EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

European Association of Public Banks

Contact person

Mr/Ms

First name

Surname

Email address

Telephone number

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

General comments

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

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

Deadline:	15.07.2024

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
1	1. Introduction 1.1. Purpose			Clarification	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.	If the ECB intends all aspects of the guidance to be strictly adhered to, rather than permitting firms to **adopt a risk based proportionate approach**, this should be clearly set out.	European Association of Public Banks	Don't publish
2	2. Introduction 1.1. Purpose		2	Clarification	What is exactly meant by CSP in case of SaaS? The SaaS provider or the underlying cloud platform provider?	Concentration risks are on platform level	European Association of Public Banks	Don't publish
3	3. Introduction 1.1. Purpose		2	Amendment	Align the definition of "critical or important function" with the DORA definition of "Critical or Important Function"	Ensure we do not have different definitions across different regulatory documents to ensure harmonisation and clarity	European Association of Public Banks	Don't publish
4	4. Introduction 1.1. Purpose		2	Amendment	Align the definition of "ICT assets" with the DORA definition of "ICT asset"	Ensure we do not have different definitions across different regulatory documents to ensure harmonisation and clarity	European Association of Public Banks	Don't publish
5	5. Introduction 1.1. Purpose		2	Amendment	Align the definition of 'service provider' with the definition of 'third party service provider' under DORA	Ensure we do not have different definitions across different regulatory documents to ensure harmonisation and clarity	European Association of Public Banks	Don't publish
6	6. Introduction 1.1. Purpose		2	Amendment	Which definition of outsourcing is used here?	Unclarity about definition of outsourcing	European Association of Public Banks	Don't publish
7	6. Introduction 1.1. Purpose		1	Clarification	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 DORA definition should be applied for a harmonized understanding.	European Association of Public Banks	Don't publish
8	6. Introduction 1.1. Purpose		1	Clarification	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 DORA definition should be applied for a harmonized understanding.	European Association of Public Banks	Don't publish

9	1. Introduction 1.2 Scope and Effect		3	Clarification	While the guidance notes that DORA requirements remain the legally binding obligations, **certain provisions within the guidance could require further contractual remediation.**	With financial entities under severe pressure to ensure DORA requirements are met by Jan 2025, there should **no expectation of further remediations.**	European Association of Public Banks	Don't publish
10	1. Introduction 1.2 Scope and Effect		3	Clarification	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.	Misaligned timeframes will create significant confusion.	European Association of Public Banks	Don't publish
11	1. Introduction 1.2 Scope and Effect		3	Clarification	It is not always clear with **who the obligation sits**, whether a CSP or the financial entity.	Unless the CSP is the target of certain provisions, the proposed approach for example on joint testing, is unlikely to work in practice.	European Association of Public Banks	Don't publish
12	1. Introduction 1.2 Scope and Effect		3	Deletion	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 **overlapping regulatory requirements** creates conflicting expectations, in particular whether the provisions should apply to CIFs or all services.	European Association of Public Banks	Don't publish
13	1. Introduction 1.2 Scope and Effect		3	Amendment	The Guidance is using **the BRRD definition of Critical and Important Functions**, rather than the DORA defintion which is unhelpful misalignment. Similarly, the defintion of ICT asset should be that which is used in DORA.	Inconsistent regulatory context - the guidance should be using DORA definitions.	European Association of Public Banks	Don't publish
14	1. Introduction 1.2 Scope and Effect		3	Clarification	There is i**nconsistency 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?	Without clarity that this relates to cloud services supporting CIFs, the guidance will be lacking in proprtionality 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.	European Association of Public Banks	Don't publish
15	1. Introduction 1.2 Scope and Effect		3	Clarification	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.	Again, without such clarification there would be a lack of **proportionality** and enforceability.	European Association of Public Banks	Don't publish
16	1. Introduction 1.2 Scope and Effect	1.2	3	Clarification	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.	Prevent scattered details across different guidances	European Association of Public Banks	Don't publish

17	1. Introduction 1.2 Scope and Effect		3	Amendment	"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***".		European Association of Public Banks	Don't publish
18	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	3	4	Amendment	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 legal **obligation for an CSP should be on ensuring the FE can meet its regulatory requirements**; not mirroring the FE obligations.	European Association of Public Banks	Don't publish
19	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	2.1.1	4	Clarification	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."	Clarfify scope	European Association of Public Banks	Don't publish

