those required for BAU activities. As such, many exit plans involve the hiring of professional services and / or contractors to augment the institutions' normal staff. The ECB's proposed requirement for institutions to check that they have the personnel required for their exit plans could be interpreted to require institutions to maintain sufficient staff to execute against exit plans on a full-time basis, which would be an additional cost beyond what is required for BAU activities. We would propose that the ECB amend this section to read: Institutions should check that they have the personnel required for their exit plans, or a plan for the additional staff which would be required and, by conducting a walkthrough of the tasks involved, ensure that the planned staff available are would be able to perform the proposed tasks outlined in the exit plan.	The ECB considers this statement to be in line with the provisions of Article 28(8) of DORA: "Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically." Meanwhile, the use of external resources is considered acceptable, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the guide has been amended.	Yes
291	Scope	European Cloud User Coalition (ECUC) The prescriptive nature of the guidance on termination rights detracts from the prescriptive requirements set out within DORA. The value of the guidance is in supplementing the legal requirements, not proposing alternative criteria.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	No
306	Termination rights	European Cloud User Coalition (ECUC) Can you please explain what is exactly meant with 'an excessive increase in expenses under the contractual arrangements that are attributable to the CSP'? In particular, please explain if and how this differs from a contractual breach and please provide (an) example(s).	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
307	Subcontractors Cybersecurity risk	European Cloud User Coalition (ECUC) What is meant exactly with (vii) significant changes to the 'management' of cybersecurity risk in the chain of subcontractors? Could you please provide a good practice?	The ECB has clarified the expectation regarding "significant changes".	Yes
308	Termination	European Cloud User Coalition (ECUC)	Similar to other ECB Guides	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
	rights	Whilst it is referred to clause 28(7) DORA, various reasons for termination are listed form (i) tot (ix) but is is not clear where those reasons originate from exactly. Can you please elaborate?	this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	
313	Termination rights	European Cloud User Coalition (ECUC) Please clarify if “conflicting legislation” is a scenario that needs to be catered for in case the service provider is an EU company	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such confusion.	Yes
315	Proportionality	International Business Machines Corporation IBM recommends that subcontract flow down requirements be aligned with the specific DORA Regulatory Technical Standards on the same topic, when finalized. IBM recommends that those provisions incorporate practical concepts of risk-based relevance, flexibility and proportionality.	The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations. Moreover, the ECB considers that the proportionality principle is sufficiently highlighted in Section 1.2 “Scope and effect”: “[...] When applying these expectations, account should be taken of the principle of proportionality.”	Yes
317	Termination rights	International Business Machines Corporation IBM recommends that termination rights be as specified by DORA Article 28(7). Many of the proposed additional triggers for termination are not risk based and are not commercially reasonable.	Similar to other ECB Guides, this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes
369	Exit strategy	European banking Federation With reference to the provision: “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.” Clarification is needed with respect to the meaning of “principle-based”.	The term “principle-based” used in the draft Guide was not clear. The Guide has been amended accordingly.	Yes
370	Exit strategy	European banking Federation The statement regarding exit strategy definition on outsourced cloud services performing critical or important functions seems to be a brand new requirement. We propose to remove: “Exit strategies with clearly defined roles and responsibilities and estimated costs should be drawn up for all outsourced cloud services performing critical or important functions before those systems go live, and the time required to exit should be in line with the transition period indicated in the relevant contractual agreement”.	The statement Is already contemplated in EBA/GL/2019/02 on outsourcing arrangements and the ECB considers it part of a comprehensive and documented plan according to Article 28(8) of DORA.	Yes
371	Termination rights	European banking Federation Regarding 2.4.1 paragraph (2) describing other changes that could also lead to such a reason for termination, including in particular:	The Guide has been amended, since some items cannot be clearly defined as a change in the social,	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		(iv) relocation of the data centeI. and (vi) a change in the regulations applicable to data location and data processI ... With reference to the se“tence "(vii) significant changes to the management of cybersecurity risk in the chain of sub-cont”actors", we suggest an amendment by generalising the requirement as fo“lows: "(vii) violation of the cybersecurity obligations indicated in the contractual clauses, also with reference to the chain of sub-cont”actors".	political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists.. The ECB has also clarified the expectation regarding “significant changes”.	
372	Subcontractors cybersecurity risk	European banking Federation With reference to the se“tence "(vii) significant changes to the management of cybersecurity risk in the chain of sub-contr”ctors,", the proposal is to generalize the requirement as f“llow: "(vII) violation of the cybersecurity obligations indicated in the contractual clauses, also with reference to the chain of sub-cont”actors"	The ECB has clarified the expectation regarding “significant changes”.	Yes
373	Termination rights	European banking Federation "Other changes that could also lead to such a reason for termination inIde [...] (vii) continuous failure to achieve agreed service levels or a substantial loss of service, and (ix) a failure to successfully execute cloud provider test migrations at the ag”eed times". The last two points are not classi“iable a” "changes" but they are specific condition. We deem necessary to separate them from the previous termination reasons.	The ECB has reviewed the reasons for termination to align with the provisions of DORA. Point (ix) has been retained to emphasise that the ECB expects exit strategy tests to be conducted.	Yes
374	Termination rights	European banking Federation The statement regarding termination right seems to be a brand new requirement we propose to remove th“ chapter "2.4.1 Terminat”on rights" considering that many aspects are in overlap with other regulations. We need clarification on “hat does "an excessiv” increase" means in “(iii) an excessive increase in expenses under the contractual arrangements that are attributable to the CSP”.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
375	Scope	European banking Federation These provisions go far beyond DORA, thus we suggest an alignment with DORA. Article 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	The ECB provides only good practice to illustrate how the supervisory expectations regarding the content of an exit strategy and its alignment with the exit plan, could be implemented in light of Article 28(8) of DORA and bearing in mind the principle of proportionality as described in Article 28(1)(b). As a result, the Guide has been amended.	Yes
376	Granularity of exit plan	European banking Federation The statement regarding detail levels of exit plans seems to be a requirement (with regard to critical milestones, skill sets, etc.). We propose to remove th“ chapter "2.4.3 Granularity of ”xit plans" considering that many aspects are in overlap with other regulations.	The Guide sets out to specify the supervisory expectations regarding the granularity of exit plans, in accordance with Article 28(8) of DORA and bearing in mind the principle of proportionality as described in Article 28(1)(b). The Guide does not aim to	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	
377	Proportionality	European banking Federation If our proposal to delete th“ chapter "2.4.3 Granularity of ”xit plans" is not taken on board, we would suggest the following wording: "A dedicated exit plan as referred to in Article 28(8) of DORA should ensure that a supervised entity is able to react quickly to any deterioration in the service provided by a CSP. It is good practice for exit plans to include, as a target, the critical milestones, a description of the tasks or steps and general skill sets that are necessary to perform the exit, and a rough estimate of the time required and the costs involved. Exit plans should be reviewed and tested on a regular basis, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. Supervised entities should at least perform an in-depth desktop review, ensuring that such reviews are conducted by staff who are sufficiently knowledgeable about cloud technologies. Institutions should also review the amount of data and the complexity of the applications that would need to be migrated, thinking about the potential data transfer method, in order to produce meaningful estimates of the time required. Institutions should check that they have the personnel required for their exit plans, allowing for the impromptu allocation of external resources if necessary and, by conducting a walkthrough of the tasks involved, ensure that the proposed tasks outlined in the exit plan can be performed within the previously described bounds. For the most critical steps in the migration process, employees' ability to perform their assigned roles in the allotted time should be considered when performing reviews. Supervised entities should check, on a regular basis, to what extent the general skill sets required to perform the tasks set out in their exit plans are represented among staff members, or whether the support of external consultants would generally be needed in order to exit a cloud outsourcing arrangement. The feasibility of each exit plan should be independently verified (i.e. checked by someone who, possibly while still being part of the institution, is not responsible for drafting the plan in question, comparable to internal audit”process)."	The Guide sets out to specify the supervisory expectations regarding the granularity of exit plans. In terms of the migration process, the ECB acknowledges that the principle of proportionality should be taken into account for the use of internal/external resources, in accordance with Article 28(8) of DORA and as described in Article 28(1)(b). The Guide does not aim to be prescriptive, as it depends on the specific situation of each institution. As a result, the Guide has been amended.	Yes
378	Business continuity and exit strategy	European banking Federation The paragraph 2.4.4 collapses Business Continuity and Exit Strategy considerations and introduces the conc“pt of an "exit under stress or an exit without the cooperation of ”he CSP(s)". This requirement is quite impossible to be respected, as recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, maintain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenan”e effort."	The ECB recommends a supervised entity to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	No
379	Termination rights	European banking Federation "Regardless of any contractual agreement, such a termination could be caused by external events such as conflicting legislation."Conflicting legislation is unlikely to happen without a transitionary grace period. The scenario outlined here appears to be the legal counterpart to the extinction level event described above. Given the legal (and contractual) transitionary periods, it appears prudent to limit the expectations to cautioning institutions against this kind of threat.	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			confusion."	
380	Exit strategy	European banking Federation It should be noted that any kind of outsourcing retains the risk of a contractual party not fulfilling their duties in this way. However, a provision that necessitates a more or less seamless transition away from any outsourced service may put in question the use of cloud services as a concept. We therefore suggest to delete these interpretations because they go far beyond DORA.	The ECB recommends a supervised entity to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations.	No
455	Exit plan	Dutch Banking Federation (DBF) The requirement on obliging CSPs to assist with a transition is superfluous given the legal obligations set out in the Data Act. Similarly the Data Act stipulates 7 months for the transition, which is not reflected in the ECB guidance. The guidance should be embedded in the wider regulatory landscape.	The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854.	Yes
456	Termination rights	Dutch Banking Federation (DBF) The value of the guidance is in supplementing the legal requirements, not proposing alternative criteria. Additionally there are other ways in which to tackle the underlying risks and provide comfort to regulators, without the need to resort to termination. For example additional safeguards on risk management, including through the incoming CTPP regime. The Guidance creates new additional termination rights which go beyond existing practice. Various reasons listed for termination from (i) to (ix) are not in accordance with Article 28(7) of DORA and EBA requirements. Also it is is not clear where those additional reasons originate from. The following reasons for termination should be deleted: "i) an excessive increase in expenses ii) relocation of business units or data centres iii) merger or sale iv) failure to successfully execute cloud provider test migrations at the agreed times. (vii) significant changes to the management of cybersecurity risk in the chain of sub-contractors" Seeking to create non-binding termination rights which do not reflect existing legal or market practice is lacking both proportionality and feasibility. Furthermore CSPs are unlikely to accept additional termination rights given the non-binding nature of the Guidance.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The ECB has also clarified the expectation regarding “significant changes”. The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
457	Scope	Dutch Banking Federation (DBF) The lack of proportionality in not limiting such expectations to only services supporting CIFs is stretching the feasibility of the guidance. As is the requirement that exit plans should be reviewed and tested regularly. This is especially the case with regards to strong authentication for all users, as opposed to	The ECB limits the expectations to critical or important functions, as DORA delimits exit strategies to critical or important functions only and	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		focusing on accessing those systems deemed critical.	refers to general comments. The Guide has been amended.	
458	Termination rights	Dutch Banking Federation (DBF) The reference to conflicting legislation is likely pointing to potential third country sanctions. The guidance should remain technical in nature, rather than incorporating political discussions best reserved for other policy vehicles.	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such confusion.	Yes
459	Data Act	Dutch Banking Federation (DBF) With regard to "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.", we would like to know whether the enforcement of the interoperability requirements of the Data Act support this.	The Data Acs should ensure that through data portability requirements, FEs retain control over their data, even during transitions. Data-sharing contracts should avoid unfair clauses that might complicate or prevent a smooth exit (e.g. excessive fees for data migration). Interoperability is critical for the transfer of data between systems. This is beneficial to the exit strategies required under DORA, as interoperability reduces the technical challenges associated with switching providers. This synergy ensures that when supervised entities activate their exit strategies, the technical process of transferring data is straightforward, thus reducing downtime and operational risk.	No
493	Termination rights	DIGITALEUROPE The first two paragraphs of Section 2.4.1 should be deleted.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The ECB has also clarified the expectation regarding “significant changes”. The Guide has been amended since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	
494	Sub-outsourcing	DIGITALEUROPE The penultimate paragraph should be deleted, or, as a minimum amended as follows: On the basis of the requirement concerning key contractual provisions contained in Art. 30(2)(a) of DORA, institutions should ensure that WHERE RELEVANT all SUPPLIERS OF SUBCONTRACTED SERVICES SUPPORTING THE CSP SUBCONTRACTORS THAT EFFECTIVELY UNDERPIN THE PROVISION OF THESE ICT SERVICES (I.E. ALL THE SUBCONTRACTORS PROVIDING ICT SERVICES WHOSE DISRUPTION WOULD IMPAIR THE SECURITY OR THE CONTINUITY OF THE SERVICE PROVISION) comply WITH EQUIVALENT THE SAME contractual obligations that apply between the institution and the CSP, (including obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and back-ups) if termination rights are exercised.	The ECB has clarified the expectation regarding “significant changes”. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854).	Yes
495	Termination rights	DIGITALEUROPE As drafted, 2.4 introduces requirements that are not included in DORA, are unrealistic and too rigid while not increasing the resiliency of financial entities. Sub-subsection 2.4 should be DELETED in its entirety.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages.	Yes
563	Data Act	European Association of Public Banks The requirement on obliging CSPs to assist with a transition is superfluous given the legal obligations set out within the Data Act. Similarly the Data Act stipulates 7 months for the transition, which is not reflected in the ECB guidance.	The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854).	Yes
564	Termination rights	European Association of Public Banks The Guidance creates new additional termination rights which go beyond existing practice. The following should be deleted: "i) an excessive increase in expenses ii) relocation of business units or data centres iii) merger or sale iv) failure to successfully execute cloud provider test migrations at the agreed times."	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The ECB has also clarified the expectation regarding “significant changes”. The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			the Data Act (Regulation (EU) 2023/2854) and DORA.	