20	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	2.1.1	4	Amendment	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.	Please replace 'equivalent' by 'appropriate'.	European Association of Public Banks	Don't publish
21	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question		4	Amendment	"Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls."	It is not appropriate for third-parties to establish "*equivalent* " risk management practices to a financial entity. Risk management and contractual frameworks between FEs 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.	European Association of Public Banks	Don't publish
22	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Clarification	Under Art. 28 (4) DORA, instititutions 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..."	Within the framework of the requirements care must be taken to ensure that the institutions do not always conclude contracts with service providers who have already implemented such controls. Normally, service providers set up such controls once they want to work with us. In these cases, the institutions cannot check whether the controls are functional and suitable as part of the pre-outsourcing audit. Therefore, an audit of the controls before outsourcing should not end up on the mandatory agenda of the auditors, and only be considered "best practice".	European Association of Public Banks	Don't publish

23	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Amendment	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.		European Association of Public Banks	Don't publish
24	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	4	4	Clarification	It is unclear why the ECB has said some c**onsiderations should be required and others are good practice**. Is the expectation in practice going to differ?	The guidance is extending **beyond DORA obligations** by stating that all these considerations should be included, rather than permitting a risk-based approach.	European Association of Public Banks	Don't publish
25	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	5	4	Amendment	It should be added that institutions should perform **analysis of the control processes "on the basis of the data flows provided"**.	In order to boost the **feasibility** of the guidance.	European Association of Public Banks	Don't publish
26	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	6	5	Deletion	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	Lack of **feasibility and proportionality**. The Guidance is building on existing requirements, rather than providing an interpretation.	European Association of Public Banks	Don't publish
27	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	DORA is not limited to outsourcing -> definition of outsourcing in this document is confusing.	DORA is not limited to outsourcing -> definition of outsourcing in this document is confusing.	European Association of Public Banks	Don't publish
28	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	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.	Do not recognize part of this text	European Association of Public Banks	Don't publish
29	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	Data Storage and processing risks: Does this also include data localisation risks, i.e. risks of transferring data to a country and impedements in transferring data out of that country?	Clarify whether this includes localisation risk	European Association of Public Banks	Don't publish
30	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	physical: We would expect that physical risks are also region specific?	Clarify	European Association of Public Banks	Don't publish
31	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Amendment	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.	remove this element	European Association of Public Banks	Don't publish
32	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	Multi-tenant environment risk: What specific risks are meant, on top of unauthorized access to data?	Clarify	European Association of Public Banks	Don't publish

33	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy		5	Clarification	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 **guidance is extending beyond DORA obligations** and creating misalignmment.	European Association of Public Banks	Don't publish
34	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Amendment	"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	Should we have backups for all data in Microsoft Azure in another cloud?	European Association of Public Banks	Don't publish
35	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2	6	Deletion	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).	This **goes beyond the EBA/DORA existing requirements and suggests a disconnect from technical reality**. The DORA requirements, whcih followed significant debate, settled on physical and logical segregation (Art 12). Recent experiences (for example with Unisuper) has demonstrated that back-up from within the same cloud service is at times criticial for recovery.	European Association of Public Banks	Don't publish
36	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	3	6	Deletion	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 center. 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 standard approach to date with BCP testing has been **severe but plausible. This should not be departed from.**	European Association of Public Banks	Don't publish

37	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	3	6	Deletion	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"	Having **on-premises backups is not always technically feasible** in many cases	European Association of Public Banks	Don't publish
38	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Clarification	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.	Clarify that back-ups can be within the same service provider	European Association of Public Banks	Don't publish
39	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Clarification	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.	Please clarify requirement to set RTOs and RPOs for different scenario's.	European Association of Public Banks	Don't publish

40	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Clarification	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 datacenter 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.	Our counter-proposal would be tailored-business continuity plans to the specific risks and capacities of the institution, focusing on practical and achievable measures.	European Association of Public Banks	Don't publish
41	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Deletion	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.		European Association of Public Banks	Don't publish

42	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Deletion/Amendment	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 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 […]".		European Association of Public Banks	Don't publish
43	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2	7	Amendment	Concerning an exit without cooperation from the CSPs we suggest taking into account that	Lacking in **proportionality**	European Association of Public Banks	Don't publish
44	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	3	7	Deletion	Recommend deleting: *To this end, institutions should consider using t**echnologies 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*	This level of prescription 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.	European Association of Public Banks	Don't publish
45	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	4	6	Clarification	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.	Potential lack of confidence from industry	European Association of Public Banks	Don't publish

46	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	4	6	Clarification	Regarding the reference to Article 6(8) of DORA, it should be viewed as a **general provision that encompasses all technologies, including the Cloud**.	Developing **ad-hoc strategies** for each project could weaken its implementation and relevance	European Association of Public Banks	Don't publish
47	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6	Amendment	Concerning the separation of data centers 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.	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.	European Association of Public Banks	Don't publish
48	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6	Deletion/Amendment	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.	Smaller banks may not have data centers or on-prem is very expensive, it would make more sense to refer to another technical area (no on-prem) or rather use a risk-based approach based on the bank's own risk assessment as a recommendation	European Association of Public Banks	Don't publish