565	Termination rights	European Association of Public Banks The prescriptive, yet non-exhaustive, nature of the guidance detracts from the prescriptive requirements set out within DORA. Additionally the reference in any changes in cybersecurity obligations being cause for termination should be exchanged with violations to cybersecurity obligations. CSPs are unlikely to accept additional termination rights given the non-binding nature of the Guidance.	The ECB has clarified the expectation regarding “significant changes”.	Yes
566	Termination rights	European Association of Public Banks “2.4.1 (2) describes other changes that could also lead to such a reason for terminating for termination, including in particular (iv) relocation... and (vi) change in the regulations applicable... For iv)and iv) we suggest to add “unless the data is immediately transferred to a host country that also otherwise meets the requirements of the outsourcing agreement".	The Guide has been amended, since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists.. The ECB has also clarified the expectation regarding “significant changes”.	Yes
567	Termination rights	European Association of Public Banks Point (iii) (“an excessive increase in expenses under the contractual arrangements that are attributable to the CSP”) should be deleted, as it goes beyond DORA and could not be implemented with legal certainty. Extraordinary termination rights in the event of an unreasonable price increase by the service provider should generally be covered by civil law.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
568	Termination rights	European Association of Public Banks "(iii) an excessive increase in expenses under the contractual arrangements that are attributable to the CSP" how must this be understood in contractual context, because this is not defaulting/breaching a contract, so no termination for cause	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not to add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
569	Termination rights	European Association of Public Banks "an excessive increase in expenses under the contractual arrangements that are attributable to the CSP." Please reconsider these criteria. Concern is that qualifications as 'ongoing inadequate performance' or 'serious breaches' are not clearly and consistently defined in applicable civil law. Also, it may be hard to proof for the institution that the expenses are increased due to the CSP, other than an increase in the applicable rates. Setting out these criteria in this guide may	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		result in the CSPs offering termination rights only in these circumstances. Such termination rights may prove difficult to enforce. Please reconsider whether the termination rights in the DORA and EBA GL are sufficiently clear and please bear in mind that most CSPs offer the right to terminate for convenience and for breach that is not cured within 30 days. The main concern in practice is if the CSP requires a certain volume or fee commitment over a certain period of time. Such fee commitments may form a barrier for termination.	expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	
570	Termination rights	European Association of Public Banks ECB interpretation of art. 28(7) of DORA. Please clarify that the ECB expects that the institutions will take these circumstances into account when considering whether to terminate a contract in accordance with 28 (7) of DORA.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations The Guide has been amended.	Yes
571	Scope	European Association of Public Banks These interpretations go far beyond DORA, we suggest to be aligned with DORA. Art. 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	The ECB provides only good practice on how the supervisory expectations regarding the content of an exit strategy and its alignment with the exit plan, could be implemented in light of Article 28(8) of DORA and bearing in mind the principle of proportionality as described in Article 28(1)(b). As a result, the Guide has been amended.	Yes
572	Exit plan	European Association of Public Banks We suggest following wording: "A dedicated exit plan as referred to in Article 28(8) of DORA should ensure that a supervised entity is able to react quickly to any deterioration in the service provided by a CSP. It is good practice for exit plans to include, as a target, the critical milestones, a description of the tasks or steps and general skill sets that are necessary to perform the exit, and a rough estimate of the time required and the costs involved. Exit plans should be reviewed and tested on a regular basis, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. Supervised entities should at least perform an in-depth desktop review, ensuring that such reviews are conducted by staff who are sufficiently knowledgeable about cloud technologies. Institutions should also review the amount of data and the complexity of the applications that would need to be migrated, thinking about the potential data transfer method, in order to produce meaningful estimates of the time required. Institutions should check that they have the personnel required for their exit plans, allowing for the impromptu allocation of external resources if necessary and, by conducting a walkthrough of the tasks involved, ensure that the proposed tasks outlined in the exit plan can be performed within the previously described bounds. For the most critical steps in the migration process, employees' ability to perform their assigned roles in the allotted time should be considered when performing reviews. Supervised entities should check, on a regular basis, to what extent the general skill sets required to perform the tasks set out in their exit plans are represented among staff members, or whether the support of external consultants would generally be needed in order to exit a cloud outsourcing arrangement. The feasibility of each exit plan should be independently verified (i.e. checked by someone who, possibly while still being part of the institution, is not responsible for drafting the plan in question, comparable to in internal audit process).	The Guide sets out to specify the supervisory expectations regarding the granularity of exit plans. In terms of the migration process, the ECB acknowledges that the principle of proportionality should be taken into account for the use of internal/external resources in accordance with Article 28(8) of DORA and as described in Article 28(1)(b). The Guide does not aim to be prescriptive, as it depends on the specific situation of each institution. As a result, the Guide has been amended.	Yes
573	Exit strategy	European Association of Public Banks	The ECB recommends a	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		It should be noted that any kind of outsourcing retains the risk of a contractual party not fulfilling their duties in this way. However, a provision that necessitates a more or less seamless transition away from any outsourced service may put in question the use of cloud services as a concept. We therefore suggest to delete these interpretations because they go far beyond DORA.	supervised entity to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides ,this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations.	
574	Scope	European Association of Public Banks The lack of proportionality in not limiting such expectations to only services supporting CIFs is stretching the feasibility of the guidance. As is the requirement that exit plans should be reviewed and tested regularly. This is especially the case with regards to strong authentication for all users, as opposed to focusing on accessing those systems deemed critical.	The ECB limits the expectations to critical or important functions, as DORA delimits exit strategies to critical or important functions only and refers to general comments. The Guide has been amended.	Ye
575	Termination rights	European Association of Public Banks The reference to conflicting legislation appears to be referencing potential third country sanctions. This should be dealt with separately.	The reference to termination due to conflicting legislation was indeed confusing, as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such confusion.	Yes
594	Termination rights	Google Cloud The additional grounds of termination and termination scenarios in Section 2.4.1 conflict with and exceed the DORA requirements. The first two paragraphs of Section 2.4.1 should be delete	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
595	Sub-outsourcing	Google Cloud The subcontractor requirements in Section 2.4.1 overlap with and create confusion regarding the RTS on Subcontracting. The fifth paragraph of Section 2.4.1 should be deleted.. Alternatively, the text should be amended as follows: On the basis of the requirement concerning key contractual provisions contained in Article 30(2)(a) of DORA, institutions should ensure that WHERE RELEVANT all SUBCONTRACTORS THAT EFFECTIVELY UNDERPIN THE PROVISION OF THESE ICT SERVICES [DELETE: suppliers of subcontracted services supporting the CSP] comply with EQUIVALENT [DELETE: the same] contractual obligations that apply between the institution and the CSP, (including obligations relating to confidentiality, integrity, availability, the	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		retention and destruction of data, configurations and back-ups) if termination rights are exercised.		
629	Exit strategy	Bitkom "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”	The term “principle-based” used in the draft Guide was not clear. The Guide has been amended accordingly.	Yes
630	Termination rights	Bitkom 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 ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854) and DORA.	Yes
631	Exit plan	Bitkom 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 supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854).	Yes
632	Exit plan	Bitkom 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	The supervisory expectations set out in the Guide are intended to assist supervised entities and do not add new requirements. The Guide has been amended to align with existing regulations such as the Data Act (Regulation (EU) 2023/2854).	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
633	Termination rights	Bitkom "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).	The ECB recommends a supervised entity to be prepared for a scenario of exit under stress. This would include having a business continuity policy and ensuring access to the data required to operate the service. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	No
643	Termination rights	European Savings and retail Banking Group (ESBG) New requirements in contractual clauses related to termination rights and exit plans. In the first paragraph, reference is being made to the ECB's understanding of general termination rights and lists that such termination rights “could”, inter alia, include “an excessive increase in expenses under the contractual arrangements that are attributable to the CSP” next to “ongoing inadequate performance” and “serious breaches of the contractual terms, or of the applicable law or regulations”. We note in this context that while ongoing breaches and (even only) one-time serious breaches are usual and market standard termination rights in service agreements (i.e., points (i) and (ii) as listed in the first paragraph), a general termination right due to “an excessive increase in expenses” is unusual since pricing is – next to the service description – a core element of any service contract and as such has to be negotiated and agreed by both Parties. Therefore, an “excessive increase in expenses” should not happen unilaterally and thus such termination right is usually not needed and thus not usually included by default in such agreements. The RTS to specify the policy on ICT services performed by third parties (Art.28.10 of DORA) that were published in March 2024 did not include some of the requirements set out in the revised guidance. For example, there is a request for termination rights for excessive incremental costs attributable to the CSP, or the obligation to regularly review the best options provided for in the exit plans. Given that the negotiation of contractual aspects is a complex process, especially when one of the parties is a large cloud service provider, these types of new requirements should be reflected in the Directive and not in the Guide, so that entities have a better negotiating leverage point, otherwise these requirements are almost impossible to negotiate when it comes to finalising the clauses. With regard to "exit under pressure", it is outside the sphere of influence of institutions when there is a conflict with non-EU legislation, to which CSPs are subject, because this is a political issue.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations The Guide has been amended.	Yes
665	Termination rights	Futures Industry Association (FIA) The Guide significantly expands the scope of termination rights beyond what is currently established in DORA and the EBA GLs. It would be unreasonable to expect the reasons for termination detailed in the guide should be reflected in contractual arrangements with CSPs. This would complicate	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words “should” and “ensure” are used, the Guide means	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		implementation of effective contracts and does not align with existing risk management and contracting principles and best practice. For example: • the relocation of business units or data centres would be captured by material breach termination rights given existing outsourcing requirements that providers seek FIs consent ahead of changing the service or data storage locations • changes to national legislation or regulations applicable to data location and processing would be covered by contractual rights to terminate for legal/regulatory reasons under the impediments capable of altering performance concept required by the EBA Guidelines • significant changes to the management of cyber risk in the subcontracting chain is covered by general termination rights related to subcontractors under EBA GLs and DORA. More specifically, in relation to the below guidance provided in the ECB Guide, FIA Members note this requirement does not reflect risk management practices whereby the notice period for termination has little to do with the transition of services, which is generally for a defined period post the effective date of the termination of services. "The institution should ensure that the CSP's termination rights are aligned with the institution's exit strategy. In particular, the notice period set out in the contract with the CSP should be sufficient to allow the institution (or any third-party service provider employed by the institution that uses cloud services in its outsourcing chain) to transfer or insource the relevant services in accordance with the schedule in the exit plan."	to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	
684	Scope	German Banking Industry Committee (GBIC) C.f. our comments regarding the definition of critical or important functions (ID #1): How does this relate to the more „institution-focussed" definition within DORA?	The ECB limits the expectations to critical or important functions, as DORA delimits exit strategies to critical or important functions only and refers to general comments. The Guide has been amended.	Yes
685	Termination rights	German Banking Industry Committee (GBIC) 2.4.1 (2) describes other changes that could also lead to such a reason for terminating for termination, including in particular (iv) relocation... and (vi) change in the regulations applicable... We suggest to add "unless the data is immediately transferred to a host country that also otherwise meets the requirements of the outsourcing agreement".	The Guide has been amended since some items cannot be clearly defined as a change in the social, political or economic climate. The Guide also specifies the reason for termination related to a change in regulation applicable to data location and data processing. The ECB recommends a supervised entity to be bound to a contract if no specific regulation exists..	Yes
686	Termination rights	German Banking Industry Committee (GBIC) Point (iii) ("an excessive increase in expenses under the contractual arrangements that are attributable to the CSP") should be deleted, as it goes beyond DORA and could not be implemented with legal certainty. Extraordinary termination rights in the event of an unreasonable price increase by the service provider should generally be covered by civil law.	The ECB acknowledges that an excessive increase in expenses under a contractual arrangement that is attributable to the CSP is a business decision that would be made upon reaching the end of that arrangement. Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			The Guide has been amended.	