49	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Clarification	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.	Please align with Data Act	European Association of Public Banks	Don't publish
50	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	1	8	Amendment	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"	This appears to suggest a lack of understanding about Cloud in a multi-tenanted environment.	European Association of Public Banks	Don't publish
51	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2	8	Deletion	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)	This clashes with the **contract remediation requirements** as part of DORA, which already represent a significant operational uplift for financial entities.	European Association of Public Banks	Don't publish
52	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	3	7	Clarification	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**.	To avoid misinterpretation and ambiguity	European Association of Public Banks	Don't publish
53	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	4	7	Amendment	Spot checks on all services as part of diaster 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.	Lacking in **proportionality**	European Association of Public Banks	Don't publish

54	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy		8	Amendment	While generally reasonable, the original phrasing of the section on personell (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.	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. Such suggested guidance risks creating an undesirable environment of continual off-cycle contract renegotiations without meaningfully addressing the real issue or risk.	European Association of Public Banks	Don't publish
55	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Clarification	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.	It is unreasonable to expect FEs to account for all these indicators. In particular, the expectation for firms to consider the extent to which other supervised firms are reliant on the same CSPs requires an assessment of sector-level concentration risks, which is beyond individual FEs capacity and responsibility to consider. We would suggest to delete the last sentence in 2.2.4 given that new functions are difficult to take into account at the moment of an evaluation of concentration risk	European Association of Public Banks	Don't publish
56	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes		9	Amendment	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 "examplary measures".	The overall encryption process creates an unnecessary amount of work. Some institutions do not use cryptography entirely, but different means to obtain the same level of security.	European Association of Public Banks	Don't publish
57	2.3 ICT, security, data confidentiality and integrity 2.3.2 Risks stemming from location		10	Deletion	„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."	This is extremely demanding and for most of the time more than 100 subcontractors of a CSP not feasible in practice". In addition, so far from a data protection point of view the assessment obligation is only given for the sub-contractor in scope, and not holistically for the entire sub-contractor chain	European Association of Public Banks	Don't publish

58	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.3 Consistent inclusion of outsourcing assets in an institution's inventory of ICT assets		10	Clarification	"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 inclusion of all ICT assets is an immense burden for the reporting entities and does not reflect the rationale behind DORA of identifying the CCSPs.	European Association of Public Banks	Don't publish
59	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.3 Consistent inclusion of outsourcing assets in an institution's inventory of ICT assets	1	11	Clarification	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, so there should be no broader obligation on other types of ICT assets.	European Association of Public Banks	Don't publish
60	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	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.		European Association of Public Banks	Don't publish
61	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	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.		European Association of Public Banks	Don't publish
62	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	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	Given the complexity and frequent changes of IAM policies the reflection ot the exact content in the outsourcing agreement goes beyond the DORA framework. Therefore only the existence and regular review of the IAM policy should be stated.	European Association of Public Banks	Don't publish
63	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	4	11	Deletion	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 guidance is going beyond the obligations of DORA in prescribing the form as well as substance.	European Association of Public Banks	Don't publish

64	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.1	11	Clarification	"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.	What is meant by 'clauses' here?	European Association of Public Banks	Don't publish
65	2.4 Exit strategy and termination rights 2.4.1 Termination rights	1	13	Deletion	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 guidance should be embedded in the wider regulatory landscape.	European Association of Public Banks	Don't publish
66	2.4 Exit strategy and termination rights 2.4.1 Termination rights	4, 5	12	Deletion	The Gudiance 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 succeessfully execute cloud provider test migrations at the agreed times."	Seeking to **create non-binding termination rights** which do not reflect existing legal or market practice is lacking both proportionality and feasibility. This goes beyond DORA and EBA requirements.	European Association of Public Banks	Don't publish
67	2.4 Exit strategy and termination rights 2.4.1 Termination rights	4,5,6	12	Deletion	The prescriptive, yet non-exhaustive, nature of the guidance detracts from the precriptive 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 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.	European Association of Public Banks	Don't publish
68	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Amendment	"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".	None of these points are within the CSP's sphere of influence. Such clauses must give the CSP an opportunity to perform the contract correctly. Therefore the institutions may not be able to enshrine a corresponding clause in the context of general terms and conditions in a legally effective manner unless at the same time a remedy for the CSP is agreed (e.g. by moving). In a case of doubt it should be sufficient that a service will then be provided by another CSP and not by the institution itself.	European Association of Public Banks	Don't publish
69	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Deletion	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.	To be deleted as it cannot be adhered to.	European Association of Public Banks	Don't publish
70	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1		Clarification	"(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	Clarify	European Association of Public Banks	Don't publish