687	Exit strategy	German Banking Industry Committee (GBIC) These expectations go far beyond DORA and should be deleted, as they are neither necessary nor practible. Acc. to Art. 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	The ECB provides only good practice on how the supervisory expectations regarding the content of an exit strategy and its alignment with the exit plan, could be implemented in light of Article 28(8) of DORA and bearing in mind the principle of proportionality as described in Article 28(1)(b). As a result, the Guide has been amended.	Yes
688	Exit plan	German Banking Industry Committee (GBIC) We suggest the following wording (part1): "A dedicated exit plan as referred to in Article 28(8) of DORA should ensure that a supervised entity is able to react quickly to any deterioration in the service provided by a CSP. It is good practice for exit plans to include, as a target, the critical milestones, a description of the tasks or steps and general skill sets that are necessary to perform the exit, and a rough estimate of the time required and the costs involved. Exit plans should be reviewed and tested on a regular basis, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. Supervised entities should at least perform an in-depth desktop review, ensuring that such reviews are conducted by staff who are sufficiently knowledgeable about cloud technologies. Institutions should also review the amount of data and the complexity of the applications that would need to be migrated, thinking about the potential data transfer method, in order to produce meaningful estimates of the time required. Institutions should check that they have the personnel required for their exit plans, allowing for the impromptu allocation of external resources if necessary and, by conducting a walkthrough of the tasks involved, ensure that the proposed tasks outlined in the exit plan can be performed within the previously described bounds."	The Guide sets out to specify the supervisory expectations regarding the granularity of exit plans. In terms of the migration process, the ECB acknowledges that the principle of proportionality should be taken into account for the use of internal/external resources, in accordance with Article 28(8) of DORA and as described in Article 28(1)(b). The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	Yes
689	Exit strategy	German Banking Industry Committee (GBIC) We suggest the following wording (part 2): "For the most critical steps in the migration process, employees' ability to perform their assigned roles in the allotted time should be considered when performing reviews. Supervised entities should check, on a regular basis, to what extent the general skill sets required to perform the tasks set out in their exit plans are represented among staff members, or whether the support of external consultants would generally be needed in order to exit a cloud outsourcing arrangement. The feasibility of each exit plan should be independently verified (i.e. checked by someone who, possibly while still being part of the institution, is not responsible for drafting the plan in question, comparable to in internal audit process)."	The Guide sets out to specify the supervisory expectations regarding the granularity of exit plans. In terms of the migration process, the ECB acknowledges that the principle of proportionality should be taken into account for the use of internal/external resources, in accordance with Article 28(8) of DORA and as described in Article 28(1)(b). The Guide does not aim to be prescriptive, as it depends on the specific situation of each supervised entity. As a result, the Guide has been amended.	Yes
690	Termination rights	German Banking Industry Committee (GBIC) Conflicting legislation is unlikely to happen without a transitionary grace period. The scenario outlined here appears to be the legal counterpart to the extinction level event described above. Given the legal (and contractual) transitionary periods, it appears prudent to limit the expectations to cautioning institutions against this kind of threat.	The reference to termination due to conflicting legislation was indeed confusing , as an external factor should not trigger contract termination. The supervised entity should be able to react in advance to political changes. The Guide has been amended to avoid such confusion.	Yes
691	Exit strategy	German Banking Industry Committee (GBIC) It should be noted that any kind of outsourcing retains the risk	Similar to other ECB Guides this Guide does not lay down new legally binding	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		of a contractual party not fulfilling their duties in this way. However, a provision that necessitates a more or less seamless transition away from any outsourced service may put in question the use of cloud services as a concept. We therefore suggest to delete these interpretations because they go far beyond DORA.	requirements. Where the words “should” and “ensure” are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations. The Guide has been amended to better reflect the existing regulation.	

2.6 Table 6 – Comments on Section 2.5: Oversight, monitoring and internal audits

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
22	Oversight	AWS 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	The ECB is of the view that while third-party certifications may be taken into consideration, these should be in addition to independent assessments/reviews conducted by the supervised entity’s own internal audit team. The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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." 		
23	Monitoring tools	AWS 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."	It is the responsibility of supervised entities to verify compliance with the ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
24	Contractual clauses	AWS 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	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
50	Third-party certification	Association of German Public Banks "An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts). "	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
51	Pooled audits	Association of German Public Banks The Guidance should state that institutions are encouraged to consider whether pooled auditing is advisable, on a risk-based approach. It should not specify how a pooled audit works in practice, given the need for variations in approach across member states.	This is a good practice observed during ECB supervisory activities. The Guide is not meant to be prescriptive.	No
52	Scope	Association of German Public Banks The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud.	The wording is aligned with Article 6(10) of DORA.	No
53	Monitoring tools	Association of German Public Banks Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases, in which the institution has reason to believe manipulation has occurred.	It is the responsibility of the supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	
69	Oversight and monitoring	ABBL - The Luxembourg Bankers' Association Financial entities may utilise different teams and functions for oversight and monitoring of a CSP due to the nature of the cloud service, the different expertise of various teams, how it operates across multiple financial entities or services and the materiality of the service provided. Enforcement of all monitoring within one function would not utilise the expertise of the financial entity effectively and would require reorganization of well-established functions within financial entities. Oversight and monitoring can be undertaken by individual cloud teams, third party oversight, cybersecurity functions, and technology functions or a combination of colleagues within those teams. We recommend the following amendment: 2.5.1: "… supervised institutions should retain expertise in-house (to delete the following phrase: ", with a centralised function or department being recommended for the monitoring of CSPs"). The monitoring…"	The Guide has been amended.	Yes
70	Monitoring tools	ABBL - The Luxembourg Bankers' Association The guidance should suggest what other tools should be taken into account if the ECB states that monitoring tools provided by a CSP might not be sufficient.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with ICT risk management requirements.	No
71	Contractual clauses	ABBL - The Luxembourg Bankers' Association The Guide introduces new requirements, beyond those set out in DORA. Therefore, the last sentence of this section which states "Institutions should use contractual clauses to ensure appropriate incident and monitoring reports, enabling ongoing assessment of outsourced functions." should be deleted.	This sentence has been amended as a recommendation.	No
72	Contractual clauses	ABBL - The Luxembourg Bankers' Association We propose the call for Standard Contractual Clauses (SCCs) is dropped given that there is a EU forum already reviewing the issue, and it has not yet produced any standardised clauses. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	This does not go beyond DORA. The ECB considers as a good practice to consider the listed items. The Guide has been slightly amended.	Yes
73	Contractual clauses	ABBL - The Luxembourg Bankers' Association The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes.	The ECB expects supervised entities to have safeguards in place against unilateral changes. The Guide has been amended.	Yes
74	Costs of audits	ABBL - The Luxembourg Bankers' Association The recommendation that "contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost" should be deleted. This goes beyond existing practice and the EBA Guidelines in expecting this information to be set out in the contract.	The ECB considers as a good practice to consider the listed items. The Guide has been amended.	Yes
122	Monitoring tools	AFME The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud. Independent monitoring should also be limited to cases in which the institution has reason to believe manipulation can occur.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	
123	Pooled audits	AFME The document states, “It is good practice for institutions to work together to audit a CSP, putting together a joint inspection team containing at least one technical expert from each institution”, however, Financial service firms may not have the authority to force CSPs to submit to this. The section should clarify how scopes would be defined for a joint audit when firms may be utilizing different service offerings provided by a CSP with various levels of criticality. Additionally, FIs may not want to disclose to other firms in the pool the specific capabilities that they are using.	This is a good practice observed during ECB supervisory activities. Before auditing a CSP, a joint audit team should agree on the audit’s scope. The Guide is not meant to be prescriptive.	No
124	Monitoring tools	AFME The guidance should suggest what other tools should be taken into account if the ECB is to state that monitoring tools provided by a CSP might not be sufficient. We would suggest that independent monitoring tools can be replaced by relying on CSP tools if they are reviewed periodically in a risk-based approach to ensure their adequacy.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with ICT risk management requirements.	No
125	Incident reports	AFME We would propose that the ECB amend its proposed requirements that institutions’ oversight functions should be able to follow up in detail on “any incident that occurs at the CSP” to account for impact on the institution in question. CSPs offer a large number of services to a variety of institutions, including non-financial institutions. CSPs would not be able to share details of incidents which are not relevant to a give institution, given confidentiality constraints. Furthermore, institutions would not wish to have access to such information. We would propose that this statement be amended to read: The institution’s oversight function should be able to follow up in detail on any incident impacting the institution that occurs at the CSP.	The Guide has been amended.	Yes
126	Contractual clauses	AFME We propose the call for SCCs is dropped given that there is a EU forum already reviewing the issue, and it has not yet produced any standardised clauses given variations in industry practice and outlook. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	This does not go beyond DORA. The ECB considers as a good practice to consider the listed items. The Guide has been slightly amended.	Yes
127	Contractual clauses	AFME The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes.	The ECB expects supervised entities to have safeguards in place against unilateral changes. The Guide has been amended.	Yes
128	Costs of audits	AFME The recommendation that "contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost" should be deleted. This goes beyond existing practice and the EBA Guidelines in expecting this information to be set out in the contract.	The ECB considers as a good practice to consider the listed items. The Guide has been amended.	Yes
185	Oversight	ECIIA It is necessary to have a definition of 1st/2nd LoD responsibilities on oversight/monitoring.	This Guide does not provide detailed practices for oversight and monitoring responsibilities, which fall outside the scope of this document.	No
186	Audit	ECIIA Further clarification and best practices are needed on how to solve “the CSPs auditing support“ issue. This is a general	The ECB is unable to provide good practices for this aspect.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		problem - individual internal audit function cannot solve it.	When negotiating contractual terms, supervised entities should refer to the provisions of Article 30(3)(e)(i) of DORA. Moreover, DORA introduces oversight of critical third-party service providers with ESAs appointed as Lead Overseer.	
187	Third-party certification	ECIIA The sentence "An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts)." should specify if it is a bout residual or inherent risk.	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
188	Pooled audits	ECIIA Last sentence of 2.5: We acknowledge that the practice outlined is good and aligns with best practices in audit procedures provided with the pooled audit approach of the Collaborative Cloud Audit Group. By requiring individual institutions to follow up directly with the Cloud Service Provider (CSP) on specific issues identified during a pooled / joint audit that are relevant only to that institution, it facilitates a focused, tailored and effective dialogue between the institution and the CSP to address any unique concerns or issues identified during the audit. regarding the rotation, we suggest "regular basis" rather	The Guide has been amended.	Yes
189	Monitoring tools	ECIIA Clarification needed in "In order to ensure an adequate level of quality, the institution should monitor the cloud services provided by the CSP. Relying solely on monitoring tools provided by a CSP in order to assess performance might not be sufficient in the case of outsourcing of critical or important functions" about the CSP's performance that should be monitored independently.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with ICT risk management requirements.	No
190	Contractual clauses	ECIIA Request for best practice on how to establish a process to ensure that more details are being shared by the CSP	The ECB is unable to provide good practices for this aspect. It is the responsibility of supervised entities to negotiate the contractual terms, in accordance with Articles 30(2) and 30(3) of DORA and Article 9 of CDR (EU) 2024/1773.	No
191	Contractual clauses	ECIIA The contractual clauses could also include periodical checkpoints for the utilization / capacity review of the services provided.	Supervised entities could include any contractual clause they see fit to ensure adequate monitoring of the cloud services provided by a CSP, in addition to the provisions set out in Article 30(2) and 30(3) of DORA and Article 9 of CDR (EU) 2024/1773.	No
192	Costs of audits	ECIIA The sentence : •Contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indica-ting the maximum cost" should be changed : "contracts should include details of how the costs of performing audits is calculated"	The Guide has been amended.	Yes
196	Incident reports	Confédération Nationale du Crédit Mutuel Could you specify the concerned incidents are critical incidents please.	Pursuant to Article 17(2) of DORA, financial entities, as defined in Article 2, paragraphs (a) to (t), shall record all ICT-related incidents. The Guide has been	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
			amended.	
254	Contractual clauses	ABI – Italian Banking Association Given that the institutions and CSPs work closely together, we suggest to better clarify what are the CSP's performance that should be monitored independently and limiting to cases in which the institution has reason to believe manipulation can occur	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
255	Costs of audits	ABI – Italian Banking Association The statement regarding cost of performing on-site audits seems to be a brand new requirement. We propose to delete the following: "Contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost."	The Guide has been amended.	Yes
256	Contractual clauses	ABI – Italian Banking Association The paragraph mentions "standard contractual clauses developed by public authorities". Please clarify if that language refers to already-defined expectations in terms of scope and/or timeline for development of standard clauses, also in relation to the' DORA's timeline	The Guide is aligned with DORA regarding the use of “standard contractual clauses developed by public authorities”.	No
276	Audits	Banking and Payment Federation Ireland (BPFI) The proposed good practice of institutions conducting combined audits is likely to represent unacceptable levels of operational and information security risks for the institutions in question. An alternative approach would be for institutions to leverage vendors to conduct audits on behalf of groups of institutions, an approach which has proved successful in other jurisdictions. This would provide the benefits of conducting combined audits while ensuring that firms do not expose their data, systems and processes to competitor institutions.	When auditing a CSP, supervised entities should consider relying on its own internal audit function, or appointing a third party, or conducting a pooled audit in line with Article (8)(2)(a) and 8(2)(b) of CDR (EU) 2024/1773. The Guide has been amended.	Yes
277	Audits	Banking and Payment Federation Ireland (BPFI) The ECB should not enforce monitoring of CSPs to be undertaken by a single centralised function or a single department within a financial entity. Financial entities may utilise different teams and functions for oversight and monitoring of a CSP due to the nature of the cloud service, the different expertise of various teams, how it operates across multiple financial entities or services and the materiality of the service provided. Enforcement of all monitoring within one function would not utilise the expertise of the financial entity effectively and would require reorganization of well-established functions within financial entities. Oversight and monitoring can be undertaken by individual cloud teams, third party oversight, cybersecurity functions, and technology functions or a combination of colleagues within those teams. We would make the following recommendation: 2.5.1: “… supervised institutions should retain expertise in-house, with a centralised function or department being recommended for the monitoring of CSPs. The monitoring…”	The Guide has been amended.	Yes
278	Oversight	Banking and Payment Federation Ireland (BPFI) We would propose that the ECB amend its proposed requirements that institutions’ oversight functions should be able to follow up in detail on “any incident that occurs at the CSP” to account for impact on the institution in question. CSPs offer a large number of services to a variety of institutions, including non-financial institutions. CSPs would not be able to share details of incidents which are not relevant to any or all institutions, given confidentiality constraints. Furthermore, institutions would not wish to have access to such information. We would propose that this statement be amended to read: The institution’s oversight function should be able to follow up in detail on any incident impacting the institution that occurs at the CSP.	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
279	Contractual clauses	Banking and Payment Federation Ireland (BPFI) It is not clear in the current draft of the Guide as to whether the contractual clauses covered are relevant specifically to standard contractual clauses, or if these should be considered to be best practices in general. The proposed best practice to include provisions covering the costs associated with on-site audits is not regarded as conclusively best practice in industry. Currently many vendors waive costs associated with audits, but requiring this to be covered in the contractual clauses could encourage CSPs to charge firms for audits. Additionally, the requirement to have providers sign a separate digital or physical copy may introduce operational difficulties which could be more easily addressed by the simple expedient of firms taking a copy of the terms at the point of signing, and requiring notice and non-objection to amendments to terms.	The Guide has been amended.	Yes
316	Contractual clauses	International Business Machines Corporation DORA requires financial entities and ICT third-party service providers to "consider" the use of standard contractual clauses developed by public authorities for specific services. Changing the statutory requirement to "consider" to supervisory guidance that "recommends" such use is inappropriate, especially when no standard contracts currently exist and any standard terms' suitability across a diverse range of future service offerings, potential use cases, and risk scenarios is questionable.	The Guide is aligned with DORA regarding the use of “standard contractual clauses developed by public authorities”.	No
381	Audits	European Banking Federation “An institution’s internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts).” This section goes beyond DORA in scope as the latter only mention "audit on critical ICT", we would ask for an amendment aiming to stick to DORA provision.	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
382	Monitoring tools	European Banking Federation "In order to ensure an adequate level of quality, the institution should monitor the cloud services provided by the CSP. Relying solely on monitoring tools provided by a CSP in order to assess performance might not be sufficient in the case of outsourcing of critical or important functions." Clarification is needed about the CSP's performance that should be monitored independently.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with ICT risk management requirements.	No
383	Contractual clauses	European Banking Federation Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases, in which the institution has reasons to believe manipulation has occurred.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
384	Contractual clauses	European Banking Federation “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”. The requirement to sign a separate digital or physical copy is not a current widely-used market practice, therefore we would suggest deleting it in order to allow for consistency in the market as regards contracting.	The Guide has been amended.	Yes
385	Costs of audits	European Banking Federation The statement regarding cost of performing on-site audits seems to be a brand new requirement. We propose to delete the following: "Contracts should include details of how the cost of performing on-site audits is calculated, ideally including a	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		breakdown and indicating the maximum cost."		