71	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	"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 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.	Reconsider this criterium	European Association of Public Banks	Don't publish
72	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Clarification	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.	Please clarify that insitutions would take this into account when terminating in line with art. 28(7) DORA	European Association of Public Banks	Don't publish
73	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan		13	Deletion	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	Art. 28 (8) DORA does not outline a principle based exit strategy with granular technical exit plans for individual cloud outsourcing arrangements: The exit plan should follow the risk based approach as outlined the overall framework of DORA. It has to be realistic and feasible, based on plausible scenarios and reasonable assumptions incl. a timeline which corresponds to the exit and termination conditions:	European Association of Public Banks	Don't publish

74	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans		13/14	Amendment	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 atarget, 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).	Since the guide specifies the possibility of taking into account external support, this has been added for clarification. The option to take on board additional help as the need arises is an important step to retain the necessary flexibility needed. Therefore, it should also be noted, that a general description of necessary skill sets may be more prudent than preemptively allocating personell resources in order to retain the necessary flexibility to conduct an exit regardless of fluctuations within the institution. We also suggest to stay aligned with the Data Act.	European Association of Public Banks	Don't publish
75	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress		14	Deletion	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.		European Association of Public Banks	Don't publish

76	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	3	14	Amendment	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.	Lacking in proportionality	European Association of Public Banks	Don't publish
77	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	3	14	Deletion	The reference to conflicting legislation appears to be referencing potential third country sanctions. This should be dealt with separately.	The guidance should remain technical in nature, rather than incorporating political discussions best reserved for other policy vehicles.	European Association of Public Banks	Don't publish
78	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	1	15	Amendment	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 fulfill 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.**	We believe that it should be clarified: i) the role of IA as the third line in the control model; ii) that it provides assurance following a risk-based approach; iii) IA performs a risk assessment, which is independet from the RA perfoms by the first/second line; iv) this risk assessment process allows us to assess the risks to which the entity is exposed and, based on the result of this assessment, to prioritise the Internal Audit Plan.	European Association of Public Banks	Don't publish
79	2.5 Oversight, monitoring and internal audits		15	Clarification	"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). "	Audits of hyperscalers should be replaced by regular neutral and independent certification for the services concerned initiated by the hyperscaler and confirmed by the supervisory authorities.	European Association of Public Banks	Don't publish
80	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	3	15	Amendment	The Guidance should state that institutions are encouraged to consider whether pooled auditing is adviseable, 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.	In light of separate guidance being produced on pooled auditing this guidance should refrain from overlap.	European Association of Public Banks	Don't publish
81	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	4	15	Clarification	The guidance should suggest what other tools should be taken into account if the ECB states that monitoring tools provded by a CSP might not be sufficient.	Lack of clarity about ECB expectations without further examples.	European Association of Public Banks	Don't publish

82	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	4	15	Amendment	The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud.	Extension of scope in the guidance beyond Cloud.	European Association of Public Banks	Don't publish
83	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs		15	Clarification	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.		European Association of Public Banks	Don't publish
84	Box 2: Contractual clauses		15	Clarification	“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”.	This recommendation does not reflect how contractual negotiations with CSPs actually occur and it will not be practically feasible to achieve. Standard contractual clauses may limit the ability of the industry to embrace technological advancements, they may hinder the ability of firms to negotiate effectively with their providers and are not effective in an innovative space unless regularly update. Any standard contractual clauses should be set out as indicative examples with no requirement for rigid adherence.	European Association of Public Banks	Don't publish
85	Box 2: Contractual clauses	2.5.3	16	Clarification	It would be helpful if the EBA provides actual best practice clauses / addendum that could be applied to strengthen CSP contracts		European Association of Public Banks	Don't publish
86	Box 2: Contractual clauses	2.5.3	16	Clarification	"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)?	Clarify in case there are no SCCs available	European Association of Public Banks	Don't publish
87	Box 2: Contractual clauses	4	16	Deletion	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.	Risk of incoherent approach from EU institutions.	European Association of Public Banks	Don't publish
88	Box 2: Contractual clauses	7	16	Deletion	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 **Guidance should interpret the existing legal obligations, rather than adding to them** through new levels of practical prescription.	European Association of Public Banks	Don't publish

89	Box 2: Contractual clauses	8	16	Amendment	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.	European Association of Public Banks	Don't publish