386	Contractual clauses	European Banking Federation The paragraph mentions "standard contractual clauses developed by public authorities". Please clarify if that language refers to already-defined expectations in terms of scope and/or timeline for development of standard clauses, also in relation to the' DORA' timeline.	The Guide is aligned with DORA regarding the use of “standard contractual clauses developed by public authorities”.	No
460	Audits	Dutch Banking Federation (DBF) We strongly suggest To adopt our amendments to the texts in bold. (..:) the internal audit functions of the institutions as the third line of the control model should regularly review, following a risk based approach, the risks stemming from the use of a CSP’s cloud services. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity. The institutions fulfil these requirements if the internal audit carries out, on the basis of up-to-date information, an overall risk assessment of the ICT risks of the institution for the purpose of drawing up the appropriate internal audit work plan. Depending on the outcome of the overall risk assessment, the intensity and frequency of the audit assignments may differ between specific areas. This Internal Audit risk assessment process is independent of the one mentioned in Section 12.2, although it will be used to inform the Internal Audit Risk Assessment, which will also take into account, inter alia, the third party certifications.	The three lines of defence model ensures sound management of ICT third-party risk. Supervised entities should already be compliant with the requirements under Directive 2013/36/EU and further specified in the EBA Guidelines on internal governance (EBA/GL/2021/05). Therefore, it is not necessary to further clarify the role of internal audit, beyond the provisions of Article 28 of DORA.	No
461	Pooled audits	Dutch Banking Federation (DBF) The Guidance should state that institutions are encouraged to consider whether pooled auditing is advisable on a risk-based approach. It should however not specify how a pooled audit works in practice, given the need for different approaches across member states. In light of separate guidance being produced on pooled auditing this guidance should refrain from overlap.	This is a good practice observed during ECB supervisory activities. The Guide is not meant to be prescriptive.	No
462	Monitoring tools	Dutch Banking Federation (DBF) We suggest to introduce other (monitoring) tools which should be taken into account as the ECB states that monitoring tools provided by a CSP might not be sufficient.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with the ICT risk management requirements.	No
463	Scope	Dutch Banking Federation (DBF) The wording currently refers to all ICT risk management requirements rather than those relating to cloud.	The wording is in line with Article 6(10) of DORA.	No
464	Audit	Dutch Banking Federation (DBF) With regard to " An institution’s internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews…..". It's the responsibility of the designated owner in cooperation with the 3-lines and not of the IA.	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
465	Audit	Dutch Banking Federation (DBF) We suggest to add the requirements for an "independent expert" as described in the title.	Not relying solely on monitoring tools provided by the CSP implies independent expertise. The section header has been amended. Supervised entities must comply with Articles (8)(3) and 9(2)(b) of CDR (EU) 2024/1773.	Yes
466	Scope	Dutch Banking Federation (DBF) These requirements are in accordance with the DORA legislation and existing EBA guidelines. A general statement in the beginning of the document can limit further details that are	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		already known.		
467	Contractual clauses	Dutch Banking Federation (DBF) We strongly recommend the call for SCCs is dropped given that there is a EU forum already reviewing this issue. and it has not yet produced any standardised clauses. Risk of an incoherent approach from EU institutions is then not inconceivable. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	The Guide has been amended.	Yes
468	Costs of audits	Dutch Banking Federation (DBF) The recommendation that "contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost" should be deleted. This goes beyond existing practice and is not in accordance with the EBA Guidelines. The Guidance should interpret the existing legal obligations rather than adding to them through new levels of practical prescription.	The Guide has been amended.	Yes
469	Contractual clauses	Dutch Banking Federation (DBF) The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes. Setting out requirements for particular incidents will create partial coverage. The guidance should be outcomes focused	The ECB expects supervised entities to have safeguards in place against unilateral changes. The Guide has been amended.	Yes
470	Contractual clauses	Dutch Banking Federation (DBF) We recommend to delete the following sentence "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 this will not be acceptable to most commonly used non-tailor-made services by CSPs. The requirement should be only related to those CSPs that are under the direct supervision due to DORA.	The Guide has been amended.	Yes
496	Contractual clauses	DIGITALEUROPE Sub-subsection 2.5.3 should be amended to better align with the DORA text, reduce the possibility for increased misinterpretations and costs for financial entities, and remove unsubstantiated assertions that CSPs can commit fraud (‘manipulation’). Specifically, it should be AMENDED to read: 'Taking this into account, the ECB recommends that financial entities use standard contractual clauses when outsourcing cloud computing services, WHERE APPLICABLE AND RELEVANT TO THE FINANCIAL ENTITY’S USE OF CLOUD COMPUTING SERVICES'. Proposed sub-subsection 2.5.3 should also be AMENDED to DELETE the sentence beginning 'IF CONTRACTUAL PROVISIONS ARE STORED ONLINE, THE PROVIDER SHOULD BE REQUIRED TO SIGN A SEPARATE DIGITAL OR PHYSICAL COPY TO PREVENT ANY RISK OF UNILATERAL CHANGES' as it represents an unsubstantiated assertion, does not reflect the one-to-many cloud model, and is not required in DORA.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
497	Contractual clauses	DIGITALEUROPE Section 2.5.3 should be deleted	The Guide has been amended.	Yes
498	Contractual clauses	DIGITALEUROPE The last sentence of this section which states 'INSTITUTIONS SHOULD USE CONTRACTUAL CLAUSES TO ENSURE APPROPRIATE INCIDENT AND MONITORING REPORTS, ENABLING ONGOING ASSESSMENT OF OUTSOURCES FUNCTIONS' should be deleted.	Supervised entities should have a sound ICT risk management framework in place that includes the monitoring of any incidents that may impact their activities. The Guide has been slightly amended.	Yes
576	Audits	European Association of Public Banks Below we highlight the modification proposal in bold: (..:) the internal audit functions of the institutions as the third line of the control model should regularly review, following a risk based approach, the risks stemming from the use of a CSP’s cloud services. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity. The institutions fulfil these requirements if the internal audit	The three lines of defence model ensures sound management of ICT third-party risk. Supervised entities should already be compliant with the requirements under Directive 2013/36/EU and further specified in the EBA Guidelines on internal	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		carries out, on the basis of up-to-date information, an overall risk assessment of the ICT risks of the institution for the purpose of drawing up the appropriate internal audit work plan. Depending on the outcome of the overall risk assessment, the intensity and frequency of the audit assignments may differ between specific areas. This Internal Audit risk assessment process is independent of the one mentioned in Section 12.2, although it will be used to inform the Internal Audit Risk Assessment, which will also take into account, inter alia, the third party certifications.	governance (EBA/GL/2021/05). Therefore, it is not necessary to further clarify the role of internal audit, beyond the provisions of Article 28 of DORA.	
577	Audits	European Association of Public Banks "An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts). "	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
578	Pooled audits	European Association of Public Banks The Guidance should state that institutions are encouraged to consider whether pooled auditing is advisable, on a risk-based approach. It should not specify how a pooled audit works in practice, given the need for variations in approach across member states.	This is a good practice observed during ECB supervisory activities. The Guide is not meant to be prescriptive.	No
579	Monitoring tools	European Association of Public Banks The guidance should suggest what other tools should be taken into account if the ECB states that monitoring tools provided by a CSP might not be sufficient.	Considering the diverse array of services offered by CSPs and their potential combinations, additional independent tools need to be determined on a case-by-case basis by the supervised entities to ensure compliance with ICT risk management requirements.	No
580	Scope	European Association of Public Banks The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud.	This wording is in line with Article 6(10) of DORA.	No
581	Monitoring tools	European Association of Public Banks Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases, in which the institution has reason to believe manipulation has occurred.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
582	Contractual clauses	European Association of Public Banks "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".	The Guide has been amended.	Yes
583	Contractual clauses	European Association of Public Banks It would be helpful if the EBA provides actual best practice clauses / addendum that could be applied to strengthen CSP contracts	Not only is the EBA involved in the process of establishing the regulatory framework, but also the three ESAs, since DORA applies to financial entities. Supervised entities could include any contractual clause they see fit to ensure adequate monitoring of cloud services provided by a CSP, in addition to the provisions set out in Article 30(2) and 30(3) of DORA and Article 9 of CDR (EU) 2024/1773.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
584	Contractual clauses	European Association of Public Banks "Can be regarded as a guide to best practices in this respect". Please clarify that the expectation of the ECB in this respect is that if standard contractual clauses are not available, the contract must meet at least the requirements set out in the four bullets (in addition to the other contractual requirements under DORA and relevant RTS)?	This is how the ECB interprets, as a good practice, the provisions of Article 30(2) and 30(3) of DORA. The four bullet points are meant as examples and do not impose a minimum requirement. The Guide has been amended.	Yes
585	Contractual clauses	European Association of Public Banks We propose the call for SCCs is dropped given that there is a EU forum already reviewing the issue, and it has not yet produced any standardised clauses. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	The Guide has been amended.	Yes
586	Costs of audits	European Association of Public Banks The recommendation that "contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost" should be deleted. This goes beyond existing practice and the EBA Guidelines in expecting this information to be set out in the contract.	The Guide has been amended.	Yes
587	Contractual clauses	European Association of Public Banks The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes.	The ECB expects supervised entities to have safeguards in place against unilateral changes. The Guide has been amended.	Yes
596	Incident reports	Google Cloud Use of cloud services does not necessarily entail outsourcing of reporting obligations under Article 19(5) of DORA. The reference to Article 19(5) of DORA in Section 2.5.2 should be clarified to explain the relationship between Section 2.5.2 and Article 30(2)(f) of DORA.	The Guide has been amended. Irrespective to the decision of a supervised entity to outsource its incident reporting obligation, when an ICT incident occurs at the CSP, it should be contractually obliged to provide assistance to the supervised institution according to Article 30(2)(f) of DORA.	Yes
597	Contractual clauses	Google Cloud The recommendation to use standard contractual clauses in Section 2.5.3 is premature as no such clauses yet exist. Section 2.5.3 should be deleted	The ECB Guide aims to encourage supervised entities to use standard contractual clauses developed by public authorities when available. Supervised entities may use the contractual clauses developed by the European Commission for cloud computing services, as mentioned in Recital 75 of DORA. This wording is in line with Articles 8 and 30(4) of CDR (EU) 2024/1773 on contractual clauses.	Yes
634	Oversight	Bitkom 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	The ECB is of the view that while third-party certifications may be taken into consideration, these should be in addition to independent assessments/reviews conducted by the institution's own internal audit team. The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.”.		
635	Monitoring tools	Bitkom 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.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that, in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
636	Contractual clauses	Bitkom 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.”	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that, in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
637	Contractual clauses	Bitkom 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	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		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.		
638	Contractual clauses	Bitkom 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 Guide has been amended.	Yes
639	Contractual clauses	Bitkom ECB recommends that financial entities use standard contractual clause (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 helpful.	The ECB Guide aims to encourage supervised entities to use standard contractual clauses developed by public authorities when available. Supervised entities may use the contractual clauses developed by the European Commission for cloud computing services, as mentioned in Recital 75 of DORA. This wording is in line with Articles 8 and 30(4) 8 of CDR (EU) 2024/1773 on contractual clauses.	Yes
644	Audits	European Savings and Retail Banking Group (ESBG) On the effectiveness of the certifications presented by the CSP (issued by third parties). This point highlights the possible weaknesses in terms of the validity of certifications issued by third parties. On the other hand, it is admitted that, in addition to the guarantees of having the possibility of carrying out internal audits of the provider, this can be subcontracted by an entity or group of entities to a third party, which could lead to entities contracting the same third party that carried out the review that led to the certificate being obtained. It would be more efficient to make progress in defining for the whole sector which companies and with what framework and depth these cloud services should be audited, making it compulsory, if necessary, for the auditing companies	Supervised entities should demonstrate to their supervisory authorities that they comply with the provisions of Article 8(3) of CDR (EU) 2024/1773 supplementing DORA when relying on third-party certifications. Supervised entities should rely on certifications such as ISO 27001.	No

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		themselves to be certified as cloud services auditors, and for their review work to be issued, as a result of this certification and specific review framework, with sufficient guarantees of confidence for both institutions and supervisors. Such a solution exists for example with the US SOC II framework, which enjoys a guarantee of confidence for all parties. Such an approach would avoid inefficiencies and high costs for all European institutions and for the cloud service providers themselves.		
645	Contractual clauses	European Savings and Retail Banking Group (ESBG) We consider it a great support to have the standard contract clauses developed by public authorities for specific services, as included in the guidance and in Article 30(4) of DORA, however, as of today, except for the core clauses of Article 30. We consider its publication well in advance of the entry into force of DORA very positive, as entities will be required to renegotiate a large part of the contracts to include the requirements of DORA. This process could be carried out more efficiently if we had them.	The ECB Guide aims to encourage supervised entities to use standard contractual clauses developed by public authorities when available. Supervised entities may use the contractual clauses developed by the European Commission for cloud computing services, as mentioned in Recital 75 of DORA. This wording is in line with Articles 8 and 30(4) of CDR (EU) 2024/1773 on contractual clauses.	Yes
646	Contractual clauses	European Savings and Retail Banking Group (ESBG) The third point refers to on-site-audits and proposes to deal with the costs of on-site audits via “standard contractual clauses”. We note in this context that we understand the reference to “standard contractual clauses” as meaning that the contract drafters should have available a set of standard clauses that should be used by default when entering into relevant contractual documentation. In our view the use of such standard clauses is good practice in the area of contract drafting and banks are already working with such standard clauses also with regard to requirements that were already raised in the past (e.g. in the context of resolution resilience of service contracts). The side benefit of such use is that it helps to streamline and facilitate the drafting and negotiation of contracts. However, experience also shows that the drafting of such clauses poses some challenges since they should at the one hand be detailed enough to provide clear guidance on what the respective parties want to agree on, and on the other hand should be drafted general enough to allow for a wide-spread use and in order to make them future-proof so that they need not be changed every other month. We thus usually avoid going into too much detail and rather agree on general principles – like, e.g., who bears what costs, are some costs already included in the fees, et cetera.	When supervised entities negotiate contractual arrangements with a CSP, it is their responsibility to ensure that such arrangements contain sufficient details to adequately monitor the cloud services supporting a critical or important function. The ECB agrees with the comment. The Guide has been amended by removing “the breakdown and maximum cost of audit”.	Yes
666	Oversight and monitoring	Futures Industry Association The ECB should not enforce monitoring of CSPs to be undertaken by a single centralised function or a single department within a financial entity. Financial entities may utilise different teams and functions for oversight and monitoring of a CSP due to the nature of the cloud service, the different expertise of various teams, how it operates across multiple financial entities or services and the materiality of the service provided. Enforcement of all monitoring within one function would not utilise the expertise of the financial entity effectively and would require reorganization of well-established functions within financial entities. Oversight and monitoring can be undertaken by individual cloud teams, third party oversight, cybersecurity functions, and technology functions or a combination of colleagues within those teams. Amendment proposed: 2.5.1: “… supervised institutions should retain expertise in-house, with a centralised function or department being recommended for the monitoring of CSPs. The monitoring…” The European Central Bank (ECB) emphasizes that financial institutions should not rely exclusively on monitoring tools offered by Cloud Service Providers (CSPs). Instead, they should complement this information with independent monitoring tools. While we recognise the ECB’s intent to ensure there is not a reliance on CSP information, current	The Guide has been amended.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		market availability for independent tools would still require information to be provided by the CSP. In all likelihood, any independent tooling would still be dependent on the CSP. Therefore, the mandatory nature of this requirement should be evaluated with a risk-based perspective.		
692	Third-party certification	German Banking Industry Committee (GBIC) In 2.5,""An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts)"" should be clarified.	The ECB considers as a good practice that audits of hyperscalers are replaced with regular, neutral and independent certification of the services concerned, initiated by the hyperscaler and confirmed by the supervisory authorities.	No
693	Monitoring tools	German Banking Industry Committee (GBIC) Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases in which the institution has reason to believe manipulation has taken place. In addition to this, joint audits should stay on a voluntary basis.	It is the responsibility of supervised entities to verify compliance with ICT risk management requirements. The ECB is of the view that in the case of critical functions, the monitoring tools provided may not be sufficient to ensure compliance with the requirements and therefore independent tools should be used to enhance the surveillance. The Guide has been amended.	Yes
694	Audits	ISACA Art.28.5 of the RTS on ICT risk management framework under DORA specifies that auditors should possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. Recognised professional certifications are a convenient and effective tool to ensure the quality of perspective testers, as recognised in the TIBER-EU procurement guidelines Accordingly, we suggest a similar specification is made in the ECB guidance as well. A line could be added specifying that auditors should possess the appropriate skills to perform their task in accordance with this guidance and be certified in line with recognised market standards for the performance of their activitie""	The Guide has been amended.	Yes

2.7 Table 7 – Comments not referring to a particular section

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
129		American Chamber of Commerce to the European Union Provide flexible and risk-based guidance focusing on proportionate outcomes rather than prescriptive expectations. The ECB should not prescribe specific forms of technology solutions that inadvertently define a financial entity's future technology stack and adoption. We encourage the development of a holistic, risk-based approach to third-party risk management for the EU financial sector instead of the multitude of frameworks currently in place that cover overlapping outsourcing and ICT populations. This would allow financial institutions (FIs) to adapt their risk management frameworks to any cloud-specific or evolving technology risks that the ECB considers as not adequately covered by current regulatory frameworks.	The ECB believes that the term "good practice" should be treated as a suggestion that supervised entities are invited to follow, unless they decide not to after duly considering the matter based on a risk-based approach.	Yes
132		American Chamber of Commerce to the European Union Align key definitions to the relevant DORA definitions.	The definitions have been aligned with DORA.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
133		American Chamber of Commerce to the European Union Critical or important functions: There is already a significant divergence across different regulations in the terminology and criteria used to identify what is 'critical'. The ECB's Guide currently uses two different definitions of criticality: 'Critical Functions' for which it uses the definition of 'Critical or Important Functions' from the EBA's Outsourcing Guidelines; and 'Critical or Important Functions' for which is uses a slightly amended version of the definition for 'Critical Functions' under the Bank Recovery and Resolution Directive (BRRD). Neither of these is aligned with DORA's definition of 'Critical or Important Functions'. Given the ECB's Guide is purported to reflect the ECB's understanding of DORA and how its requirements apply to the banks it supervises in the context of cloud outsourcing, aligning the Guide's definition to DORA would provide clarity and consistency to help industry meet supervisory expectations.	The definition of "critical or important function" has been aligned with DORA When implementing good practices as set out in the Guide, supervised entities may resort to the principle of proportionality...	Yes
134		American Chamber of Commerce to the European Union Subcontractors: The Guide uses the phrase 'suppliers of subcontracted services supporting the CSP'. This phrase is not used in DORA or the secondary texts. To reduce confusion, the ECB should align the terminology in the Guide about subcontracted services with language in the Implementing technical standards (ITS) on the Register of Information (ie 'subcontractors that effectively underpin the provision of these ICT services').	The definitions have been aligned with DORA.	Yes
135		American Chamber of Commerce to the European Union Directive on measures for a high common level of cybersecurity across the Union (NIS2): It has been confirmed that DORA applies with lex specialis status with regards to NIS2 for those areas where they overlap. The ECB's referencing of NIS2 requirements that overlap with the coverage of DORA does not recognise this status, and risks basing the ECB's expectations on an incorrect legislative basis and creating confusion across industry regarding the application of NIS2 and DORA. The Guide should reference the interpretation in regards to DORA and remove all references to NIS2 in order to reduce this uncertainty for the sector.	All references to the NIS 2 Directive have been removed from the Guide.	Yes
136		American Chamber of Commerce to the European Union Ensure consistency with the DORA level 1 text and avoid gold-plating. The Guide is positioned as an explanation of the ECB's understanding of DORA. However, in several cases the Guide either places more limitations on or create additional requirements for financial institutions using cloud services that are not contemplated in DORA. For example:	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes
141		American Chamber of Commerce to the European Union Furthermore, the draft mentions in its scope and effect chapter that non-CSP third-party providers (TPPs) that are reliant on cloud services are expected to fall under the same supervisory regime as the CSP. This expectation is not consistent with DORA; the term 'reliant' gives too much room for interpretation, making this requirement disproportionate for TPPs.	The ECB has clarified that the supervisory expectations apply to non-CSP TPPs only in cases where critical or important functions are addressed.	Yes
143		American Chamber of Commerce to the European Union Determine the timing of requirements associated with ECB Guide in a pragmatic way, aligned with overall DORA timelines. The ECB has not clearly communicated the anticipated timeline for implementation of its expectations. Four supplementary technical standards have yet to be finalised (Register of Information, Subcontracting of CIFs, Threat-led penetration testing and Major ICT incident reporting). To allow the ECB's Guide to reflect both these technical standards and those that have been recently published in the Official Journal of the EU, the ECB should defer publication of the Guide until all of the supplementary technical standards are completed. Given the pace of ongoing work on DORA's implementation across industry, the ECB should also allow for an appropriate	The ECB Guide will take effect as of its publication date. It does not constitute a new legal requirement.	Yes

No	Topic	Comment(s) received	ECB response and analysis	Amended (yes/no)
		implementation period.		
144		American Chamber of Commerce to the European Union The financial services industry and its third parties are currently grappling with their implementation of DORA's comprehensive requirements. Industry has highlighted DORA's significant compliance challenges and the tight implementation timeline, and these concerns have been acknowledged by the ESAs. DORA specifically contemplates the types of risks associated with ICT third-party service providers, such as CSPs, and sets out enhanced and harmonised risk management requirements, alongside an oversight framework that is expected to capture those CSPs that pose the most significant threats to the stability of the EU financial sector. Not only does the ECB's approach risks undermining DORA's harmonisation objectives, but additional prescriptive guidance will require EU financial entities to interpret and comply with more expansive, specific and overlapping rules, creating an increasing convoluted and complex regulatory environment.	Similar to other ECB Guides this Guide does not lay down new legally binding requirements. Where the words "should" and "ensure" are used, the Guide means to say that these requirements are covered by existing legislation, which is also cited in the relevant passages. When the Guide refers to good practices, these are recommendations	Yes